A USER-CENTRIC FRAMEWORK FOR ADDRESSING VULNERABILITY TO SOCIAL ENGINEERING IN SOCIAL NETWORKS

A MIXED METHODS STUDY OF A SAUDI ACADEMIC COMMUNITY

SAMAR MUSLAH ALBLADI

Department of Computer and Information Sciences
University of Strathclyde

A Thesis Submitted in Fulfilment of the Requirements for the Degree of
Doctor of Philosophy

2019

This thesis is dedicated to my loving parents, my husband, my kids, my brothers and sisters for their endless love, support, and encouragement

DECLARATION

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: 

Date: 09/09/2019

ACKNOWLEDGEMENTS

First and foremost, I would like to thank almighty Allah for giving me the knowledge, strength, and ability to complete this research.

I would like to express my great appreciation to my supervisors, Dr. George Weir and Dr. John Wilson, for their fine supervision and guidance throughout my PhD study. Thanks should also go to my fellow PhD students, academics and support staff in the department of computer and information sciences at the University of Strathclyde for their unlimited advice, support, and assistance throughout this journey.

I would also like to extend my deepest appreciation and gratitude to my father (my idol) and my mother (my inspiration) for believing in me and for their prayers, endless love and support throughout my life. My sincere thanks go also to my brothers and sisters for their encouragement and support over many years. I am so lucky and so proud to have such a wonderful family.

I cannot begin to express my thanks to my beloved husband, Abdulmajeed, who has always been supportive and caring. The completion of this thesis would not have been possible without his help and encouragement; and for all of that I am eternally grateful. Special thanks to my little angels, Musab and Leen, for their patience during my long absence to work on this thesis. You have made all the years spent in this journey bearable, exciting, and more fun.

I am sincerely grateful to the many individuals who voluntarily participated in my research and to all the experts and reviewers who provided me with insights, feedback and recommendations. Finally, the financial support of the University of Jeddah is also gratefully acknowledged.

PUBLICATION LIST

The following articles have been presented and published in scientific journals or conferences' proceedings based upon the research of this thesis. One further journal article has been submitted for publication, yet, still under review.

Peer-Reviewed Publications:

- Albladi, S. M., & Weir, G. R. (2018). User Characteristics that Influence Judgment of Social Engineering Attacks in Social Networks. *Human-Centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7
- Albladi, S. M., & Weir, G. R. (2018). A Semi-automated Security Advisory System to Resist Cyber-Attack in Social Networks. In N. Nguyen, E. Pimenidis, Z. Khan, & B. Trawiński (Eds.), *Computational Collective Intelligence* (pp. 146–156). Springer, Cham. https://doi.org/10.1007/978-3-319-98443-8_14
- Albladi, S. M., & Weir, G. R. (2017). Personality Traits and Cyber-attack Victimisation: Multiple Mediation Analysis. In *2017 IEEE Internet of Things - Business Models, Users, and Networks* (pp. 1–6). Copenhagen, Denmark: IEEE. https://doi.org/10.1109/CTTE.2017.8260932
- Albladi, S. M., & Weir, G. R. (2017). Competence Measure in Social Networks. In *2017 IEEE International Carnahan Conference on Security Technology (ICCST)* (pp. 1–6). Madrid, Spain: IEEE. https://doi.org/10.1109/CCST.2017.8167845
- Albladi, S. M., & Weir, G. R. (2016). Vulnerability to Social Engineering in Social Networks: a Proposed User-centric Framework. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1–6). Vancouver, Canada: IEEE. https://doi.org/10.1109/ICCCF.2016.7740435

Conference Presentations:

- Albladi, S. M., & Weir, G. R. (2019). A Conceptual Model to Predict Social Engineering Victims. In *12th IEEE International Conference on Global Security, Safety & Sustainability*, London, United Kingdom
- Albladi, S. M., & Weir, G. R. (2018). Does the Type of the Cyber-attack Matter? In *the International Conference of Big Data in Cybersecurity*, Edinburgh, United Kingdom.
- Albladi, S. M., & Weir, G. R. (2017). Factors Affecting Users' Judgment of Cyberattacks. In *the International Conference on Big Data in Cyber Security*, Edinburgh, United Kingdom.

ABSTRACT

The popularity of social networking sites has attracted billions of users from around the world to engage with and share their information on these networks. The vast amount of circulating data and information exposes these networks to several security risks. Social engineering is one of the most common types of threat that may face social network users. Social engineering is an attack technique for manipulating and deceiving users in order to access or gain privileged information. Training and increasing users' awareness of such threats is essential for maintaining continuous and safe use of social networking services. Identifying the most vulnerable users in order to target them for these training programs is desirable for increasing the effectiveness of such programs. In this context, the present research investigates user characteristics that impact on susceptibility to social engineering-based attacks, using a sequential exploratory mixed methods approach designed in three study phases. The first study phase proposed and validated a user-centric framework that was formulated on the basis of four different perspectives: socio-psychological, habitual, perceptual, and socio-emotional. The measurement scales for the selected user-centric characteristics were developed and validated in the second study phase. The third study phase constructed a conceptual model that predicts users' susceptibility to social engineering victimisation. According to the scenario-based experiment that was conducted to test the proposed conceptual model, there are direct and indirect effects of users' characteristics on their susceptibility to social engineering-based attacks on social networks. Users' trust, level of involvement, and experience with cybercrime were found to be the strongest predictors of users' vulnerability; while personality traits and users' motivation to use social network were found to have an indirect impact on their vulnerability and to be mediated by other factors in the model. This research contributes to the existing knowledge of social engineering in social networks, particularly by augmenting the research area of predicting user behaviour towards security threats with the proposal of a novel framework and model to show how user vulnerability to social engineering-based attacks can be predicted. Socio-emotional and perceptual factors, which have been given less attention in previous literature, were revealed by the findings of this research as critical aspects in predicting users' vulnerability. Social network users have different personalities, experiences, and backgrounds. The present research has considered these differences and offers personalised advice that targets the individual user's needs by designing an architecture for a semi-automated security advisory system which provides new insight into combatting social engineering threats.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AVE	Average Variance Extracted
CB-SEM	Covariance Based Structural Equation Modelling
CCEXP	Cybercrime Experience
Comp_K	Computer Knowledge
DV	Dependent Variable
EFA	Exploratory Factor Analysis
Frq_use	Frequency of Usage
IS	Information Security
IVs	Independent Variables
KnownFR	Percentage of Known Friends
Num_Con	Number of Connections
Per_T	Personality Traits
PLS	Partial Least Squares
PLS-SEM	Partial Least Squares Structural Equation Modelling
SE	Social Engineering
SN	Social Network
SNEXP	Social Network Experience
SNSs	Social Networking Sites
TrustM	Trust Member
TrustP	Trust Provider
UCF	User-Centric Framework
VCFA	Verification Code Forwarding Attack
VIF	Variance Inflation Factor

Chapter 1. INTRODUCTION

1.1 Research Overview

Although stronger security measures are increasingly developed, promoted and deployed, the number of security breaches is still increasing (Ponemon Insititute LLC, 2017). This may be because cybercriminals often target a weak and easy access point, namely the user. No security issue can arise unless there is a weakness that can be exploited by cybercriminals (Mulligan & Schneider, 2011). Security breaches are causing significant damage to organisations in different industries by decreasing customer trust (Martin, Borah, & Palmatier, 2017) and stock returns (Hinz, Nofer, Schiereck, & Trillig, 2015). According to a report published in 2015, the estimated cost of the 2013 data breach affecting Target, a retail company in the US, ranges between $11 million and $4.9 billion (Weiss & Miller, 2015). Furthermore, a recent study conducted by the Ponemon Institute (2017) states that cyber breaches among 419 organisations cost an average of $3.62 million. Using advanced and sophisticated deception methods that manipulate the user in order to access sensitive information is the essence of social engineering (SE). Most communication media, such as email, telephone, and recently social networks, have been affected by social engineering threats.

This research focuses on social engineering attacks in social network environments because social networks are among today's most popular communication media, attracting billions of active users to share and express their thoughts, photos, and locations with others. This popularity has attracted cybercriminals who find social networks a rich setting for their illegal activities. Through social networking sites (SNSs), social engineers can execute direct attacks, such as social network phishing (Vishwanath, 2015) and reverse social engineering (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011), or indirect attacks, such as hijacking the victims' social network accounts to collect information that facilitates subsequent attacks in other contexts. Examples are locating employees' personal information by tracking their online footprints on social networking sites (Shindarev, Bagretsov, Abramov, Tulupyeva, & Suvorova, 2018), or linking employees' profiles across multiple social network channels (Edwards, Larson, Green, Rashid, & Baron, 2017), which can facilitate successful social engineering attacks on their company.

Relying on social network providers to protect their users' privacy and security from cybercriminals is a common approach among users of such networks. These users may tend

to reveal their sensitive information online without being aware of potential exploitation (Polakis et al., 2010). Rather than exploiting technical means to reach their victims, cybercriminals may instead use deceptive social engineering strategies to convince their targets to accept the lure.

The risks to users persist, with a recent study revealing that only 25% of its participants have detected phishing attacks (Iuga, Nurse, & Erola, 2016). Thus, research aiming to comprehend human activities and practices that lead to potential abuses is vital to thwart the effectiveness of any security threats (Darwish, Zarka, & Aloul, 2012). Existing social engineering vulnerability studies have concentrated on variables that make human users powerless against social engineering threats, such as personality traits (Uebelacker & Quiel, 2014), demographics (Mohebzada, Zarka, Bhojani, & Darwish, 2012), and online habits (Vishwanath, 2015), and considered them separately. However, previous studies have never attempted to analyse their impact together within the same structure in the context of social networks.

In this context, the present research proposes and validates a user-centric framework (UCF) with a view to building a coherent understanding of human susceptibility to social engineering-based attacks in the social network (SN) setting. Additionally, this research develops a conceptual model that reflects the extent to which the user-related factors and dimensions that have been identified in the UCF are integrated as a means to predict users' susceptibility to social engineering-based attacks. This research also examines whether users' vulnerabilities differ across cyber-attack categories in the context of social networks, with a focus on the possibility of segmenting social network users based on their characteristics and weaknesses. In turn, this provides a means of designing an architecture for a personalised semi-automated security advisory system that sends awareness posts to target individual users' needs.

This research included three main phases and utilised a sequential exploratory design to reach the research objectives. The first phase comprises a review of the literature undertaken to build the UCF while using a mixed methods expert review that involves collecting both quantitative and qualitative data to validate the proposed framework. The second research phase includes a content validity test to evaluate the constructs measurement that will be used in the third phase. The third phase uses a scenario-based experiment to examine the relationships between the behavioural constructs in the conceptual model and the model's ability to predict user vulnerability to SE victimisation. The results of the third research phase

have helped in designing an architecture of a semi-automated security advisory system that responds to individual users' vulnerabilities.

1.2 Motivation

Recent review research has addressed different limitations in terms of practice and theory of security and privacy research in the information security (IS) field (Lowry, Dinev, & Willison, 2017). The review research acknowledged three promising contexts for future security and privacy research: online platforms, internet of things, and big data. Online platforms have achieved a massive business transformation in recent years. The online platforms Amazon and Facebook have become two of the world's most valuable and successful companies (Barwise & Watkins, 2018). Yet, security and privacy of the information held are among the critical issues associated with online platforms. Social network platforms like Facebook promote uncontrolled and excessive sharing of private information with network friends (Rathore, Sharma, Loia, Jeong, & Park, 2017). However, in social networks behavioural research, extensive attention has been given to privacy-related issues, while limited research has focused on the social network's pertinent information security problems (Saridakis, Benson, Ezingeard, & Tennakoon, 2016).

With social networking sites witnessing a huge increase in the number of accounts communicating every day, protecting the users from malicious accounts becomes even more challenging. Social engineering is considered one of the biggest threats to information security nowadays. Such attacks are continuously developed to deceive a high number of potential victims. The number of social engineering attacks has risen dramatically in the past few years, causing significant damage both to organisations and to individuals. However, little research has discussed social engineering in the virtual environment of social networks. With the human being repeatedly found to be the weakest link by IS research, the focus being on expansion of training programs and education for online users. Thus, the factors that influence users' vulnerability must be investigated to address this issue and to help in building a profile of vulnerable users. Investigating human aspects in detail is essential in order to reduce people's deficiencies and improve their competencies, which will contribute to enhancing information security management (Soomro, Shah, & Ahmed, 2016). Therefore, research that examines the factors that influence social network users' judgement of social engineering-based attacks is essential if people are to be protected against falling victim to such attacks.

People's vulnerability to cyber-attacks, and particularly to social engineering-based attacks, is not a newly emerging problem. Social engineering issues have been studied in email

environments (Alseadoon, Othman, & Chan, 2015; Halevi, Lewis, & Memon, 2013; Vishwanath, Harrison, & Ng, 2016), organisational environments (Flores, Holm, Nohlberg, & Ekstedt, 2015; Flores, Holm, Svensson, & Ericsson, 2014; Workman, Bommer, & Straub, 2008), and recently in social network environments (Algarni, Xu, & Chan, 2017; Saridakis et al., 2016; Vishwanath, 2015). Yet, the present research argues that the context of these exploits affects peoples' ability to detect them, and that the influences create new characteristics and elements which warrant further investigation. In addition, after analysis of the literature, it became clear that limited research focuses on social engineering in the virtual environment of social networks. Moreover, there is no agreement regarding the users' characteristics that may make them more vulnerable to social engineering on social networks.

Current research goals, the methodology adopted, and the findings aim to fill a substantial gap in information security literature. Cao et al. (2015) have conducted a review of SN-related research between January 2004 and August 2013, which concluded with some recommendations for future research. The first recommendation is to focus on social network research outside the western regions. Secondly, this work emphasised the need to develop SN-specific theories, as social network studies have made limited use of theoretical foundations to justify their findings (Cao, Basoglu, Sheng, & Lowry, 2015). Finally, the research called for more investigation into human characteristics that play a critical role in SN-related studies, and for the adoption by such investigation of a variety of research methods and data analysis techniques. Therefore, the present research attempts to consider all these recommendations.

1.3 Statement of the Problem

Social engineering is a serious problem for information security. Previous research has focused on developing defensive techniques such as training sessions and the use of technical preventive tools to combat this threat. However, those techniques have yet to solve the problem. According to the human-factor report (2018), the number of social engineering attacks that exploit human vulnerabilities dramatically increased over the year examined. While technical defence tools might successfully prevent some types of cyber-attacks, other categories such as social engineering cannot be detected by such tools, especially when humans are the target (Flores et al., 2015).

Additionally, training sessions may not fully address an individual user's needs and weak points in relation to detecting online security threats. An investigation of the social network user's privacy awareness and behaviour calls attention to the need for a personalised education that focuses on end-user needs (Wisniewski, Knijnenburg, & Lipford, 2017).

Therefore, identifying those of the user's characteristics that influence their ability to detect social engineering is essential for developing proper preventative techniques or strategies. Technology-based defensive techniques usually assume that there are no differences between online users, while in fact, users can be classified according to their weaknesses in detecting online threats. This classification will help to assign the right defensive technique or direct appropriate defensive training to potential victims.

Although previous studies have examined some user characteristics and their effects on user vulnerability to social engineering, they did not explore the usefulness of these characteristics in predicting the users' judgement of SE attacks in different contexts, containing varieties of setting, culture, and language. For instance, little research has investigated users' vulnerability to social engineering attacks in Arab countries. The majority of the deception models have been examined in western countries. Thus, there remains a need to discuss and explore their effectiveness in Arab countries where the culture is different. With reference to culture, this study argues that identifying the location of the target of the attack is essential for estimating their vulnerabilities. For example, people who live in developing countries, like Arab countries, may be influenced by different factors that affect their judgement and assessment of SE attacks. However, due to time and funding constraints, the present study examined factors that affect user vulnerabilities in Saudi Arabia, but could not apply the study model to another culture to compare the impact of two different cultures on people's susceptibility to social engineering in social networks.

Additionally, incorporating experts' opinion on determining and confirming users' characteristics that impact on their susceptibility to SE victimisation is a new practice that only limited research has adopted before. This approach could reveal essential and novel aspects of users' ability to detect SE. Experts have also contributed by rating the importance of the influencing factors that have been derived from the literature and included in the UCF.

Therefore, the present study will contribute to existing knowledge in two ways. Firstly, by investigating human vulnerabilities to social engineering attacks in a new environment, namely that of social networks, the challenging and demanding characteristics of which differ from the email environment that has been thoroughly studied before. Secondly, by providing a new conceptual model that relies on user characteristics to predict users' behaviour toward social network deception. This conceptual foundation can open up new insights into professional practices aimed at building robust and personalised countermeasures.

1.4 Research Questions

Protecting social network users from social engineering threats demands identifying the users' characteristics, from multiple perspectives, that make them more susceptible to social engineering victimisation. This would help to build a profile of susceptible users in order to target them by proper advice and training programs. Therefore, the main research question of this thesis is:

"What user characteristics influence user's susceptibility to social engineering victimisation on social networking sites?"

In order to answer the main research question, two steps need to be taken. First, it is important to propose a holistic framework that includes different perspectives of user-related characteristics that may impact user vulnerability to social engineering-based attacks. This step has led to the first research question (RQ1). Second, the identified framework's factors (from the first step) should be empirically tested to examine their effectiveness to predict vulnerable social network users. This essential step has led to the second research question (RQ2).

- **RQ1: What framework can be used as a basis for the user characteristics that influence user susceptibility to social engineering victimisation on social networking sites?**

The first research question (RQ1) is concerned with identifying the user characteristics that would influence the user's judgements of different social engineering attacks on social networking sites. To answer this question, the literature will be reviewed to select relevant theories and frameworks for indicating the appropriate factors to form a UCF. After defining the UCF, an evaluation method needs to be applied to validate this framework. Accordingly, two further sub-questions need to be addressed as follows.

  - RQ1.1: What are the dimensions and attributes of the user characteristics framework that would influence user susceptibility to social engineering on social networking sites?
  - RQ1.2: What is the evaluation method that could be used to validate the proposed user-centric framework?

- **RQ2: How can the selected factors in the user-centric framework be tested in order to indicate whether these factors and dimensions can predict the user's poor judgement of social engineering attacks on social networking sites?**

To answer the second research question (RQ2), a conceptual model will be proposed to represent the hypothesised theoretical linkage between users' characteristics and their

impact on predicting users' susceptibility to social engineering attacks in the context of social networks. Then, an empirical study (scenario-based experiment) will be conducted to test the importance of each factor in predicting users' susceptibility. Thus, another research sub-question must be addressed.

- RQ2.1: To what extent does each of the conceptual model factors predict users' susceptibility to social engineering-based attacks on social networking sites?

The analysis of the results of the empirical study will be used to answer the research sub-question (RQ2.1). If users' vulnerability could be predicted using the proposed model, the present study results could be consolidated in the design of theory and practical recommendations. Additionally, an architecture for a semi-automated security advisory system could be designed, based upon the results of the empirical study.

1.5 Research Objectives

1. To review deception and information security theories and relevant frameworks and models.
2. To identify the dimensions and attributes of users' characteristics that would influence users' judgement of SE attacks on SNSs.
3. To construct and validate a user-centric framework based on different perspectives of users' characteristics.
4. To develop a conceptual model to illustrate the relationships between users' characteristics and users' susceptibility to social engineering victimisation.
5. To empirically test the proposed model to examine the effect of each user characteristic on predicting users' susceptibility to SE on SNSs.
6. To consider how the conclusion could be applied to the benefit of social network users.

1.6 Research Methodology

The present study adopted a sequential exploratory mixed methods design to answer the research questions. Figure 1.1 summarises the research design and process. Using both qualitative and quantitative approaches helps to impart a comprehensive view of the research problem. Therefore, the present research was composed of three main phases.

1.6.1 First Phase: A Mixed Methods Study

In this phase, existing user characteristics frameworks and related theories have been reviewed to facilitate the development of the proposed framework. Based upon this literature study, four varieties of factors have been formulated: (i) Socio-psychological variables, (ii) Habitual variables, (iii) Perceptual variables, and (iv) Socio-emotional variables. The details of such characteristics have been synthesised to produce a UCF. Previous research tends to

rely on parts of these perspectives and, to the best of the researcher's knowledge, has never tried to combine them for a more cohesive understanding of the user's susceptibility, relevant factors and dimensions. Consequently, a mixed-methods experts' review has been used as an approach to validate the proposed framework dimensions and components. By the end of this phase, the first research question (RQ1) and sub-questions (RQ1.1) and (RQ1.2) have been answered.

1.6.2 Second Phase: Measurement Scales Validation

After proposing and validating the UCF, it was mandatory to develop a measurement scale for each factor in the framework in order to examine its impact on user vulnerability to social engineering in the third phase of the current research. Thus, in this phase, various adapted and adopted measures have been used to develop the study instrument. Subsequently, a content validity test was conducted as an approach with which to validate the measurement scales of the study constructs.

1.6.3 Third Phase: A Quantitative Study

This phase includes the development of the conceptual model and conduct of the empirical study to examine the impact of different human-related characteristics on users' susceptibility to social engineering-based attacks on SNSs. To accomplish this goal, a scenario-based experiment has been conducted that engaged 316 participants. This experimental study examined the conceptual model's predictive ability and helped to test the research hypotheses. Additionally, the empirical study makes it possible to examine whether users' vulnerabilities differ across cyber-attack categories in the context of social networks with a focus on classifying social network users based on their vulnerabilities. By the end of this phase, the second research question (RQ2) and sub-question (RQ2.1) have been answered.

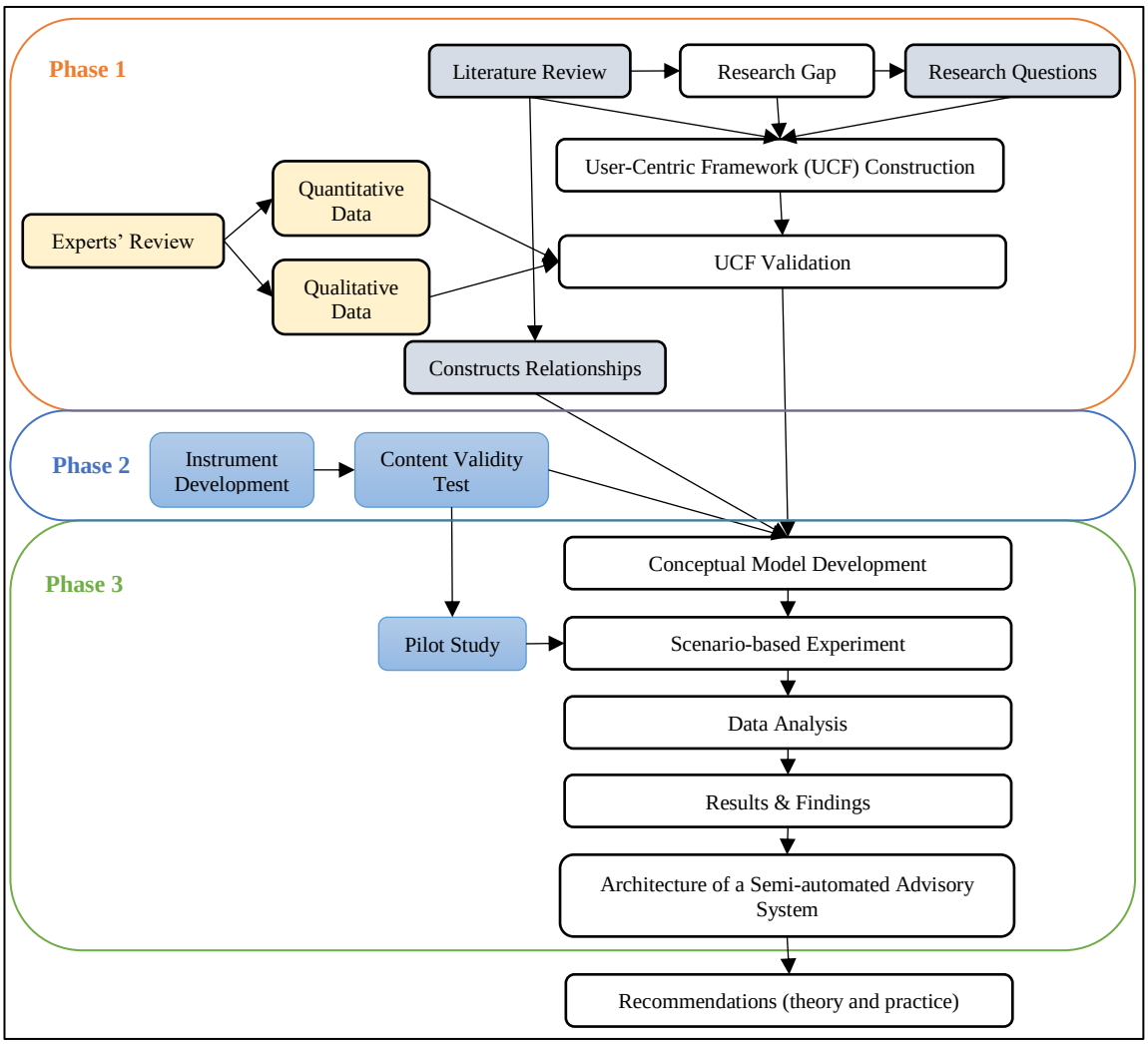


Figure 1.1 Research Design

1.7 Main Contributions

Social engineering is a growing source of information security concern. Exploits appear to evolve, with increasing levels of sophistication, to target multiple victims. Despite increased concern over this risk, there has been little research activity focused upon social engineering in the potentially rich hunting ground of social networks. In this setting, factors that influence users' proficiency in threat detection need to be understood if we are to build a profile of susceptible users, develop proper advice and training programs, and generally help address this issue for those individuals most likely to become targets of social engineering on social networks.

To this end, the present research affords novel theoretical and practical contributions to understanding and predicting human vulnerabilities to social engineering in the social network context. It begins by developing a UCF that includes four user characteristics

dimensions: socio-psychological, habitual, perceptual, and socio-emotional. Previous research tends to rely on selected aspects of these perspectives and has not combined them into a single model for a more cohesive understanding of user susceptibility. Combining multifaceted factors and various theories in one framework to understand human behaviour when encountering online threats represents a critical attempt to understand this serious problem. Incorporating experts' opinions in determining the most influential factors impacting on users' threat detection abilities is a crucial element that should increase the feasibility and efficiency of the proposed framework.

The study develops a conceptual model to test the factors that influence social network users' judgement of social engineering-based attacks in order to identify the weakest points of users' detection behaviour, which also helps to predict vulnerable individuals. Proposing such a novel conceptual model helped in bridging the gap between theory and practice by providing a better understanding of how to predict vulnerable users. The findings of this research indicate that most of the considered user characteristics are factors that influence users' vulnerability either directly or indirectly. Furthermore, the present study provides evidence that individuals' characteristics can identify vulnerable users so that these risks can be considered when designing training and awareness programs.

This research also contributes to the existing knowledge of social engineering on social networks, particularly augmenting the research area of predicting user behaviour toward security threats by proposing a new influencing perspective, the socio-emotional, which has not been satisfactorily reported in the literature before, as a dimension affecting user vulnerability. This new perspective could also be incorporated to investigate user behaviour in several other contexts.

Additionally, the current research aims to gain insight into user competence in detecting security threats in the context of online social networks and investigates the multidimensional space that determines this user competence level. The role of user competence and its dimensions in facilitating the detection of online threats is still a controversial topic in the IS field. The dimensions used to measure the concept are self-efficacy, security awareness, and privacy awareness. The scales used to measure those factors can determine the level of user competence in evaluating risks associated with social network usage. The measurement scales employed here have been validated using an item-categorisation approach that, to our knowledge, has never been used before in IS research. The result of this study provides evidence for the suitability and validity of the user competence dimensions and associated measurement scales. This competence measure could be relevant

in identifying highly and less competent users in relation to security and privacy threats in other contexts.

This study also offers a practical solution that relies on people segmentation and targeting based on users' characteristics and vulnerabilities, in an attempt to help mitigate the problem of users' susceptibility to social engineering. Social networking sites often witness various types of social engineering attacks. Yet, limited research has addressed the most severe types of social engineering on social networks. The present study investigates the extent to which people respond differently to different kinds of attack in a social network context and how we can segment users based on their vulnerability. In turn, this leads to the prospect of a personalised security advisory system. This research attempts to fill a gap in the knowledge, in keeping with Nurse, Creese, Goldsmith, and Lamberts (2011), who emphasised the need to consider personalisation when designing cybersecurity risks countermeasures, as current tools operate on the basis of "one-size-fits-all". The present research finding reveals that people respond to cyber-attacks differently based on their characteristics. For instance, some identified factors such as people's competence, social network experience, and the limited connections with strangers in social networks, could decrease users' likelihood of falling victim to some types of attacks more than to others. Thus, the present research proposes an architecture of a semi-automated advisory system that aims to segment users based on their characteristics and then to target the vulnerabilities of each segment of users by sending the package of advice that they need.

1.8 Research Scope, Context, and Limitation

Individuals and organisations are becoming increasingly dependent on working with computers, accessing the Internet, and more importantly sharing data through virtual communications. This makes cybersecurity one of today's most significant issues. Protecting people and organisations from being targeted by cybercriminals is becoming a priority for industry and academia (Gupta, Arachchilage, & Psannis, 2018). This is due to the substantial damage that may result from losing valuable data and documents in such attacks. When investigating social engineering-based attacks, it is essential to consider four main entities: the context (email, social network, or SMS), the attacker (human or software), the attack type (direct or indirect), and the victim (individual or organisation). The present study focuses on the social engineering attacks that target individual users in the social network context, particularly Facebook, as it is difficult to study different networks due to time and funding constraints. Furthermore, this study focuses only on the impact of the characteristics of the

receivers of the attack on their response to different types of social engineering-based attacks that could target social network users, without consideration of the type of attributes of either the attacker or the message of the attack.

However, when investigating human behaviour in relation to online threats, it is essential to focus on the interaction between the individual's attributes, his/her current context, and the message persuasion tactic (Williams, Beardmore, & Joinson, 2017). Most previous studies that have considered persuasion tactics in social engineering exploits have focused on phishing as the typical form of cyber-attack, while limited research has investigated other categories, such as malware or clickjacking. Therefore, the present study argues that people's vulnerabilities change depending upon the type of cyber-attack. This investigation, accordingly, addresses the human characteristics associated with victimisation for a range of cyber-attacks, which facilitates the design of a semi-automated security advisory system that relies on the idea of people segmentation and targeting.

This study focuses on Saudi Arabia due to its regional importance in the Middle East and its unique social values and religious beliefs. As previous studies have revealed that the younger population is more vulnerable to online threats (Algarni et al., 2017; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010), Saudi Arabia was a suitable context for the present study, with young people being in the majority: 39% of the population are aged under 20, and 59% are aged under 30 (General Authority for Statistics, 2016). Saudi Arabia has witnessed continual rapid development and growth in many aspects in recent years, especially after the Saudi government's initiation of the "2030" vision. This vision is described as "providing the Kingdom with the directions, commitment, goals, and objectives to achieve its identified aspirations and define itself nationally, regionally, and globally" (Mitchell & Alfuraih, 2018). The three main pillars of this vision are a vibrant society, a thriving economy, and an ambitious nation (Vision 2030, 2016). Each of these pillars involves short-term and long-term strategic objectives that the country plans to achieve by 2030 through the cooperation of public, private, and non-profit sectors.

According to an online statistics portal, Statista (2019), Saudi Arabian users on Facebook have rapidly increased from 14.3 million in 2018 to an expected 16.8 million by 2023. However, Saudi Arabia is among the countries with the highest percentage of economic crime; as stated in the Global Economic Crime Survey (2016), the crime rate has more than doubled from 11% in 2014 to 24% in 2016. Saudi Arabia is one of the few Arab countries that experience frequent cyber-attacks targeting government institutions. For instance, recent cyber-attacks have affected Saudi Aramco, the biggest oil company in the region (Bronk &

Tikk-Ringas, 2013). Since these incidents, many of the problems associated with dealing with cyber-attack threats have come to the fore. Thus, the present research aims to understand why Saudi users easily fall victim to cyber-attacks, in order to contribute to the mitigation of such threats.

Another limitation concerns the selected samples of participants. The population sample, especially in the third quantitative study, is mainly derived from Saudi Arabia, which limits participation to a specific culture and religion. However, the research process is mostly constrained by time and funding limitations, which justify focusing on a particular sample of the population. Nevertheless, to reduce the impact of this limitation, samples in the current research include various genders, ages, education levels, and types of expertise. The limitations of each phase of the current research are considered further in chapter 10.

1.9 Thesis Structure

This thesis is organised as follows. Chapter 2 includes a review of the relevant literature. Chapter 3 provides details of the methodology that has been adopted in the present research. Chapters 4 and 5 concentrate on the first phase of the current research, which focused on the construction and validation of the user-centric framework. The method and the steps followed to build the proposed user-centric framework are described in chapter 4. Following this, the approach used to validate the proposed user-centric framework, and the results of the validation, are discussed together with the findings in chapter 5. Chapter 6 presents the results of the second phase, which concentrates on development of the instrument and validation of the measurement scales of the study constructs.

Chapter 7 and chapter 8 concentrate on the third phase of the present research, which focused on the development and evaluation of the conceptual model. Chapter 7 describes the procedure that has been followed to build the study hypotheses and the conceptual model. Chapter 8 analyses the collected data of the scenario-based experiment and presents the empirical study results that aim to evaluate the conceptual model constructs and their hypothesised relationships. Chapter 9 provides the outline for a semi-automated advisory system that could be developed based upon the empirical study results. Finally, the thesis concludes with chapter 10, which provides a discussion of the theoretical and practical implications of the findings in this work.

Chapter 2. LITERATURE REVIEW

2.1 Overview

This chapter presents a review of the relevant literature related to the research problem and topic. Diverse concepts are explored in Section 2.2 which are related to the social engineering security issue. Furthermore, Section 2.3 includes a discussion of the antecedents and consequences of failing to detect social engineering-based attacks within the channel of social networks. Different proposed solutions to prevent the success of social engineering-based attacks will be presented and discussed in Section 2.4.

The importance of identifying vulnerable individuals based on their characteristics is also elaborated in Section 2.5. Following this, a general taxonomy of social engineering attacks in social networks is presented in Section 2.6. Section 2.7 in this chapter sheds light on the gap of theory and knowledge in this area, especially in identifying the characteristics that make users more or less vulnerable to cyber-attacks victimisation (Section 2.8). Finally. Section 2.9 provides a summary of this chapter.

2.2 Social Engineering Security Threats

Social engineering (SE) is a persistent threat that has emerged from traditional communication security threats to become a major online security issue. The term 'social engineering' was first used in the political field before being adopted within cybersecurity research (Hatfield, 2018). The term has been defined in the information security (IS) field as "The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" (Mouton, Leenen, Malan, & Venter, 2014). Social engineers exploit individuals' motives, habits, and behaviour to manipulate their victims (Mitnick & Simon, 2003). Traditionally, social engineers rely on physical deception techniques such as dumpster diving or shoulder surfing to reach their victims (Peltier, 2006), while, with the invention of the world wide web, social engineering techniques have made the transition and started to reach a massive number of victims at the same time. This section will explain social engineering techniques and offer a brief description of areas that have been affected by this security threat.

When online security threats are under study, the context of the investigation plays a critical role. Most social engineering research is focused on three contexts of threats which are organisations' information technology and systems, traditional communication channels such as the email environment, and modern communication channels, such as social networks. The following will summarise the relevant literature based on these three contexts.

2.2.1 Social Engineering as a Threat to Organisations

Due to their financial and economic positions, organisations have been the focus of social engineers for many years. Social engineers have great success when using traditional techniques such as face-to-face, dumpster diving, shoulder surfing, and voice phishing (Peltier, 2006). However, the information technology era has changed peoples' work and life extensively as it contributes to making the work cycle more effective and easier day by day. This makes it necessary for social engineers to adapt their techniques to cope with this revolution. Using information technology could not provide assurance to people that all their information will be kept safe as there are other aspects associated with this environment that couldn't be controlled such as human-related errors.

Within organisations, the insider threat is considered one of the biggest security issues. In this threat, the human element is included in violating access policies with either a malicious intention to steal sensitive information or even with unintentional actions that could be exploited by cybercriminals (Greitzer et al., 2014). In this context, Khlobystova, Abramov, and Tulupyev (2019) proposed an approach to distribute access rights to critical documents among employees which in turn could facilitate identifying the most critical paths of social engineering attacks. Yet, employees are also part of the prevention of such threats if they comply fully with the organisation's security policies (which will be discussed further in Section 2.4.2).

One of the first information security researchers who investigated social engineering based attacks in an organisational context was Workman (2008b). Workman used grounded theory to investigate why employees fall victim to social engineering threats. In subsequent work, Workman (2008a) conducted a field study to explore user's behaviour toward SE attacks by sending a phishing email, to examine the effects of two of Cialdini's (2001) persuasion principles (authority and commitment). The experiment's result shows that threat assessment, commitment, trust, and obedience to authority were significant variables in maximising the success of social engineering tactics (Workman, 2008a).

Flore et al. (2014) have also focused on social engineering victimisation in an organisational context and investigated factors that cause employees to comply with phishing requests by conducting two experiments, scenario-based and actual phishing experiments. The result of their scenario-based survey revealed that computer knowledge at work, desire to help other people, and gender have a significant impact on the likelihood of attack success. Their actual phishing experiment found that adding information about the targeted victim in the phishing email increased the success rate of the attack and also indicated that individual's trust as well as their risk perception correlated with employee response to the actual phishing attack. Their study concluded with a recommendation that organisations should balance between the benefits of making enterprise-specific information - such as employees' names and email addresses - publicly available, and the risk associated with such a practice. Since this accessible information could be used by cybercriminals to design personalised phishing emails.

2.2.2 Social Engineering as a Threat to Traditional Communication Channels

Social engineering attacks have moved from being a traditional threat that could happen in physical space, such as gaining access to a particular office (Bullée, Montoya, Pieters, Junger, & Hartel, 2015), to a more enduring threat that targets online services. Social engineers started to use the internet to gain credential information by designing fake and malicious websites. Therefore, assessing and enhancing peoples' ability to detect malicious websites is another important area in tackling the social engineering problem. Despite this, research has found that, when they encounter phishing websites, users give less attention to browser security indicators than the content of the websites (Alsharnouby, Alaca, & Chiasson, 2015).

In order to increase the spread of their malicious websites, offenders found email services to be the perfect tool to serve their goal. Email communications are essential for all organisations and the individual's working cycle. Launching cybersecurity attacks in an email environment have shown high success rates over the past few years because exploiting one email in a company is sufficient to spread the phishing attacks to other employees, even to those working in high and critical positions (Heartfield & Loukas, 2015; Vishwanath et al., 2016).

Phishing attacks are the most commonly investigated types of cyber-attack in IS research. Three important elements have been investigated as having an influence on phishing email success. Firstly, the title of the malicious email is usually chosen very carefully in order to generate a persuasive subject for the email as this may induce the receiver to open the

message (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Secondly, the content of the email plays an important role. Designing professional looking emails and taking care of the general layout of the message can make a significant difference (Alsharnouby et al., 2015). Thirdly, the individual characteristics of the receiver of the email could increase the success of the phishing attacks as research shows that demographics, such as the age and gender of the receiver, could affect their susceptibility to email phishing (Alseadoon et al., 2015; Iuga et al., 2016).

Including personal information in the email content has also been claimed to increase the response rate (Bullee, Montoya, Junger, & Hartel, 2017). In email phishing, it is important that the content of the message is personalised to increase the deception effect. An experiment conducted on 593 employees found that 19% provided their personally identifiable information when they received a general phishing email while 29% provided their personally identifiable information in response to a personalised spear-phishing email (Bullee et al., 2017).

2.2.3 Social Engineering as a Threat to Modern Communication Channels

Recently, modern communication mediums such as mobile applications, instant messages, and social network platforms have been exploited by cybercriminals to disseminate their malicious activities. Social network websites are attracting billions of users to use their services. These networks offer a variety of attractive communication tools that make users more connected with their friends or other people who share the same interests. Yet, despite their many advantages, there is some risk associated with using social networks. The large amount of data makes social networks more exposed to privacy intrusion and security risk (Mansour, 2016).

Service providers of modern communication channels tend to use out-of-band authentication methods as an extra layer in their security mechanism (Fire, Goldschmidt, & Elovici, 2014). In out-of-band authentication methods, when users want to enter their accounts, they receive a verification code via their mobile phones or email. Entering this verification code is mandatory to gain access to their account. This authentication technique is considered beneficial to protect against unauthorised access, and it has been adopted by many companies in the financial and banking sectors, especially where high-risk operations are undertaken such as large currency transactions (Siadati, Nguyen, Gupta, Jakobsson, & Memon, 2017). However, social engineers recently developed sophisticated deception attacks called Verification Code Forwarding Attacks (VCFA) to defeat this layer of authentication. This sophisticated attack relies on human deception to get hold of these verification codes. An

investigation of such attacks on SMS-based 2-factor authentication indicated that around 50% of targeted individuals had been tricked into sending their verification code to the attacker (Siadati et al., 2017).

Hackers and offenders are also using social networks to reach their victims as an increasing number of organisations establish social network accounts due to their huge popularity. There are different types of security threats associated with using social networks. People can face different security risks from the amount of information they share in the network, as this information can directly or indirectly reveal sensitive information about individuals and make them more exposed to cybercriminals. The next section will explore social engineering threats in social networks context in more detail.

2.3 Social Engineering in Social Networks

Using social networking sites has both positive and negative consequences for individuals and organisations. From an organisational perspective, using social networks at work for utilitarian and hedonic purposes have been found to maximise employee work performance (Leftheriotis & Giannakos, 2014). However, there are many security issues in social network environments that can be classified into four categories, as privacy issues, viral marketing, network structural-based attacks, and malware attacks (Gao, Hu, Huang, Wang, & Chen, 2011). This section will focus on the social engineering security threat in the context of social networks. Furthermore, this section provides an overview of the most common types of social engineering attacks in social networks.

Social engineering attacks have previously been studied in traditional contexts such as email, face to face, and by telephone calls. A famous model of the social engineering cycle was proposed by Mitnick and Simon (2003). Research, developing rapport and trust, exploiting the trust, and utilising information are the four main steps that are reflected in every social engineering attack according to this model.

Nowadays, social engineers have moved their attacks to the new rich context of social networks. The number of social network users has dramatically increased to billions in recent years. This large number of users, who are interacting and generating information, seems to attract offenders and criminals to use those networks to exploit user vulnerabilities. Human frailty poses a threat to information security as most of the worst breaches caused by human error (Proofpoint, 2018). Mulligan and Schneider (2011) pointed out that it is hard to achieve absolute cybersecurity, especially in a context of human users. In a social network context, the

structure of social engineering-based attacks is slightly different when compared to traditional contexts. This aspect is discussed in the next sub-section.

2.3.1 Main Entities in Social Engineering Attacks

According to the routine activity theory, proposed by Cohen and Felson (1979), changes in the pattern of routine activity could influence the incidence of crime significantly. There are three main entities associated with conducting criminal acts, as shown in Figure 2.1. These entities, the existence of likely offenders, lack of guardianship, and presence of suitable targets, would considerably contribute to an increase in crime. Yet, if one of these three entities is missing, this could prevent crimes from being committed.

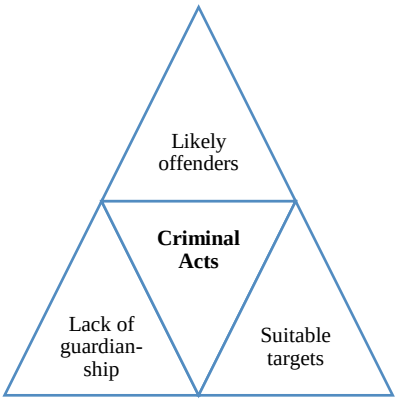


Figure 2.1 Three Main Entities of Routine Activity Theory (Cohen & Felson, 1979)

The deception message is also considered important to increase the attack success rate. Heuristic-Systematic model has been proposed by social psychology researchers to explain human attitudes and information processing in relation to received messages that include persuasion (Chaiken, Liberman, & Eagly, 1989). This model has been applied in different fields and contexts such as communication risk-related behaviours (Griffin, Neuwirth, Giese, & Dunwoody, 2002), and the influence of online customer reviews in e-commerce (Zhang, Zhao, Cheung, & Lee, 2014). Recently, social engineering researchers have utilised this model to explain email phishing victimisation (Luo, Zhang, Burd, & Seazzu, 2013; Vishwanath et al., 2016). According to this model, when the user receives the persuasive message, they would start validating the message content by two different information processing modes. First, Heuristic processing, which is the process of quickly assessing the validity of a message based on the cues or factors that are shown in the message, such as message subject, or message source; second, Systematic processing, which is the process of strictly assessing the validity of the message by conducting proper research on the message content.

The review of the literature on social engineering attacks in the context of social networks revealed a structure for social engineering attacks (Algarni, Xu, Taizan Chan, & Yu-Chu Tian, 2013). Three main actors play critical roles in this structure, i.e., attacker, context, and victim. Each of these has its own dimensions and attributes which will be discussed in more details in the following.

2.3.1.1 The Role of the Attacker

Social engineers usually could not reach their goal by hacking a system but rather by using deception methods to persuade the target to permit access. Persuasion techniques such as Cialdini's (2001) principles of influence have been widely discussed in security research as to significantly influence human behaviour. Attackers found it easier to use a variety of methods to convince people to accept the trick rather than breaking the security countermeasures. Figure 2.2 summarises the process that the attacker goes through to conduct a successful social engineering attack in social networks.

Social engineers always start their attack by choosing the victim. This step is very important to increase the chance of success. The social engineers rely on user characteristics to choose the best target which is easily deceived. Then, the attacker will gather as much information as possible about the victim, either from the victim's social network account if the account is public, from search engines, or sources such as other online platforms that belong to the victim. After that, based on the collected data, the best persuasion technique will be chosen. For example, if the target likes online shopping, the attacker can offer a shopping discount or coupon if the victim clicks on a link to register at a specific site. According to interpersonal deception theory, which has been proposed by Buller and Burgoon (1996), the deceiver uses three different strategies to foster the target in a conversational context. Firstly, falsification, where the deceiver attempts to lure the target by telling a lie. Secondly, concealment, where the deceiver attempts to lure the target by hiding the truth or part of it. Finally, equivocation, where the deceiver attempts to lure the target by intentionally being obscure or intentionally changing or obscuring the truth.

After choosing a persuasion strategy, the attacker will choose an attack technique which can be either direct or indirect. Direct attack techniques use social networking sites to communicate with the victim and conduct the attack. Indirect attack techniques use social networking sites to gather the victim's personal information in order to facilitate attacks in other SE contexts, such as email, telephone, or face to face. Finally, conducting the attack in social network contexts usually goes through various phases based on the network's environment. For example, on Facebook, there are two phases in conducting the SE attack

(Vishwanath et al., 2011). The first phase is sending a friendship request. Since the target privacy setting may otherwise prevent receipt of any message from non-friends, the attacker would be unable to send the lure message or post to the target. If the first attack stage has been successful, then the second phase will start, which includes sending the lure.

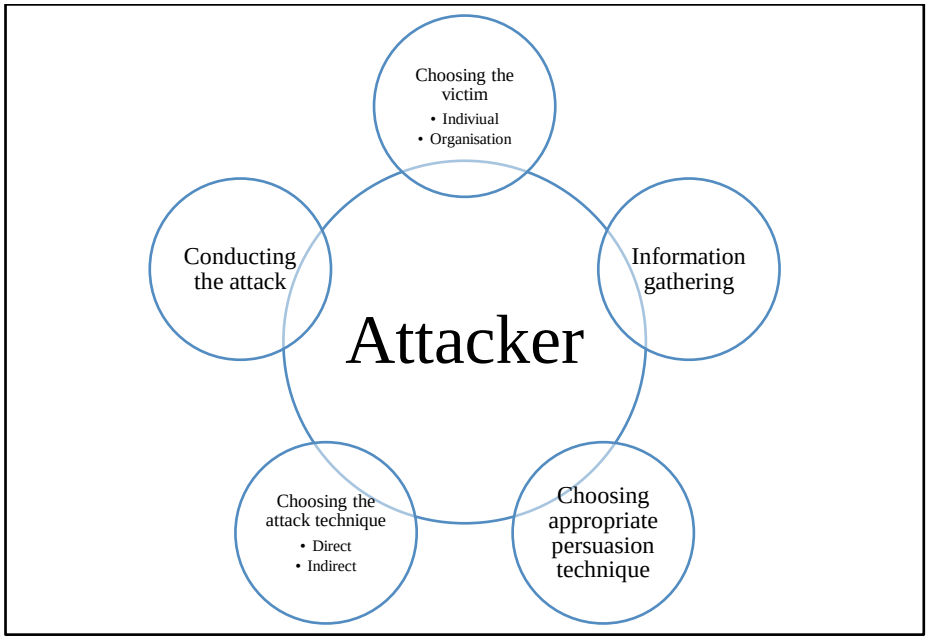


Figure 2.2 Social Engineering Attack Phases in Social Networks

2.3.1.2 The Role of the Context

Context plays a critical role in the attack because it will define the complexity of the exploit, especially for the attacker. Privacy and security settings are important features for user protection. For example, if the user changes the privacy setting of his/her account to be private, the attacker cannot use the account to gather the user's information. However, Research have indicated serious flaws and concerns over social networks privacy and security settings (Madden, 2012; Madejski & Bellovin, 2011).

When comparing people expectation of Facebook privacy settings and their actual settings, the majority of Facebook users reported to be unaware of the implication of their account privacy settings (Liu, Gummadi, Krishnamurthy, & Mislove, 2011). This might be partially because 48% of social network users seem to find difficulty in managing their profile's privacy control settings (Madden, 2012). Providers should enhance the privacy and security mechanisms in their networks by adopting advanced and practical authentication mechanisms and enforcing strict information sharing and accessing policies (Saridakis et al., 2016).

2.3.1.3 The Role of the Victim

The target of the attack is always responsible for evaluating and recognising the attack in order to prevent it from succeeding. Many theories attempt to explain the cognitive process that the user goes through to evaluate the received messages. One of these theories is the model of deception detection proposed by Johnson et al. (2001). This model explains the cognitive processes that the targeted individual adopts in order to interpret the received information. According to this model, detecting a threat consists of four processes: activation process, hypothesis generation process, hypothesis evaluation process, and global assessment process. In contrast, interpersonal deception theory, which was discussed earlier, focusses on the effect of the communication between the receiver and the deceiver.

The theory of deception defined detection as a cognitive process that focuses on several cues that could identify a suspicious message or behaviour, such as interpreting the voice tone of the caller or identifying spelling errors in the message (Alseadoon et al., 2015). According to this theory, detecting the deception occurs when comparing the observed and the expected cues (Grazioli, 2004). Moreover, this theory mainly relies on the level of information richness in the domain (Alseadoon et al., 2015; Tsikerdekis & Zeadally, 2014). For example, if the deception occurs in a domain that involves face to face communication, rich cues such as direct response, facial expression, and voice tone can be examined by people to detect the deception. For this reason, this theory is often applied in such rich communication contexts.

Grazioli (2004) has extended the deception detection model to fit lean communication mediums such as the email environment in order to understand why people succeed or fail to recognise online deception attempts. Alseadoon et al. (2015) and Vishwanath et al. (2011) are among a few researchers who have utilised the model of deception detection to investigate social engineering victimisation.

Another theory that has been found relevant and adopted by IS researchers when investigating user vulnerabilities to email phishing is the Elaboration Likelihood theory (Vishwanath et al., 2011; Workman, 2008b). Petty and Cacioppo (1986) proposed the Elaboration Likelihood Model to describe the dual processing of a persuasive message that explains attitude changes toward that message. The model has two persuasion processing modes: central and peripheral routes. In the central route, the attitude change will be based on the strength of the argument which involves more cognitive effort. While in the peripheral route, the attitude change will consider source/message factors, such as source credibility, as cues to judge the persuasive message.

Source credibility has been found to impact user judgement of social engineering attacks in Facebook (Algarni et al., 2017). Four dimensions of source credibility have been identified as influencing peoples' behaviour toward deception requests. These are perceived source sincerity, perceived source competence, perceived source attractiveness, and perceived worthiness of the source.

Different types of user characteristics determine user ability to detect the attack. Demographic variables, personality traits, and expertise are among many factors that authors claim have an effect on peoples' detection ability (Algarni et al., 2017; Alseadoon et al., 2015; Saridakis et al., 2016; Vishwanath et al., 2011). Previous research has given socio-psychological variables major attention when investigating peoples' resistance and vulnerability to social engineering while limited consideration was given to other user-related characteristics and perspectives, such as perceptual, habitual, and emotional factors. The present study will focus on investigating the receiver characteristics that make the end-user more vulnerable to social engineering attacks. This will be discussed in more detail in Section 2.5.

2.3.2 Social Networking Sites as a Source for Social Engineering

Social Networking Sites (SNSs) are considered as a major resource for social engineering. SNSs are developed day after day to encourage people to engage more with others and to disclose more private information. The major security threats in online social networks have been categorised into four groups by Fire et al. (2014). The first group is classic threats which includes threats that can occur in other Internet contexts and not only in social network environments, such as malware, and phishing attacks. The second group is characterised as modern threats and includes threats that exclusively occur in the social network context, such as clickjacking, and identity cloning attacks. The third group is combination threats which includes overlapping and integrating different strategies to conduct a sophisticated attack. Finally, the fourth group consists of threats that target children in social networks, such as cyberbullying. Clearly, most examples in these different groups of social network threats are closely linked and would all be considered types of social engineering threat.

Attackers might use SNSs to target their victims or use it to acquire victims' personal information to gain victims' trust in other SE attacks. Figure 2.3 shows that SNSs can be used as a direct source or indirect source for social engineering attacks. However, it is hard to include all types of possible attacks in this section as criminals are always evolving new methods and techniques to conduct their offensive actions. A brief summary of the most

common types of social engineering threat that may occur in social networks will be covered in this section.

2.3.2.1 Direct Source to Social Engineering

Social networks could be considered a direct source of SE attack when cybercriminals use social networking sites to communicate with the victim and conduct the attack. The following is a list of the most common methods of direct SE attacks.

Identity cloning attack. Attackers take advantage of the number of different SNSs available online and the idea that users tend to have accounts in several. The attacker can find through search engines the social networking sites that the victim has not registered in yet and open an account in the victim's name. Then the attacker can collect the victim's friend's information from the victim's real profiles in other SNSs and thereby easily deceive the victim friends by sending friendship requests (Bilge, Strufe, Balzarotti, & Kirda, 2009). This attack is considered a persistent threat that targets social networks (Sahoo & Gupta, 2019).

Using direct messages. Social networking sites usually provide instant messages as a feature to their users. However, research revealed that social engineers could conduct successful attacks using social network chat services as a contact method to request sensitive information or send malicious links (Bossetta, 2018).

Reverse attack. The attacker can abuse the friend-finding features in SNSs to trick the victims by persuading them to initiate the friendship. The victims will show a high degree of trust to the attacker as they are the ones who request the friendship (Irani et al., 2011). Hatfield (2018) has described this type of attack as being severe and effective.

Social spamming. Spammers try to gain creditability by opening fake accounts on SNSs. Fake accounts start to maintain social relationships with legitimate users and will reduce their detection and help them to carry out successful spam activities (Fu, Feng, Guo, & Li, 2018).

ASE botnet attack. This type of attack is an automated social engineering exploit whereby cybercriminals use software to conduct the attack after identifying initial parameters such as Facebook account information and victim details, such as the name of the organisation or the characteristics of the required victims. The software can then execute the attack through chat features by sending links (Huber, Kowalski, Nohlberg, & Tjoa, 2009), or steal personal information (Ferrara, Varol, Davis, Menczer, & Flammini, 2016).

2.3.2.2 Indirect Source to Social Engineering

Social networks may also be considered as an indirect source of SE attack when cybercriminals employ social networking sites to find victim's personal information in order to use this as input to an attack in another context, such as email, telephone, or face to face.

Phishing attack. Attackers may target the victim's accounts in SNSs and collect valuable data from these accounts by reading their walls or tweets or by knowing the victim's friends. They can acquire the victim's email address, work location, hobbies, and favourite places. By possessing this information, the attacker can manipulate the victim in a bid to harvest more sensitive information, such as bank account, username, and passwords, by conducting a phishing email (Binks, 2019).

Spear phishing. Cybercriminals use information, such as shopping history and banking institutions, taken from the victim's social networking sites to facilitate gaining the victim's trust (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Cybercriminals use such collected information to design an effective personalised trick (Bullee et al., 2017).

Data and information leakage. It is common among social network users to share their locations or holidays with friends or even the public. Tweeting, for instance, with geolocation turned on, could reveal private information that could lead to identifying other social network accounts that belong to a particular subject (Gan & Jenkins, 2015). Additionally, the leakage of key information such as a person's location could induce burglaries as the shared information indicates an empty property (Gan & Jenkins, 2015).

Automatic data harvesting. Employees' personal information may also be determined by tracking their online footprints in social networking sites (Shindarev et al., 2018). Employee profiles can be easily distinguished in an automated way from the online footprint of the organisation, such as their public website, and Twitter account (Edwards et al., 2017). This also facilitates linking employees' profiles across multiple social network channels and can aid successful SE attacks on their organisation.

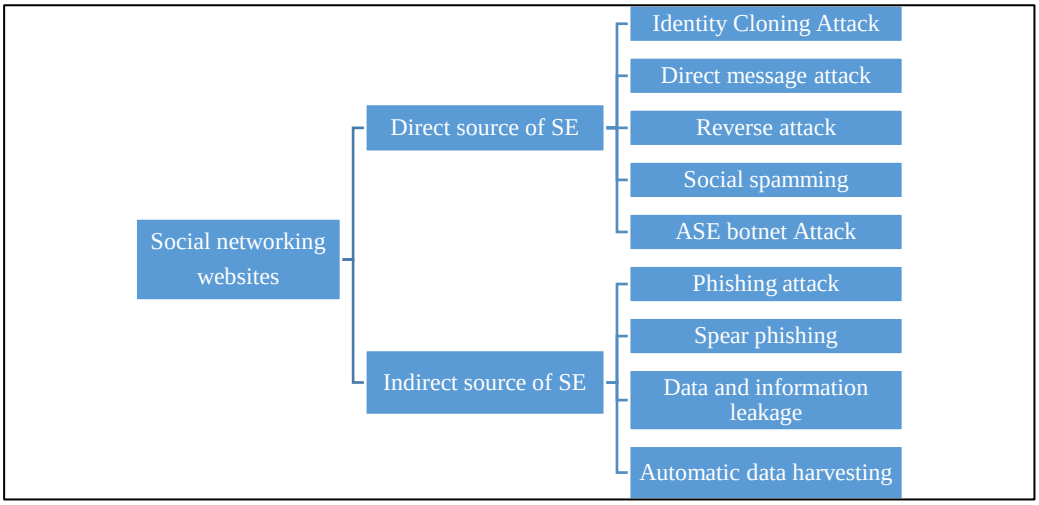


Figure 2.3 Social Networks as a Direct and Indirect Source of SE

2.3.3 The Impact of Social Engineering

Social engineering attacks are a serious threat to social network users and might subject people to different kinds of harm. Manipulation attacks could affect the market through providing fake information such as bogus ratings and reviews, to persuade people to buy (or not buy) certain products. The impact of such attacks has progressed from stealing sensitive information and spreading misleading information to political discourse penetration and financial market manipulation (Ferrara et al., 2016). For example, social engineering attacks have been found to serve commercial or political goals by targeting company reputations (Messias, Schmidt, Oliveira, & Benevenuto, 2013).

It is widely agreed that social engineering attacks cause vast damage to governments, organisations, and individuals. The cost of such attacks can vary and include direct costs, indirect costs and defence costs (Anderson et al., 2013). Yet, estimating security-related costs is hard to achieve, as indicated in the Hyman (2013) report. The first reason is that many organisations fail to report security incidents so as to protect their reputation or because of the lack of trust on how these data of the estimated damage will be treated. The reported figures might also suffer from selection bias as organisations who reported their statistics to cybercrime surveys might not have faced a huge security penetration. Furthermore, there is no existing fixed standard on how to measure security costs across organisations, and this makes comparisons between them unreliable. Some organisations may not be aware that social engineering attacks had victimised them and this contributes to the difficulty of calculating the breach-related cost in those organisations.

Furthermore, Thomas et al. (2013) point out that the cost of a security breach includes intangibles such as loss of reputation. Misestimating is another problem as indirect or future

effects of security breaches are usually not realised or ignored. Furthermore, conflicts of interest among stakeholders is a critical problem to estimate the impact of social engineering attacks. For instance, customers highly value a data privacy leakage while organisations give loss of resources greater priority. Therefore, detecting and combating social engineering attacks in social networks is an important research area that could help preserve network systems as well as our society from a range of dangerous threats.

2.4 Protection against Social Engineering Threats

Various efforts have been made to protect individuals and organisations from cybersecurity attacks. While most researchers agree that social engineering threats cannot be eliminated yet, they can be reduced (Fan, Lwakatare, & Rong, 2017). Many proposed security mechanisms and techniques are available in the literature while more are still in development in the face of still-evolving security threats. This section will summarise and categorise these protection mechanisms.

2.4.1 Countermeasures in Social Networks Context

Most of the countermeasures that have been proposed to combat different social engineering attacks are focused on investigation approaches and strategies to detect either the criminal, the context vulnerabilities, or the victim's vulnerabilities.

2.4.1.1 Detecting the Criminal

A taxonomy of features that facilitate detecting malicious accounts in social networks has been proposed by Adewole, Anuar, Kamsin, Varathan, and Razak (2017). Various means have been proposed to distinguish malicious accounts and legitimate accounts, especially in the area of research that focuses on spamming and social-bot attacks**.** These attempts could be divided into three categories: detection based on leveraging the social graph, detection based on blacklists comparison approach, and detection based on using a machine learning approach.

2.4.1.1.1 Detection Based on Leveraging the Social Graph

The social ties among social network users provide rich information that can be used to increase the accuracy of malicious accounts detection. In this approach, the analysis of social networks is based on two major components which are users (referred to as nodes) and the connections among users (edges). Legitimate accounts usually have more connection with trusted accounts which minimise the likelihood of being malicious.

Some studies have focused on analysing the social network structures to identify the malicious community in order to detect spam accounts (Liu, Mei, Chen, Lu, & Du, 2015), or

fake accounts (Viswanath, Post, Gummadi, & Mislove, 2010). These studies rely on dividing social network users into groups based on their community similarity which facilitates identifying the malicious community. Yet, imitating the way legitimate users built their communities can prevent the identification of malicious communities. A further limitation of using graph-based detection is dealing with large network graphs might require very complex computation. Therefore, in-depth investigation of accounts inner and outer relationships in social networks can provide a decent prediction of malicious account (Yang, Harkreader, Zhang, Shin, & Gu, 2012).

2.4.1.1.2 Detection Based on Blacklist Filters

Most social engineering attacks in social networks context include URL. Some research tends to analyse the content of social network posts to identify malicious posts by comparing the URL or domain used in the posts with those classified as malicious in public or domain blacklist APIs.

Grier, Thomas, Paxson, and Zhang (2010) indicated that only 8% among 25 million URL shared on Twitter found to be categorised as malicious in popular blacklists. Another major issue with using blacklist methods is that long time is needed for a link to be classified as malicious and included in the blacklist with a report of 90% of users accessing a page before it is blacklisted (Grier et al., 2010).

Furthermore, short URLs have been widely used in social media posts and messages. This kind of links has risen security concerns recently as it has been used to cover malicious links. Yet, several attempts (e.g., Gupta, Aggarwal, & Kumaraguru, 2014; Nikiforakis et al., 2014) have been proposed to deal with this kind of threats.

2.4.1.1.3 Detection Based on Using a Machine Learning Approach

Using artificial intelligence and machine learning techniques to identify and detect cybercriminals or malicious activities in various social engineering contexts such as email (Islam & Abawajy, 2013), websites (Lakshmi & Vijaya, 2012), online social networks (Fu et al., 2018) has shown noticeable success and provides promising results. Therefore, this trend and promising approaches have gained popularity among researchers. To distinguish malicious users from legitimate users, researchers used various machine learning techniques such as supervised, unsupervised, semi-supervised approaches.

Abulaish and Bhat (2015) used topological and community-based social network features to detect spammers in online social networks by adopting various ensemble learning approaches such as bagging and boosting. Their empirical results indicated that the

performance of spammer detection when using bagging ensemble learning approach via J48 (decision tree) classifier is better than the performance of other ensemble learning approaches. Yet, social network structural and content features are also important to be included to increase the performance and accuracy of the classification process. A high success rate has been claimed when using supervised machine learning algorithm specifically Support Vector Machines to detect spammers after extracting a set of features from the users' social behaviour as well as from the generated contents (Zheng, Zeng, Chen, Yu, & Rong, 2015). However, most of previous detection approaches ignores temporal characteristics and only rely on static data and features that have been extracted at a single time point from the social network to conduct the classification which make the effectiveness of these strategies to be reduced with the evolution of users' behaviour and activities (Fu et al., 2018).

Some research has noticed the benefit of integrating supervised and unsupervised approaches to increase the reliability and accuracy of the detection performance. For instance, integrating message content and user behaviour together with some social relation information have also been proved effective to identify spammers in online social networks using a novel framework that is based on semi-supervised learning approaches such as constrained non-negative matrix factorization algorithm (Yu, Chen, Jiang, Fu, & Qin, 2017). A recent study (Fu et al., 2018) considered users temporal evolution patterns to distinguish between spammers and legitimate users and proposed a framework that is designed based on the integration of supervised and unsupervised techniques to detect spammers accounts. This approach relies on measuring the change in users' behaviour patterns which make it an effective means to combat the rapid evolving spamming strategies.

However, using classification tools usually focus on extracting behaviour-based features with a limited focus on other critical network data such as the relationship ties among users. These relationships information could increase the accuracy of identifying malicious accounts as those criminal accounts tend to connect with each other to make a small social network (Yang et al., 2012).

2.4.1.2 Detecting the Context Vulnerabilities

Social networks providers and commercial companies could contribute to the solution of preventing social engineering threats by different means. Islam et al. (2017) have investigated the limitations of current social network privacy control systems and recommended constructing new user-focused privacy features that give social network users the ability to control and protect their contents.

Enhancing social network's access policies has been a focus of research to protect people private data from being exploited by criminals. Carminati et al. (2009) are among the first researchers who propose a relationship-based access control mechanism. In their model, three factors have been used to assess the relationship between the information requester and the owner which are the relationship type, depth and trust level. In order for the requester to grant access over a resource, proof of authorisation must be provided.

Disclosing private and sensitive information to the public without enforcing privacy restriction means is considered risky behaviour among social network users. Some users are aware of that risk, yet, have no authority to manage their private information when published by other users such as time, place, and pictures of people attending an event. People have conflict opinion and preferences regarding quantifying privacy which increase the challenge of solving this dilemma. Some research proposed manual techniques that include users' interventions to resolve the conflict (Wishart, Corapi, Marinovic, & Sloman, 2010). While others arise automatic approaches that use agents to take the user role in the privacy negotiations (Mester, Kökciyan, & Yolum, 2015; Such & Rovatsos, 2016).

Other research relies on a voting aggregation method among the information co-owned parties. For instance, Hu, Ahn, and Jorgensen (2013) proposed an access control model that attempts to find a solution for managing shared information that is co-owned by a number of people based on multiple aggregation methods. The model incorporated vital features such as multiparty authorisation requirements, a multiparty policy specification scheme, and a policy enforcement mechanism which considered as a novel solution for enhancing collaborative management of shared data among social network users.

Furthermore, commercial companies could design security and privacy tools to protect social network users from online threats. For instance, Rahman, Huang, Madhyastha, and Faloutsos (2012) has proposed a Facebook application called (MyPageKeeper) that aims to protect Facebook users from spam and malware attacks. The app was designed based on the idea of testing similarity features in which measuring the similarity score across different posts can provide a sense of the probability of spam existence. The goal of this app is to detect and alert users of any spam or malware that appeared in the individual user account walls or feeds.

Other context-related tools that are believed to aid peoples' privacy and security decisions apply soft paternalism or nudging. Dealing with interventions that support people to make beneficial privacy and security decisions has two sides to consider. Improving the privacy and security settings by including advanced and large amounts of feature settings

might help increase user control over their profile. Yet, this approach is not usually the best solution for privacy and security issues as this will increase the complexity of making safe and accurate decisions (Acquisti et al., 2016). Reaching a balance between designing strong and usable security and privacy settings is necessary to simplify user assimilation. Using user-tailored privacy could afford this balance by providing a personalised decision-support based on predicting the profile owner's needs and preferences (Knijnenburg, 2017). Tailoring privacy awareness and education programs to the individual user's needs requires profiling the end-users based on their characteristics and vulnerabilities as discussed in the next section.

2.4.1.3 Detecting the Victim Vulnerabilities

Focusing on the vulnerabilities of the target of the attack is critical to fighting against social engineering threats as human are responsible for detecting such threats and preventing them from spreading out. Unfortunately, people have repeatedly shown poor performance in detecting deception (Algarni et al., 2017; Iuga et al., 2016; Saridakis et al., 2016). All previous technical countermeasure cannot entirely protect social network users. The users themselves should practice safe activities and be tentative about existing threats. Social engineers are keen to exploit user vulnerabilities rather than system vulnerabilities due to the huge success rate and low needed effort associated with these approaches. Research that investigates users' vulnerabilities is demanded to increase user awareness of their weaknesses in order to target them by training and awareness programs.

Social networks features have been found to predict users' behaviour and preferences in electronic marketing research (Buettner, 2017). Networks' features could also contribute to identifying vulnerable users to social networks deceptions. Individuals with high network's size are found to be more vulnerable to online risks when compared with those with a limited number of connected friends in the network (Buglass, Binder, Betts, & Underwood, 2016). Furthermore, vulnerable users can be determined based upon their loose privacy settings which could also place all of the connected friends of the individual user's network at risk (Gundecha, Barbier, & Liu, 2011). It has been also claimed that monitoring the privacy settings of individual's network friends and unfriending those who are classified as vulnerable could increase the security and privacy of the individual's network.

The importance of investigating user vulnerabilities directs this research to focus on understanding human behaviour and perception of social networks in order to facilitate predicting vulnerable users based on human characteristics. Section 2.5 will provide more details on user vulnerabilities.

2.4.2 Countermeasures in Other Social Engineering Contexts

In this section, a brief description of other prevention approaches and techniques are provided that have been proposed to combat social engineering attacks in other contexts such as email and organisation environment. Since these techniques could open insight for notions of innovation or improvement opportunities to be adopted in social network contexts.

2.4.2.1 Compliance with Policy

Policy compliance is considered one of the most effective solutions to protect organisations from security exploitations. Yet, failure to comply with organisations information security policies is a persistent problem among employees (Vance, Siponen, & Pahnila, 2012). In an organisational context, complying with information security policies can mitigate the risk that might arise from employees' behaviour (Sohrabi Safa, Von Solms, & Furnell, 2016).

Increasing employees' perception of the importance of complying with security policies is usually the element of most security training programs (Aldawood & Skinner, 2018; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Yet, along with training interventions and information security experience, sharing security information and news among the employees and encouraging the collaboration between them could significantly contribute towards complying with organisational information security policies (Sohrabi Safa et al., 2016).

2.4.2.2 Training

Phishing embedded training has been found to protect vulnerable email users (Jansson & von Solms, 2013). This training is designed in "education-on-demand" manner which targeted only users who have been found not capable enough to deal with phishing. Previous studies revealed that anti-phishing training was much effective and helpful when targeting only vulnerable victims after conducting a mock attack (Kumaraguru et al., 2009). However, some research found that training alone is not considered an effective measure to combat social engineering threats. Yang et al. (2017) found that integrating the knowledge gained from anti-phishing training and including effective warning messages could provide significant protection against phishing.

Other research focuses on examining the effectiveness of using online games in users' security training and education. For instance, a mobile game called Anti-Phishing Phil has been designed to increase people detection ability of phishing websites (Arachchilage, Love, & Beznosov, 2016). The experiment result indicated that subjects have distinguished between

good and malicious website by the success rate of 56% while after playing the game the success rate was raised to 84%. Yet, only 20 subjects have participated in the experiment which makes the reliability of this experiment considered limited.

Despite the fact that training programs and awareness campaigns are implemented by most organisations from all around the world, online risks are still existing. This might be due to the deficiency of research that use theoretical backgrounds to design and measure the usefulness of these training programs.

2.4.2.3 Warnings and Notifications

The role of warning messages in combating social engineering threats is considered substantial and are thoroughly studied in the literature as an anti-phishing solution (Yang et al., 2017), an anti-malware solution (Modic & Anderson, 2014), and even as a solution against VCFA (Siadati et al., 2017).

With the goal to investigate if warning messages can have a significant role in combating social engineering threats, some research has empirically investigated the benefits of sending announcements and notification about potential threats incidents to elicit people reaction (Reeder et al., 2018). Priming and warnings about the risk of sharing personally identifiable information found to be not effective enough to prevent shoppers from disclosing their email addresses, their bank account details, products they normally purchase, and which online shops they use (Junger, Montoya, & Overink, 2017). All of this disclosed information can be used by offenders to conduct an easy and successful spear phishing attack. People seem to lack understanding of what considered private information and what information they can disclose safely. Focusing on educating people about personally identifiable information role in privacy and security interventions are needed. Furthermore, people seem more likely to ignore malware warning messages and rely on security advises received from their friends (Modic & Anderson, 2014).

People have been observed to have different reasons to choose to adhere or not to warning messages. It has been noticed that people concerns are different and a “one-size-fits-all” view in designing warning messages should be improved to include contextual and habitual factors (Reeder et al., 2018). Furthermore, integrating warning and training together showed a high success. Educating people about what is the meaning of every warning message could increase people compliance with the warnings (Yang et al., 2017).

Generally, applications and tools have been recommended to serve as protection against online threats. Yet, social engineering attacks usually do not rely on breaking technical

preventions. Yet, this kind of attack uses very smart deceptive techniques to reach and convince their victims to obey their requests. Therefore, the next section will focus mainly on investigating human vulnerabilities in an attempt to understand why people get easily deceived by social engineering-based attacks.

2.5 User Vulnerabilities

Vulnerability, as defined by ISO (the international organization for standardization), is the weakness of any individual, organisation, or system that can be exploited by single or various types of threats (ISO/IEC 27000, 2018). Tracking this weakness or vulnerabilities is the best solution to prevent this exploitation from happening either to a particular system or people involved. Human characteristics have been found to drive people behaviours online in different fields. A review of the most influencing factors that have been reported in previous research to predict vulnerable users will be discussed in this section.

User vulnerability to social engineering can be defined as the set of user attributes that incline that particular user (rather than other individuals) to be a potential victim to the social engineers' attack. Previous research that investigates human characteristics that influence or predict user vulnerability to cybercrimes can be divided into four groups depending on the focus of attributes that they investigated.

2.5.1 Socio-Psychological-Related Attributes

Most acknowledged human weaknesses that have been indicated by previous research to impact people judgement of deception attempts are primarily related to socio-psychological characteristics (Iuga et al., 2016; Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012).

The personality traits have been explored to have an impact on people behaviour in social networks (Moore & McElroy, 2012). As different habits and behaviour have been indicated to correlate with certain personality traits (Liu & Campbell, 2017). Further effort has been conducted to automatically predict the personality traits of social network users which revealed positive and promising results (Azucar, Marengo, & Settanni, 2018). These results might encourage social engineering research to examine the role of personality traits on people vulnerability to SE especially in social network context as if a positive correlation between personality and vulnerability is found then it could help to better anticipate and protect vulnerable users.

Social engineering researchers have noted that personality traits impact on phishing victimisation (Cusack & Adedokun, 2018; Halevi et al., 2013; Pattinson et al., 2012).

However, this has only indicated that specific traits may cause higher susceptibility rates and did not test whether specific demographics, such as gender, contribute to this relation. Existing empirical studies have measured the relationship between the big five personality traits and email phishing victimisation (Alseadoon et al., 2015; Halevi et al., 2013). However, there are still some antithetical results as Halevi et al. (2013) stated that neuroticism is the trait most correlated to responding to a phishing email, while Alseadoon et al. (2015) found that openness, extraversion, and agreeableness are the personality traits that increase the possibility of a user response to phishing emails.

A proposed framework constructed of four dimensions: personnel (including culture, age, and gender), experiential (including general, technology, and professional experience), personality trait, and phishing susceptibility (likely to respond, and time to respond) suggested that each of these dimensions plays a significant role in individual susceptibility to phishing attacks (Parrish Jr., Bailey, & Courtney, 2009). Yet, this framework is still to be empirically examined to be validated. Additionally, an investigation of the relationship between different individual's variables and people information security awareness revealed that demographics, namely age, gender, did not affect individual security awareness (McCormac et al., 2017). Yet, the study result indicated that individuals with conscientious, agreeable, and openness as a personality trait and those who have a low level of risk-taking propensity are usually highly aware of information security.

Furthermore, gender, age, and educational background are the most contradictory variables in the existing literature of phishing research and are repeatedly examined in relation to phishing victimisation (Griffin, 2018; Marriott, 2018; Sheng et al., 2010). According to the potential victim's age, some research results state that younger users are the most potential and vulnerable targets of deception (Alseadoon et al., 2015; Griffin, 2018; Halevi et al., 2013). Yet, these results are difficult to generalise as the vast majority of such studies were reported on constrained samples, mainly university students. It was found recently that among many examined demographic features, computer usage experience, as well as gender, are the most significant predictors of user's detection ability of web-based phishing attacks (Iuga et al., 2016). Yet, in the context of victimisation in social networks, self-confidence in computer skills might lead to risky behaviour as a positive relationship has been found between higher computer skills and user victimisation (Saridakis et al., 2016).

Culture has been given less attention in IS research in general and in SE victimisation research in particular. One report on email phishing (Al-Hamar, Dawson, & Guan, 2010) has stated that some cultural value might incline people to behave in a certain way such as being

trustful, or generous. Those people will be more vulnerable to phishing victimisation as they may easily be exploited if emotionally persuaded by the attacker (Al-Hamar et al., 2010). Flores et al. (2015) investigated whether culture has an impact on email phishing resistance among employees from different nations (USA, Sweden, and India). The study result proved the significant role of culture in the users' behaviours and decision-making at times of risk.

In an attempt to profile phishing victims, Darwish et al. (2012) study concluded that user demographic (included age, gender, and education) and personality traits are critical to predicting victim susceptibility to phishing attacks. The study also revealed that internet usage behaviour has a moderate influence on SE victimisation. Therefore, the next section will concentrate more on the relationship between people behaviour and SE victimisation.

2.5.2 Habitual-Related Attributes

Prior literature on email environment victimisation (Halevi et al., 2013; Vishwanath et al., 2016, 2011) has explored the effect of social network habits on predicting behaviour toward email phishing. In the virtual network setting, users tend to exhibit their trust by their degree of engagement in the network (Sherchan, Nepal, & Paris, 2013). The individual's habitual engagement in the network can be determined by one factor such as time spent in the network (Saridakis et al., 2016) or multiple factors such as frequency of interacting and checking the network, number of friendship connections, and deficient self-control over network usage (Vishwanath, 2015). High level of user engagement in social media has been found to make users more exposed to online threats in knowledge exchange networks (Saridakis et al., 2016).

A technical study (Al-Qurishi, Alrubaian, Rahman, Alamri, & Hassan, 2018) conducted on the Twitter platform found that profile and content related features are efficient predictors of malicious and legitimate users. Vishwanath (2015) also examined how user habits in Facebook can predict the user's vulnerability to social media phishing attacks. This study concluded that user's social network habits such as frequency of use, lack of control over usage behaviour, and maintaining online relationships can anticipate social engineering victimisation and that highly-active users are more susceptible to social engineers as cybercriminals consider them more valuable. For instance, highly-active users may ensure the accomplishment of the attack as the friendship connection between the victim and the attacker may lead to the victim's friends being deceived by a reverse social engineering technique (Irani et al., 2011). Conversely, users with fewer involvement components, such as a limited number of connections and less regular use, are not the best targets for the attack in light of the fact

that the lure message may not be seen at all since the user does not utilise the social network much of the time.

Moreover, the behaviour related studies reported earlier do not clarify the reasons that relate the online user's habits to the phishing victimisation. One possible explanation for this relationship is that the users' online habits may affect their perceptions, on factors such as risk and trust, which in turn affect their susceptibility to social engineering-based attacks.

2.5.3 Perceptual-Related Attributes

Protection motivation theory, which was developed by Rogers (1975), has been taken as a theoretical foundation for many studies in the field of IS. One such is Workman et al. (2008) study which suggested that perceived severity and perceived vulnerability to security threats are significant predictors of users' security behaviour motivation. According to protection motivation theory in IS research (Vance et al., 2012), when a user encounters a threat, four cognitive factors will be needed to assess the threat: perceived vulnerability (estimation of threat occurrence), perceived severity (to what extent the consequences will be cruel), response-efficacy (to what extent the protection behaviour will be efficient), and self-efficacy (assessment of individual ability to adopt protective behaviour). Martens, De Wolf, and De Marez (2019) adapted this theory and proposed an extended model in an attempt to understand what drives people to protect themselves against different types of cybercrime. Their study findings indicate significant differences in end-user's behaviour toward technical threats compared to social threats.

Perceived risk is considered a critical factor that influences security awareness and behaviour (Öğütçü, Testik, & Chouseinoglou, 2016). Perceiving the risk associated with engaging in online activities is considered a direct influence of people suspicious of existing online threats (Vishwanath et al., 2016). Notably, some research found no correlation between perceived risk and users' behaviour toward either email phishing (Wright & Marett, 2010), or social network victimisation (Saridakis et al., 2016). This contradicts the view that the individual's perceived severity of negative consequences predicts their detection or avoidance behaviour of online threats (Workman, 2007).

Furthermore, some research has focused on other individual attributes such as self-efficacy (Vishwanath et al., 2011; Wright & Marett, 2010), security awareness (Algarni et al., 2017; Wright & Marett, 2010), and privacy awareness (Halevi et al., 2013; Vishwanath, 2015), all of which play an important role in self-protection practices online. Yet, an investigation of the limitations of current social network privacy control systems suggested constructing new

user-focused privacy requirements that give social network users the ability to control and protect their contents from being exploited by cybercriminals (Islam et al., 2017).

2.5.4 Socio-Emotional-Related Attributes

The theory of socioemotional selectivity which was developed by Carstensen, Isaacowitz, and Charles (1999) suggested that people social and emotional development are changing with age. A study (Chang, Choi, Bazarova, & Löckenhoff, 2015) has used this theory to investigate if age differences could affect people motivational priorities and cause variations in social network size and composition. The findings of the study confirm that the selectivity is higher in older adults as they have a smaller Facebook network and larger percentage of actual connected friends compared to younger adults. Some user-related information could be automatically extracted from social networks. Extracting emotional-based features from a social network platform has been found to derive information that is useful to distinguish between malicious and legitimate users (Al-Qurishi et al., 2018).

Social networking sites start to compete with other communication mediums by focusing on satisfying people entertainment needs, social needs by connecting them with friends and family, and information needs by encouraging information and news sharing (Basak & Calisir, 2015; Yang & Lin, 2014). Motivation is a substantial cause that makes people engage in a certain action. This action could be considered risky if it makes the individual user exposed to social engineering. Jason Hong (2012) claimed that "A deeper understanding of end-user motivations, beliefs, and mental models is essential for the security community to build effective countermeasures". Social engineering attackers can utilise these motivations to manipulate and deceive users. For example, users who use the social network for hedonic purposes can be offered a free online game to try to encourage them to accept the trick.

The attacker's persuasion techniques are various, and their impact on the users' responses are diverse and related to the chosen inducement tactic, as revealed by Workman grounded theory investigation (2008b). As a group of people can be persuaded by trust and friendly rapport, others can be influenced by fear tactics. One of the reasons that increase the level of attack success is using the emotional state of victims such as fear, panic, and excitement. For example, attackers use trendy hashtags in twitter that is related to shocking news and take advantage of the public need for new information on the event to spread malicious links to a large group of people (Benevenuto, Magno, Rodrigues, & Almeida, 2010). Other existing research (Cheung-Blunden & Ju, 2016; Wang, Li, & Rao, 2017) has focused on emotional triggers, such as fear and anxiety that incline users to react to various types of

social engineering attack. Attackers usually exploited human emotions to maximise the chances of conducting a successful attack. For instance, fearing to lose or expecting to gain something valuable are very effective emotional triggers that make humans more vulnerable to phishing deception (Goel, Williams, & Dincelli, 2017).

Trust is one of the emotional variables that has not been given enough attention in previous research. In reality, trust is a basic component of any online or offline individual's communication and relationship enhancement. Farrahi and Zia (2017) proposes that friendship connections reveal high accuracy as measures of trust among social network individuals. Trust in the virtual environment of social networks can be classified into two types: trusting the medium and trusting the members (Dwyer, Hiltz, & Passerini, 2007). The density of information sharing in a social network is related to the amount of trust their users have with regards to the network providers and members (Dwyer et al., 2007). Trust regularly prompts a lesser perception of risky behaviour, which eventually may raise the likelihood of succumbing to social engineering attacks.

Moreover, some researchers have examined the influence of social network users' motivation on their usage behaviour such as frequency of use, usage time, and function of use (Chen, 2012; Wang, Jackson, Wang, & Gaskin, 2015). Since Vishwanath (2015) study stated that those behaviour have an effect on social engineering victimisation, it can be assumed that motivated users can be more vulnerable to social engineering-based attacks. Yet, this assumption needs to be validated.

2.6 Taxonomy of Social Engineering Attacks in Social Networks

When investigating human behaviour toward online threats, it is important to focus on the interaction between the individual's attributes, their current context, and the message persuasion tactic (Williams et al., 2017). Tetri and Vuorinen (2013) developed a SE framework on the basis of a multidimensional approach that relies on three dimensions: persuasion, fabrication, and data gathering. The framework focuses on the users' interpretation of the attack in relation to information security policy and education more than relying on the individual characteristics of the user. Yet, the taxonomy hasn't been evaluated or explained to how it can be used to support defensive measures. Another social engineering taxonomy was proposed by Algarni and Xu (2013) especially for social networking sites. The taxonomy provides a clear explanation of the different entities that could be involved in social engineering attacks in social network platforms with the main focus from the view of the attacker perspectives. Some studies (Jamil et al., 2018; Mouton, Leenen, & Venter, 2016) have

proposed high-level models and scenarios to detect SE attacks by addressing the attack phases and associated filtering steps. The objective of proposing those models is to enable other researchers to use them as templates to design effective countermeasures.

Krombholz et al. (2015) proposed a further taxonomy of social engineering sophisticated attacks in the virtual communication networks. The taxonomy consisted of three main entities that have been argued to form every social engineering attack which is the operator of the attack, the type of the attack, and the attack channel. The attack can be originated by either a person which reflected a limited number of victims such as identity cloning attacks and spear phishing or by malicious software which usually targeted a considerable huge number of users. Examples of the automated social engineering attacks that are usually conducted by software are ASE botnet Attack and automatic spamming.

The type of operator can also determine the chosen type of SE attack. One taxonomy (Foozy, Ahmad, Abdollah, Yusof, & Mas'ud, 2011) has classified the type of attack to be technical-based, which includes phishing, scam, and malware, or human-based, such as impersonation, identity theft, and reverse social engineering. An example of a technically based attack in social networks is the cross-site scripting attack that recently becomes popular among criminals in SNSs (Rathore, Sharma, & Park, 2017). In contrast, persuading the victim to contact the attacker by connecting with the victim's friends through a reverse social engineering technique is an example of a human-based attack in social networks (Irani et al., 2011).

Context plays a critical role in SE attacks because this determines the complexity of the attack, especially for the operator. In SNSs, there are three main sources in the user's profile that cybercriminals use to reach their victims, content, friendship connections, and privacy settings (Algarni et al., 2013). A network's privacy and security settings are important measures to protect the user. Even with the limited functionality of current social network security and privacy preferences (Bertino & Ferrari, 2018; Islam et al., 2017), if users adjust the network's privacy setting and prevent non-friends from accessing their account, the attacker would not be able to use the account to gather the information required to conduct indirect attacks.

The receiver of the attack is always responsible for evaluating and recognising the attack to prevent it from succeeding. Fan et al. (2017) has focused on investigating human weakness against social engineering and apprehended two essential levels that cause such weaknesses which are: internal characteristics of human nature and the influences of external circumstances. A range of user characteristics determines the user's ability to detect the attack.

These characteristics are included under four perspectives which are socio-psychological-related, habitual-related, perceptual-related, or socio-emotional, as discussed earlier in this chapter. Figure 2.4 presents a general taxonomy of social engineering in social networks which are developed from previous taxonomy studies. However, among the four major entities that formulate the social engineering attacks in social networks, the present study focuses only on receiver characteristics that make the end-user more vulnerable to social engineering attacks and will be discussed in more detail in Chapter 4.

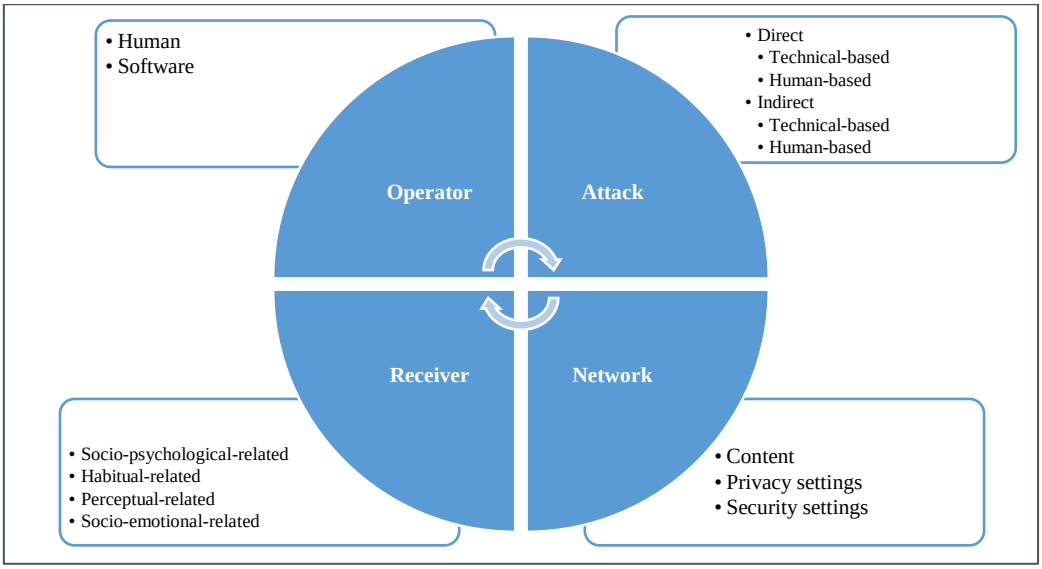


Figure 2.4 General Taxonomy of Social Engineering Attacks in Social Networks

2.7 Literature Limitations and Research Gap

2.7.1 Social Engineering in Social Networks

Previous social network-related information system research lack of research that focuses on the development of SN-specific theories as the social network research has limited use of theories to justify their findings (Cao et al., 2015). There is limited discussion of social engineering violations in the social network context in the literature. Most of the existing work focuses on phishing attacks in an email environment. While some important variables that have been reported in email phishing research have never been examined in the environment of the social network, other reported factors that assumed to affect human detection ability of social engineering threats have not been empirically tested in previous research. However, the properties that have been investigated to affect human vulnerabilities were mostly dealt with separately or combined with a limited number of dimensions and not necessarily focused on a social network context. Trust, for instance, has been dealt with as a general type of an individual personality or habit, while in a social network context trust can be perceived as a

two-dimension factor that includes trusting the network provider as well as trusting other members in the network. The literature lack such study that considers context-driven human characteristics that could predict human behaviour toward social engineering threats.

2.7.2 Human as the Weakest Link

The literature shows that security practitioners still rely on technical measures to protect from online threats while overlooking the fact that cybercriminals are targeting human weak points to spread and conduct their attacks (Krombholz et al., 2015). This raises the necessity of finding a solution that helps the user toward acceptable defensive behaviour in the social network setting. Identifying the user characteristics that make them more or less vulnerable to social engineering threats is a major step toward protecting against such threats. Identifying the weakest points can help users to recognise their perceptual and habitual limits and to target these limitations by a personalised advisory system that is designed to fit the user's needs which could provide new insight to social engineering mitigation solutions.

2.7.3 Human Perception and Behaviour

Previous social engineering and deception research haven't satisfactory identify the factors that influence users' attack detection ability. Studying users' behaviour and perception toward social engineering-based attack is vital to distinguish the weak points in users' ability to detect these attacks. Users' characteristics that influence users' vulnerability must be thoroughly investigated to eliminate this dilemma and help to build a profile for vulnerable users in order to focus on increasing the training programs and education for those individuals. Human behaviour is complicated and usually influenced by many aspects which make it difficult to be addressed based on one or two perspectives. To understand or predict human online behaviour, integration between different properties and views is needed in order to reach a holistic combination of perspectives.

2.7.4 Combining Different Perspectives

Limited studies incorporated various theories and perspectives to understand people risky behaviour online while taking into consideration the context of the study as a centre of combining these perspectives. For instance, previous research has not considered security awareness as a context-related factor. Instead, they treated the security awareness as a general knowledge of different cyber-attacks definitions. Furthermore, when reviewing the literature that investigates human vulnerabilities, emotional perspective has been found to be limited. This means that the focus was mainly on human vulnerabilities in email context in which emotions are not playing a central role in its communication comparing to other contexts such

as social networks. The literature lacks combining different perspectives to understand the human ability to detect threats on social networks context, which is the gap this study aims to fill.

2.7.5 The Interactions among Different Perspectives

Most of the previous research has stated that particular individuals' characteristics can influence their judgement or reactions to security threats. Little research has investigated if factors from different perspectives can interact and influence each other. From the models and frameworks review earlier, it was obvious that the literature did not give much attention to the direct or indirect effects among the considered factors which ultimately influence people susceptibility to online threats (more details in chapter 4). For instance, socio-psychological variables such as personality traits could have an influence on emotional factors such as trust and usage motivation.

2.7.6 The Culture of the Targeted Population

A systematic review of SN-related research has concluded with a recommendation for future research to explore users' behaviour outside the western regions and to investigate cultural factors that may open new insights for future studies (Cao et al., 2015). It was clear from the literature review that most of the previous research has been conducted in western countries. Yet, limited studies have considered Arab countries as their targeted population. Saudi Arabia is an interesting and unusual study context because it has a higher population of social media users than other areas, and has a comparatively much younger population. Recently, the Saudi government has initiated the vision of "2030" which will contribute to the continued rapid development and growth in many aspects of the country. Yet, the country has witnessed many cyber-attacks targeting government and organisational institutions which make this country a rich target for the present study.

2.8 The Focus of the Present Study

From the earlier mentioned gaps in the literature, it has been noticed that there are a huge argument and contradictory results in regards to the most influencing factors of human behaviours when dealing with online security threats in general among previous studies. In the environment of social network, limited research has investigated human characteristics that could be used to distinguish potential victims among the population. Identifying susceptible users will help to target those individuals to enhance their detection abilities. However, most of the previous studies rely on one dimension of user-characteristics to predict vulnerable users

such as focusing on user habits, or users' perception of risk, while in order to understand human behaviour toward online threats multiple perspectives should be considered to reach accurate prediction.

Furthermore, investigating if these different perspectives influence each other is another problem that this research will consider. The present study attempts to address these limitations on identifying user vulnerabilities by proposing a more holistic user-centric framework which relies on four perspectives and the process is taken to develop the user-centric framework will be discussed in further details in Chapter 4. This research on determining user vulnerabilities affords a basis for profiling users according to their weakness in respect of particular threats. In turn, this provides a means to design a personalised advisory system that sends awareness posts to target individual users' needs.

2.9 Chapter Summary

The number of victims of social engineering attacks will be decreased if the users' detection ability has improved. This improvement of the user's detection behaviour can't be occurred without investigating the users' weakness points. Thus, the present research is motivated by the goal of determining the user's attributes and dimensions that impact their detection ability of cyber-attacks. Previous research has not satisfactory explored those factors especially in the context of social networks. Therefore, the present research aims to identify the user's characteristics that influence their judgement of social engineering-based attacks in social networks.

Chapter 3. METHODOLOGY

3.1 Overview

This chapter discusses the research design and the adopted methods of the current study. The methods and techniques that have been used are also explained along with the reasons that justify their suitability for the present study. In general, this research included three main phases and utilised a sequential exploratory design to answer the research questions which is discussed in Section 3.2. The first phase, which is explained in Section 3.3, used a mixed methods expert review that involves collecting both quantitative and qualitative data at the same time. Comparing and analysing the findings of both data sources in this phase were required to validate the study framework. Section 3.4 illustrates the process of the content validity test that was conducted in the second study phase to verify the measurement items for each framework factor and to evaluate the suitability of the identified dimensions to measure the intended constructs. All of these validated measurement items for factors and dimensions together form the research conceptual model. Section 3.5 provides justification of all the methods that were used to analyse the third study phase which used a scenario-based experiment to examine the relationships between the study constructs and its ability to predict user vulnerability to social engineering (SE) victimisation. Finally, Section 3.6 offers a conclusion for this chapter.

3.2 Using a Sequential Exploratory Research Design

In general, a research design provides an overview of the procedures and approaches that will be followed in order to obtain the information that will help to answer the research questions (Saunders, Lewis, & Thornhill., 2016). Qualitative methods, quantitative methods, and mixed methods are the three main research approaches that are mostly adopted by researchers in various fields (Creswell & Creswell, 2018). A systematic review of previous SN-related research called for more investigation on the individual's characteristics that play a critical role in this research area, and suggested to do that by adopting various research methods and data analysis techniques (Cao et al., 2015). Investigating human behaviour is a very complicated task that needs different methods to comprehend. Therefore, the present research adopted an exploratory sequential mixed methods design.

According to Creswell and Creswell (2018), "a three-phase exploratory sequential mixed methods is a design in which a researcher first begin by exploring with qualitative data

and analysis, then builds a feature to be tested (e.g., a new survey instrument, experimental procedures, a website, or new variables) and tests this feature in a quantitative third phase". With this in mind, to predict users' vulnerabilities toward SE attacks in a social network context, this research included three main study phases. Where the first study phase used both quantitative and qualitative inputs to help construct and validate the user-centric framework (UCF). Then, the second phase developed and validated constructs' measurement scales to be used in the third phase. In the third phase, a conceptual model has been proposed and empirically evaluated using a quantitative approach. Figure 3.1 illustrates the three phases of the current research.

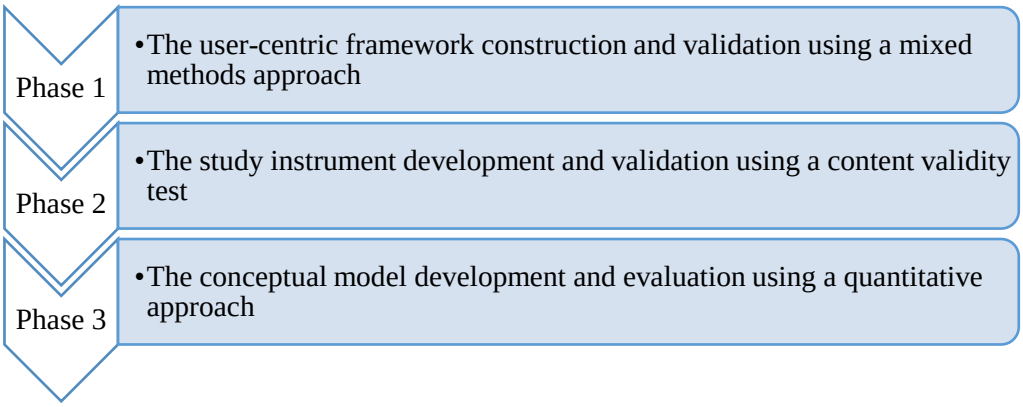


Figure 3.1 The Three Main Phases of the Current Research

3.3 First Study Phase (Mixed-Methods Approach)

The best selected approach for a particular study should be based upon the purpose and objectives of the study (Creswell & Creswell, 2018). As the aim of conducting the first study phase of the current research is to validate the proposed UCF, adopting a mixed methods approach is the most appropriate. Mixed methods experts review has been used to validate the proposed UCF. Expert review is considered an evaluation method in computing research (Holz et al., 2006). This strategy allows collecting mixed data (quantitative and qualitative) of experts' evaluation simultaneously. However, each type of data has different weight and objective to the framework's validation process. In such a concurrent strategy, one type of method, either quantitative or qualitative, will be considered as a primary method while the other will be treated as a secondary method that supports the primary results (Creswell & Creswell, 2018). For example, in the first phase of this research, the quantitative data will help to identify the level of agreements among experts regarding the proposed framework factors and dimensions while the qualitative data will help to gain a deeper insight in the experts' opinions about the framework's items.

3.3.1 The Justification for Using a Mixed-Methods Experts' Review

Collecting mixed data from the experts' review could provide a robust evaluation of the proposed framework. As the two data sources can be compared and integrated together to reach complete assessment (Creswell & Creswell, 2018). An online self-administered survey has been chosen for the present study as the approached experts are geographically dispersed. Additionally, the advantages of using this type of survey give the participants the ability to choose a convenient time to answer, respondents can answer honestly with no intervention or biased caused by the assessor, and survey can be completed and delivered in spite of place or time constraints (Sekaran & Bougie, 2010).

3.3.2 Method

Validating the framework components and dimensions are fundamental in developing any new measure that concentrates on combining new perspectives to explain a particular behaviour. Some of the framework's components have been validated in previous research, but they have never been confirmed together in one framework in a social network context. Therefore, the present study adopted expert reviews as a mixed methods approach to validate the proposed framework with an objective to approve or modify the proposed UCF.

This approach is essential to evaluate the dimensions and attributes of the newly developed framework to get proper feedback and validate the proposed framework in the study context. Furthermore, this step is important to overcome any future problems that might be caused by relying on invalidated framework components. For example, if the present framework has not been adequately validated, any future research or model based on this framework will not be reliable.

3.3.2.1 Instrument Design

In order to measure the expert agreement level of the framework dimensions and attributes, an online questionnaire has been designed (Appendix A). The questionnaire has three parts, the first part asked about participants' demographics such as their age, gender, education, and level of expertise. The second part includes the framework dimensions and factors. Each factor has a brief description to explain what it means in the study context. Participants have been asked to read each factor carefully and rate the importance of those factors regarding their effects on users' vulnerability to social engineering attacks in social networks. Respondents have been asked to rate the importance of each framework factor on a 5-point Likert-scale, from 1-not important to 5-very important.

Moreover, checking if participants gave enough attention to the questions and framework items is essential in self-report questionnaires. Using bogus items in scale-based questions was strongly recommended to identify careless responses (Meade & Craig, 2012). Therefore, to figure out if the participants were careless and not paying enough attention, the researcher added "the user's height" as an item in the socio-psychological perspective, which is obviously not an important factor in relation to the user's detection ability of social engineering.

The third part includes three open-ended questions that aim to gather the experts' opinions and recommendations to improve the proposed framework. Completing this part was optional. To ensure that responses to the second part were captured, participants could submit the questionnaire without entering any data in the third part of the questionnaire. The open questions asked the experts to indicate the following:

- From your experience, are there any factors in the framework that should be combined?
- From your experience, is there any factor in the framework that should be split?
- From your experience, do you think there are any other factors that should be included in the framework?

3.3.2.2 Sampling

To be included, participants required sufficient knowledge and significant experience in the information security (IS) field. Experts were selected with this in mind from universities' and organisations' websites. Specialists were identified in the IS field, either in academic or organisational sectors. The selected experts were sent an email asking them to participate in the survey. In the two study rounds, 63 emails have been sent with 27 responses received, of which 11 have completed the open-ended questions.

The sample used in the current study is comparable to other studies that adopted expert review as a research method. The adequacy of using a small sample in the expert review approach has been confirmed in some previous IS studies (Aguti, Wills, & Walters, 2014; Muhlbacher & Piringer, 2013; Yahya, Walters, & Wills, 2016). However, to mitigate any bias or residual limitation from sample size, the selected sample included both genders, a range of ages between 25 and 44 and also included different levels of expertise and education.

3.3.2.3 Ethical Approval

The ethical committee of the Department of Computer and Information Sciences at Strathclyde University has granted ethical consent for the experts' review study. Appendix B presents the ethical approval that was issued by the ethical committee. Participants were

informed that participation in this study is voluntary and there was no risk or harm associated with it. All responses will be anonymous, confidential, and can be accessed only by the researchers. Participants have been informed of their rights to withdraw from participating in the study. The contact details for the researcher and the supervisor provided in the cover letter and participants were encouraged to use them if they have any concerns regarding the conducted study.

3.3.3 Pilot Test

This step was conducted to test the questionnaire design and to acquire comments and feedback from a sample of experts to modify the questionnaire. Accordingly, 6 participants have tested the expert review survey. While half of them are postgraduate students in the Department of Computer and Information Sciences at the University of Strathclyde in the UK, the other half are computer science lecturers from King Abdul-Aziz University in Saudi Arabia. The questionnaire was amended in light of these responses. For example, some factors have been found to be difficult to understand. Thus, their definition in the questionnaire was amended for more clarity.

3.3.4 Study Procedure

An invitation email was sent to the selected experts asking them to participate in the study. The email described the aims of the study. If an expert agreed to participate, an online-questionnaire link could be visited (this link was included in the email). The study was conducted in two rounds:

- In the first round, an email was sent to 43 information security specialists who work either in academic or other organisational sectors asking them to participate in the survey. 15 responses were received.
- The second round was conducted one month later. An email was sent to 20 information security experts, all of whom were academic lecturers in Saudi Universities, and 12 responses were received.

Repeating the experiment more than once is a common scientific practice to ensure that the result can be replicated. According to Kimberlin and Winterstein (2008), This can be done by two different types of reliability tests intra-rater and inter-rater. Intra-rater reliability refers to repeating the test with the same raters more than once until they reach an agreement, while inter-rater reliability means repeating the same test with different evaluators with the goal to measure the degree of agreements among raters (Kottner et al., 2011). The reason behind conducting two rounds of experts' review in the present study is to increase the reliability of results by using the inter-rater reliability approach. This approach aims to identify

the degree to which the results obtained from both rounds of the evaluation are stable and yield similar results, even though different experts have been recruited in each round.

After conducting the two study rounds, the received results have been compared for similarity and differences and most importantly to confirm the experts' agreement regarding the proposed framework factors. Finally, the third qualitative part of the questionnaire which includes the open-ended questions has been analysed to indicate the experts' suggestions for the framework's modification and improvement. Figure 3.2 describes the process that has been taken to validate the proposed framework.

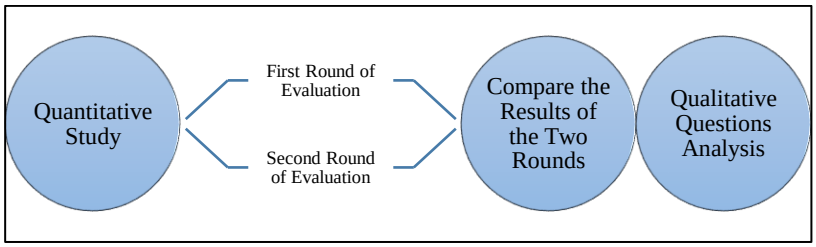


Figure 3.2 Framework Validation Method

3.3.5 Analysis Methods

Since both quantitative and qualitative data have been collected, different analysis methods have been applied. The analysis methods that have been used with the quantitative data will be discussed in Section 3.3.5.1, then the justification of the used qualitative analysis method will be explained in Section 3.3.5.2.

3.3.5.1 The Quantitative Data Analysis

The collected quantitative data were analysed using SPSS statistical software. The Likert-scale is a popular measure that is used in many research surveys. However, the analysis techniques that are used to analyse Likert-scale data generate a number of disagreements among scholars. While some scholars believe that Likert data must be analysed using nonparametric statistics such as Mann-Whitney-Wilcoxon, others think that parametric statistics such as t-test are more robust and powerful with Likert-scale data. In an attempt to clear this ambiguity, multiple studies (Mircioiu & Atkinson, 2017; Winter & Dodou, 2010) have conducted investigations to clarify which procedure between parametric and nonparametric tests should be used with five-point Likert data. These studies concluded that both methods provide similar results and have similar power in analysing five-point Likert items. Thus, the present study analysed the collected experts' review data using parametric and nonparametric statistical tests which also yield similar results (See Appendix C for more details).

Another investigation done by Norman (2010) has drawn similar conclusions after demonstrating all the opponents' arguments that parametric statistics are not suitable for Likert items. Those claims were focused on sample size, normality, and the ordinal nature of data. Norman (2010) stated that those claims must be ill-founded as all the findings of previous studies since 1930 provide evidence for the robustness of parametric procedures even with some violations. Norman's conclusion went further by suggesting that parametric tests are more powerful than nonparametric tests.

The objective of the current study phase is to confirm the framework components by measuring experts' opinion and attitude toward the framework dimensions and items. The aim is to exclude from the framework any items with importance rated lower than 3 and include any item with importance rated above or equal 3. Therefore, every expert opinion is important in this study. Using nonparametric test to analyse this data means that only the opinion of part of the experts will be considered. For example, if the nonparametric statistic (Mode) has been used, and for a particular item, the result was (2, 2, 3, 4, 5, 5), the Mode will be 2 or 5 while "2" represents "slightly important" and implies that this item must be excluded from the framework according to the opinion of only two experts, "5" represents "very important" which makes this item essential to include in the framework which reflects the opinion of four experts. To avoid such decision conflicts, nonparametric statistics were considered unsuitable for this study phase. Using parametric tests would prevent losing such important information (Mircioiu & Atkinson, 2017), as it allows considering the opinion of every single expert.

Previous arguments provided evidence for the robustness of parametric statistics with Likert-scale data. Additionally, the adequacy of using parametric statistics with experts' review data has been confirmed in previous studies (e.g., Aguti et al., 2014; Yahya et al., 2016). Thus, the present study opted to use one sample t-test to analyse the result of the first expert review round while using an independent samples t-test to compare the results of the two study rounds.

3.3.5.2 The Qualitative Data Analysis

Thematic analysis is the process of identifying codes or patterns from the data set (Braun & Clarke, 2012). Two types of thematic analysis are existed inductive (data-driven) and deductive (theory-driven). While the inductive approach is conducted if the themes need to be driven from the data only without any intervention from prior knowledge or theory, deductive approach codes and categorises the received text based upon pre-existing frames (conceptual framework) (Braun & Clarke, 2006).

Since the objective of the expert review is to verify and improve the proposed framework, hybrid (both inductive and deductive) thematic analysis was used in order to combine the advantages of both approaches (Fereday & Muir-Cochrane, 2006). While conducting thematic coding aims to find common themes or categories among the collected data and linking them to the proposed framework factors and dimensions, including new suggested themes by the experts to the proposed framework is also considered valuable. Since the qualitative part was limited to three open-ended questions, finding interchangeable answers among participants was uncomplicated. Furthermore, these open-ended questions were collected in parallel with the quantitative data. Therefore, linking each group of responses with the four perspectives that have been covered by the quantitative questions provided feasible findings.

3.4 Second Study Phase (Measurement Scales Validation)

The validated UCF has provided a set of potential factors that could impact user vulnerability to SE. Yet, in order to measure their effect, these factors should be converted into measurable variables. The present phase is intended to develop an instrument to measure the impact of the proposed constructs and to evaluate the validity of these constructs' measurement scales. In order to use these scales later to conduct the empirical study in the third study phase.

In the proposed UCF, two types of constructs are existed (first order factors and second order-factors). For the first-order factors, it is required to identify the set of items that are needed to measure them among the poll of items that could be found in the literature. While in the second-order factors, checking if their identified first order factors could accurately measure their intended second-order constructs is needed. Therefore, conducting content validity test is essential for the present research for two reasons. First, to validate the measurement items for every factor. Second, to confirm the suitability of the identified dimensions to measure the intended construct. Therefore, Mackenzie, Podsakoff, and Podsakoff (2011) guidelines have been followed to develop and validate the study constructs measurement scales. This process starts by conceptualising the constructs and precisely defining them, then developing constructs measures by identifying the items that represent and measure the study constructs. After that, conducting content validity test for these measurement scales to assess the feasibility of the selected items. More details about these three steps are provided in chapter 6.

3.4.1 Content Validity Test

Content validity can be defined as the extent to which the measurement used in the test, which could be either questions, tasks, or items, can precisely reflect the constructs that the test aims to measure (Gregory, 2007). Content validity is an important step to be assessed before conducting the original test, to guarantee that the selected measurement items sufficiently represent the constructs. Failing to confirm this validity, may lead to serious problems, especially with formative constructs (Petter, Straub, & Rai, 2007).

A review study has found that reliability tests are more commonly adopted in empirical studies, while validity tests have not received much attention from researchers (Barry, Chaney, Piazza-Gardner, & Chavarria, 2014). However, content validity must be considered when the measurements used in a test are developed or adapted (Yao, Wu, & Yang, 2007). Even when choosing specific adopted items among others, it is essential to validate whether those selected items adequately represent the sample of other potential items to measure the construct (Gregory, 2007). This helps to make sure that the study findings are accurate and may avoid misleading interpretations of the results.

Several content validation methods have been proposed in the research methods literature such as Anderson and Gerbing (1991) sorting method, Hinkin and Tracey (1999) rating method that has been illustrated by Yao and colleagues (2007), and Schriesheim and Hinkin's item-categorisation method (1990). Hinkin and Tracey (1999) rating method has been recommended by Mackenzie et al. (2011) as it depends on participant's rating of each item in relation to every construct under study using a Likert-scale from 1 (not at all relevant) to 5 (completely relevant). Yet, this method has some limitations. One limitation is that this method asks participants to rate to what extent every item is related to each construct, which overburdens the participants by increasing the rating attempts (Hoehle & Venkatesh, 2015). For example, this study has 52 items and 12 reflective constructs (social network experience is not included as it is measured by one item) which means every participant must make 624 (12 x 52) rating decisions to complete the study. Furthermore, the increasing number of items and constructs requires a considerable number of raters in order to use the rating method appropriately (Mackenzie et al., 2011). Therefore, most of the research that adopted the rating method obtained their results from university students' sample, which make it usually easy to obtain a high number of participants. However, the current study aims to focus on expert assessment of the scales items which means that the number of the sample might be small.

Similarly, the sorting method proposed by Anderson and Gerbing (1991) has some limitations. The substantive validity coefficient, C_{sv} index that is used in the sorting method to

validate the item is not accurate enough and might lead to wrong conclusions (Howard & Melloy, 2016). Moreover, the sorting method forces participants to assign each item to only one relevant construct while the multidimensional nature of the current study constructs makes it difficult sometimes to assign an item to only one dimension (as some items might fit two dimensions with different degrees of relevance).

Thus, the present study followed Schriesheim and Hinkin (1990) item-categorisation approach which has been widely used in the management and communication fields and found to be efficient with multidimensional constructs despite the number of items (Hornsby, Kuratko, Holt, & Wales, 2013). Moreover, as the current study interested on expert assessment, which reflects a small number of assessors, the item-categorisation approach is considered suitable as it can provide stable validity with small samples of participants (Hornsby et al., 2013).

3.4.2 Item-Categorisation Approach

This approach involves sorting and assigning each item to between one and three constructs depending upon the expert's judgement. If the expert thinks the item represents one construct, the expert can assign or tick "√" the intended construct. Otherwise, if the expert thinks the item can indicate more than one construct, the expert will be asked to rank-order the constructs in which the item measures from the highest relevance to the lowest relevance from 1 to 3. After collecting the data, the answers are coded as follows:

- Any tick "√" or "1" answer will be weighted as 3.
- Any "2" answer will be weighted as 2.
- Any "3" answer will be weighted as 1.

Following the recommendations of previous research (e.g., Hornsby et al., 2013; Schriesheim & Hinkin, 1990), items were retained if the percentage of the points assigned by the experts to the intended construct exceeded 60%.

3.4.2.1 Procedure

Participants have been asked to complete a short survey, which consisted of three parts. The first part is asking about some demographic factors such as age, gender, and field of expertise. The second part includes two validation matrixes. Participants have been asked to judge and assign each item in the matrixes with its relevant constructs. Following the recommendation of Schriesheim et al. (1993) regarding the upper bound of the number of constructs in one matrix to be from 8 to 10 maximum to eliminate participants' distraction and boredom. The constructs have been divided into two groups based on the theoretical similarity of the constructs. The perceptual perspective has six constructs which were included in one

matrix with 29 items while the other matrix contains six constructs for both the habitual and socio-emotional aspects with 23 items to be sorted. Participants have been presented with two tables in each group. The first table includes the constructs definitions that participants must read carefully first then they can sort and assign items to their intended constructs in the second table. Items have been listed in the tables randomly to control response bias caused by the impact of item order.

In the third part, participants have been asked to list the numbers of any statements that they found unclear and to write down any concept or term that they read in the statements that they think needs more clarification. The content validity assessment survey can be found in Appendix D. The survey has been distributed to participants either by hand as a printed version or by email as a digital version to those with geographical distance. The responses have been received within three weeks. Yet, two reminder emails were sent after the first and the second week to encourage participants to send back their responses.

3.4.2.2 Sample

Schriesheim et al. (1993) have argued that the appropriate number of samples to conduct content assessment need not be large, as the aim of this assessment is to judge the suitability of the items theoretically to measure a particular set of constructs rather than trying to generalise the relationship results empirically. Therefore, according to Schriesheim et al. (1993), graduate students are considered competent assessors of the content validity tests as their high intellectual ability should make them able to perceive the constructs' definitions and correctly interpret the pool of items. Therefore, the selected participants were PhD students in computer and information sciences department from two universities in the UK.

3.4.2.3 Ethical Approval

The ethics committee of the Department of Computer and Information Sciences at Strathclyde University has granted ethical consent to conduct the content validity study as illustrated in Appendix E.

3.5 Third Study Phase (Quantitative Approach)

After confirming the framework components and factors and conducting content validity test, the hypotheses of the relationships between the constructs and their impact on user susceptibility to SE victimisation have been generated, and the conceptual model has been developed in chapter 7. Examining the relationship between these factors and their effects on predicting users' vulnerability is the goal of the third study phase. Quantitative study approach

is considered very useful when the purpose of the study is to analyse and verify theories or to discover the significance of the hypothesised relationships between variables using statistical techniques (Creswell & Creswell, 2018). Leedy and Ormrod (2015) claimed that using quantitative research methods is the best approach to examine correlations among measurable variables when the goal of the study is to explain and predict some phenomena.

Thus, to evaluate the hypotheses of the conceptual model, an online questionnaire was designed (Appendix F). This questionnaire incorporated questions that measure the four perspectives of user characteristics such as habits and perception in social networks, and a scenario-based experiment. A scenario-based experiment has been chosen as an empirical approach to examining users' susceptibility to social engineering victimisation. This section will concentrate on describing the empirical experiment design, procedure, and analysis methods that have been used to evaluate the conceptual model of the present study.

3.5.1 The Justification for Using a Scenario-Based Experiment

Using scenarios, sometimes referred to as vignettes, can be defined as the process of using "short descriptions of a person or a social situation which contain precise references to what are thought to be the most important factors in the decision-making or judgement-making processes of respondents" (Alexander & Becker, 1978). In a scenario-based experiment, the human is recruited to take a role in reviewing a set of scripted information which can be in the form of text or images, then asked to react or respond to this predetermined information (Rungtusanatham, Wallin, & Eckerd, 2011). Previous research has recommended using a scenario-based approach to investigate user behaviour in decision-making processes (Algarni et al., 2017; Rungtusanatham et al., 2011).

This method is considered suitable and realistic for many social engineering studies (e.g., Algarni et al., 2017; Iuga et al., 2016; Pattinson et al., 2012; Sheng et al., 2010) due to the ethical concerns associated with conducting real attacks. Conducting a real SE attack experiment could be seen as the best method to measure the constructs impacts on users' behaviour and susceptibility toward those actual attacks. However, real attacks experiments have ethical obstacles which make it hard or impossible to conduct. Thus, adopting a scenario-based approach is the closest way to mimic the real attacks as users can imagine themselves facing the same situation in their real accounts and respond accordingly. Furthermore, unlike real attacks, this approach enables controlling other external variables that can affect users' decisions and focus on measuring the factors under study. The incorporated attacks scenarios were cautiously designed to mimic real-world attacks. The study included six scenarios, (four high-risk SE attacks and two low-risk messages).

3.5.2 Method

3.5.2.1 Designing the Social Engineering Scenarios

The social engineering tricks have been designed based on previous studies' recommendations. When designing the trick posts, a sensational language with some spelling mistakes has been used to mimic real attacks. For example, as can be seen in Table 3.1, instead of writing "Please re-confirm your account to avoid blocking" in the scenario number 5, the message used was "Please re-confirm your account to avoid plocking" which includes a spelling mistake.

The social engineering tricks have been chosen based on the most common Facebook attacks in the past few years which have been discussed in the information security literature. The most common and spreading SE attacks have been reviewed and categorised based on their threatening nature to different types (Gao et al., 2011). One of these types is malware attack which has been ranked as a high threat to social network users which can be spread with high success rate by different ways such as by untrusted third-party software which reflect the attack scenario number 4 or by sending an affected downloadable file as in trick number 2.

Phishing also has been classified as a high threat to users especially when requesting any personal information (Gao et al., 2011). Phishing messages that include personal information taken from the social network account have a massive success rate (Jagatic et al., 2007). This explains the scenario used in the attack number 1 which asks users to register their emails and names to enter a prize draw. Previous studies also stated that phishing messages always include threatening phrases like your account will be closed if you didn't obey to their instructions which exploit the users fear of losing their accounts (Goel et al., 2017; Williams et al., 2017). Thus, this method has also been used in the present study in trick number 5.

When designing the social engineering scenarios, the designs of Facebook posts have been inspired by the study of A Algarni, Xu, and Chan (2015) which used similar tricks to investigate the Facebook source characteristics that influence the user judgements of SE attacks. While the purpose of the current study differs from Algarni et al. (2015) study, the present study scenarios design did not rely on the source of the message like the later. Instead, the focus was intended to be on the posts without displaying the whole Facebook account of the sender to reduce participants' distraction and let them decide based on their self-perceptions, beliefs, and experiences. Since the goal of the present research is to investigate the impact of users' characteristics on their judgement and response to SE attacks, the image and name of the post source have been shaded on purpose to minimise the source

characteristics impact on users' judgement and response. Additionally, due to ethical considerations, all the names and pictures used are fake and unrelated to any known person or application.

Moreover, two low-risk attacks scenarios (trick 3, and trick 6) have been added to the scenario-based experiment to examine if the considered user characteristics affect them differently than their impacts on the high-risk scenarios. For example, short URLs has been used in these low-risk scenarios as it is considered a new method to hide malicious links. Yet, these scenarios are supposed to be low-risk because the short URLs could be either malicious links or safe links. Table 3.1 presents a summary of the considered scenarios of SE attacks. The designed Facebook posts that include these scenarios can be found in Appendix F.

Table 3.1 Summary of the Social Engineering-Based Attacks

Type of Trick	Message	Risk-level
1. Phishing – requesting sensitive information such as the user's email and real name in order to win an iPhone 7 or £100 voucher.	Winner picked tonight Like= free iphone7 Comment= £100 voucher To contact you if you win, Enter your email and name here http://bit.ly/2gno8tj	High
2. Clickjacking with an executable file- a post about a shocking and a very important document that is shown in the post as a pdf file with the mouse pointer positioned on the link and the actual URL in the status bar indicates that the document is an executable file.	I don't want to believe. I just read this document. You must read it. it is very important for all public. Please someone tell me that is a lie.	High
3. Clickjacking- a post that includes a video that direct the user to an ambiguous link. However, this type of link is a low-risk since the link could be either a malicious link or a safe link; it is not clear and not safe to risk and clicks on such links.	Video: The most shocking viedo you will every watch!!	Low
4. Malware- offering an application that allows users to call and message their friends free of charge if they ignore the warning message and give permission to the application to access their profile and contact information.	Download this app. It's works perfect for calling out or messaging. All you need is Wi-Fi.	High
5. Phishing scam- a threatening message pretended to be from Facebook support team asking the user to re-confirm his/her account or blocking the account. The link in the message is the original Facebook site, but the actual URL displayed in the status bar is http://cut.uk/Facebookconfirm-login, which is apparently a phishing site.	Your account is at risk! Please re-confirm your account to avoid plocking, if you are the original owner of this account. Please re-confirm you account by following this link here: https://www.facebook.com/xsrn if you don't confirm our system will automatically block your account and will not be able to use it again.	High
6. Click on a safe link- YouTube video that shows recent news, the link appears in the bottom status bar shows a YouTube short link. Such short URLs could be either malicious links or safe links.	OMG..Tsunami hitting again ☹	Low

3.5.2.2 Instrument Design

The designed instrument consists of a cover letter and four main sections. The cover letter includes information about the purpose of the study and the ethical consent as well as the contact details of the researcher and the supervisor. The first section asks about the

participants' demographics and personality. The second section enclosed questions related to the habitual and socio-emotional constructs while the third section covered the perceptual constructs questions. Finally, the fourth part includes the scenarios of the social engineering attacks and their associated questions.

3.5.2.3 Instrument Translation

Cross-cultural studies usually use back translation approach to translate the study instrument from one language to another (Brislin, 1970). This translation approach proved to provide an accurate translation if the translators are genuinely bilingual and familiar with the study concepts and field (Bracken & Barona, 1991). The process of the back translation approach was conducted in multiple steps as follows. First, the study survey has been translated from English to Arabic by the researcher. Then, the Arabic version has been reviewed and checked by a certified translator. After that, the edited Arabic version has been translated again to English by two bilingual PhD students specialised in computer science at the University of Strathclyde. Finally, the final English copy has been compared with the original instrument to ensure the validity of the translation. Little variations have been noticed which entitled a minor modification to some words in the Arabic version. Both Arabic and English versions have been used as the study has been conducted in Saudi Arabia and participants can choose which language they prefer.

3.5.2.4 Sample Size

A convenience sample was used of university students and staff who agreed to participate in the online questionnaire which was distributed via email. Researchers often rely on the 10 times rule of thumb for estimating the minimum sample size to use partial least squares structural equation modelling (PLS-SEM) as explained by Hair et al. (2017). The present study model has nine independent variables that are intended to predict one dependent variable. Thus, according to the 10 times rule, 10x9=90 respondents is needed which represents the minimum required number of samples. Alternatively, Hair et al. (2017) suggested using a more sophisticated guideline that relies on Cohen (1988) recommendations to calculate the required sample size by using power estimates. In this case, for 9 predictors (which is the number of independent variables in the conceptual model) with an estimated medium effect size of 0.15, the target sample size should be at least 113 to achieve a power level of 0.80 with a significance level of 0.05 (Soper, 2012).

3.5.2.5 Ethical Approval

The ethics committee of the Department of Computer and Information Sciences at Strathclyde University has given ethical consent to conduct this study as illustrated in Appendix G. Participants have been informed that participation in this scenario-based experiment questionnaire involves no risk. All responses will be anonymously registered, confidential, and can be accessed only by the research team. Participants are encouraged to use the contact details which provided in the cover letter if they have any questions.

3.5.3 Pilot Test

After preparing the study instrument, a pilot test has been conducted with the aim to test the reliability and validity of the study instrument. A social media platform has been used as an approach to recruit the pilot study participants. The designed instrument that has been used in the pilot test is similar to the one used in the main study. 80 participants have been volunteered to complete the online questionnaire. All volunteered participants were current Saudi students in UK universities. Selecting participants only from Saudi Arabia was on purpose because it is the targeted population of the main study. Approximately 65% of the participants were female while 35% were male. The reliability and validity of the constructs were tested based on the collected data. The reliability of all constructs in the pilot study was above the required threshold of 0.70. Appendix H presents the full details of the reliability test in the pilot study.

One of the main objectives of conducting this pilot study is to test the validity of the dimensions of the four formative constructs before collecting the primary study data. As recommended by Hair et al. (2017), assessing each indicator weight's significance is critical to determine each indicator's relative importance to form the latent formative construct. Table 3.2 provides a summary of the bootstrapping results (more details about bootstrapping can be found in section 3.5.5.1) which shows that all the formative indicators are significant ($P<0.05$) except for the cybercrime experience indicators on user competence construct where the p-values and the confidence intervals indicate insignificant results. This means that cybercrime experience cannot be considered as a dimension of user competence. This issue has been noticed earlier in the content validity test by the experts (the second phase of this research) which allow building the conceptual model correctly by considering cybercrime experience as an independent factor and not to be included as a dimension of user competence. However, this step has been taken as further validation of the formative constructs' dimensions. Apart from that, no issues have been found in the study instrument. Therefore, the data gathering stage has commenced.

Table 3.2 Pilot Results of Formative Constructs Outer Weights Significance

Construct	Indicators	Outer Weights	Outer Loadings	T-Value	P-Value	95% Bca Confidence Interval		Sig.?
Risk	ST1	0.171	0.792	13.586	<0.001	0.151	0.198	Yes
	ST2	0.180	0.834	13.050	<0.001	0.161	0.213	Yes
	ST3	0.183	0.850	11.619	<0.001	0.159	0.222	Yes
	ST4	0.175	0.812	13.218	<0.001	0.157	0.210	Yes
	LT1	0.136	0.631	7.264	<0.001	0.093	0.165	Yes
	LT2	0.162	0.754	18.169	<0.001	0.149	0.186	Yes
	LT3	0.166	0.772	22.489	<0.001	0.155	0.183	Yes
	LT4	0.132	0.612	7.463	<0.001	0.088	0.159	Yes
Competence	SA1	0.129	0.848	11.508	<0.001	0.113	0.157	Yes
	SA2	0.114	0.751	12.058	<0.001	0.100	0.139	Yes
	SA3	0.105	0.689	11.198	<0.001	0.091	0.128	Yes
	SA4	0.115	0.756	11.910	<0.001	0.099	0.139	Yes
	PA1	0.130	0.857	12.893	<0.001	0.115	0.156	Yes
	PA2	0.110	0.722	11.403	<0.001	0.094	0.133	Yes
	PA3	0.098	0.642	7.780	<0.001	0.077	0.122	Yes
	PA4	0.093	0.611	6.098	<0.001	0.064	0.117	Yes
	SEF1	0.113	0.746	12.418	<0.001	0.100	0.133	Yes
	SEF2	0.112	0.739	13.574	<0.001	0.100	0.132	Yes
	SEF3	0.096	0.633	9.646	<0.001	0.080	0.119	Yes
	SEF4	0.110	0.725	11.206	<0.001	0.094	0.134	Yes
	PE1_It	0.025	0.167	0.816	0.415	-0.035	0.079	No
	PE2_Ph	0.040	0.265	1.390	0.165	-0.029	0.089	No
	PE3_Of	0.042	0.274	1.584	0.114	-0.020	0.082	No
	PE4_Har	0.013	0.083	0.428	0.669	-0.053	0.059	No
Trust	TP1	0.136	0.743	14.892	<0.001	0.120	0.155	Yes
	TP2	0.157	0.855	21.879	<0.001	0.146	0.176	Yes
	TP3	0.157	0.858	20.328	<0.001	0.145	0.176	Yes
	TP4	0.159	0.867	19.742	<0.001	0.146	0.179	Yes
	TM1	0.148	0.809	20.306	<0.001	0.135	0.165	Yes
	TM2	0.153	0.833	24.872	<0.001	0.142	0.167	Yes
	TM3	0.151	0.822	24.832	<0.001	0.141	0.164	Yes
	TM4	0.149	0.811	23.467	<0.001	0.138	0.164	Yes
Motivation	SM1	0.111	0.426	2.828	0.005	0.017	0.168	Yes
	SM2	0.127	0.489	3.290	0.001	0.042	0.190	Yes
	SM3	0.118	0.453	2.704	0.007	0.015	0.181	Yes
	IM1	0.191	0.733	11.846	<0.001	0.162	0.224	Yes
	IM2	0.187	0.720	8.932	<0.001	0.150	0.229	Yes
	IM3	0.173	0.667	9.137	<0.001	0.139	0.210	Yes
	HM1	0.195	0.749	9.385	<0.001	0.157	0.239	Yes
	HM2	0.215	0.828	11.948	<0.001	0.184	0.253	Yes
	HM3	0.178	0.686	8.409	<0.001	0.135	0.219	Yes

3.5.4 Data Collection Procedure

A web-based survey has been designed as an assessment instrument using the Qualtrics online survey tool to examine participants' perception and behaviour toward different threats in a social network context. An invitation email was sent to a number of faculty staff in two universities asking them to distribute the online questionnaire among their students and staff. Participants were told that this study is aiming to investigate participants' behaviour and perception in online social networks but not told that this study was being conducted to measure their victimisation to SE as this might affect the study results by increasing the user suspicious regarding the existence of SE in the proposed scenarios.

Participants who volunteered to contribute in the study were presented with the online questionnaire which consisted of four sections. The first section includes the questions

regarding user demographics, followed by questions about participants' socio-emotion and habits. Then, the third section contains the questions regarding user perception. Finally, the last section comprises social engineering scenarios for the experiments.

In the last section, participants were presented with six images of Facebook posts. Each post includes a type of cyber-attack such as phishing for sensitive information (High-risk Attack 1), clickjacking with an executable file (High-risk Attack 2), malware attack (High-risk Attack 3), and a phishing scam that impersonates a legitimate organisation (High-risk Attack 4). These four high-risk cyber-attacks have been chosen from the most prominent cyber-attacks that occur in social networks (Gao et al., 2011). The remaining two posts were images of low-risk posts as has been mentioned earlier in Section 3.5.2.1. Participants were asked to indicate their response to these Facebook posts, as if they had encountered them in their real accounts, by rating a number of statements such as "I would click on this button to read the file" using a 5-point Likert-scale from 1 "Strongly Disagree" to 5 "Strongly Agree".

3.5.5 Analysis Tools and Methods

One of the main objectives of this research is to develop a new conceptual model to predict users' vulnerability to social engineering in social networks context. Validating this model is a critical step in the present study which needs an extensive and delicate tool to analyse the collected data to support or reject the developed model. This section will describe and justify the selected analysis tools and methods.

3.5.5.1 The Justification for Using Partial Least Squares Structural Equation Modelling

Structural equation modelling is defined as "a collection of statistical techniques that allow a set of relationships between one or more IVs, either continuous or discrete, and one or more DVs, either continuous or discrete, to be examined" (Tabachnick & Fidel, 2013, p.731). Structural equation modelling is a multivariate analysis method that can be treated either as covariance based which is usually referred to as CB-SEM or variance based which is generally referred to as partial least squares structural equation modelling (PLS-SEM). Both types are considered to some extent similar except that CB-SEM is generally considered appropriate analysis method to confirming theories and PLS-SEM is better suited with developing theories and predictions models (Henseler, Ringle, & Sinkovics, 2009).

Conceptual models usually composed of a various number of constructs. These constructs can be classified as a higher order (second order), or a lower order (first order) constructs based on their natures (Wetzels, Odekerken-Schröder, & van Oppen, 2009). The

relationships between higher and lower order constructs can be either formed or reflective which generally defined based on the relation between the higher order construct and their dimensions represented as the lower order constructs (Henseler et al., 2009; Wetzels et al., 2009). Such hierarchical models that include many reflective and formative constructs are known for its complexity (Hair et al., 2017). Partial least squares (PLS) has been widely used to validate models in behavioural studies due to its suitability for dealing with complex predictive models that consist of a combination of formative and reflective constructs (Götz, Liehr-Gobbers, & Krafft, 2010). PLS has shown strength in analysing complex models even with some limitations regarding data normality and sample size as confirmed by many researchers (e.g., Chin, 2010; Hair, Sarstedt, Ringle, & Mena, 2012; Henseler et al., 2009).

The present research used PLS-SEM for many reasons. First, this research follows a sequential exploratory approach to develop a new conceptual model. PLS-SEM is better suited to such studies when the measurement used and the relationships examined are new and have not been satisfactorily tested before (Hair et al., 2017; Henseler et al., 2009). Second, PLS-SEM is more appropriate to be used when the goal of the study is to develop prediction oriented models (Chin, 2010). Third, since the proposed model includes four formative constructs, PLS-SEM is a more appropriate method that can be used to analyse formative constructs when compared to CB-SEM (Chin, 2010; Henseler et al., 2009). While CB-SEM needs construct specification modifications to deal with formative constructs, PLS provides more flexibility with complex hierarchical models (Hair et al., 2017). Finally, PLS is more robust with small sample size and data that considered slightly deviates from normality assumptions (Chin, 2010; Hair et al., 2012; Henseler et al., 2009). For all of these reasons, PLS-SEM is seen to be advantageous to be used over CB-SEM to evaluate the proposed conceptual model.

To evaluate the proposed conceptual model, the statistical package for social sciences (SPSS v24) was used to analyse the descriptive statistical results. In addition, the SmartPLS v3 (Ringle, Wende, & Becker, 2015) software package was used to analyse the model and its associated hypotheses. SmartPLS is considered suitable analysis tool for models that include both reflective and formative constructs. Furthermore, SmartPLS offers a variety of features that could contribute to the assessment of the conceptual model in the current research.

Structural equation modelling consists of two types of assessment models: the measurement model and the structural model (Tabachnick & Fidel, 2013). The measurement model includes all the observed constructs and their indicators while the structural model identifies the relationships among those constructs. Thus, following the recommendation of Henseler et al. (2009) and Hair et al. (2017), two stages of analysis have been conducted to

validate the present study model as presented in Figure 3.3. First, the measurement model has been tested and evaluated and then the structural model assessment has been conducted.

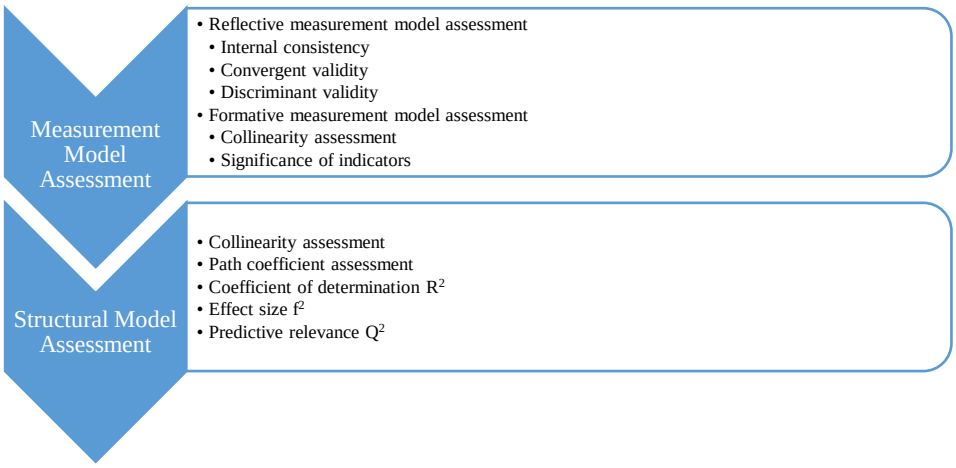


Figure 3.3 Two-Step Assessment Procedure of the PLS-SEM as Suggested by Henseler et al. (2009) and Hair et al. (2017)

Following the two-step assessment procedure, the factors in the measurement model have been assessed with regard to the reliability of the items, internal consistency between items, and the model's convergent and discriminant validity. While to evaluate the structural model, three different procedures have been conducted. First, using the PLS-algorithm to provide standard model estimations such as path coefficient, the coefficient of determination (R^2 values), effect size, and collinearity statistics. Secondly, using a bootstrapping approach to test the structural model relationships significance. In such approach, the collected data sample is treated as the population sample where the algorithm used a replacement technique to generate a random and large number of bootstrap samples (recommended to predefine as 5,000) all with the same amount of cases as the original sample (Henseler et al., 2009). The present study conducted the bootstrapping procedure with 5000 bootstrap samples, two-tailed testing, and an assumption of 5% significant level.

Finally, a blindfolding procedure was also used to evaluate the predictive relevance (Q^2) of the structural model. In this approach, part of the data points are omitted and considered missing from the constructs' indicators, and the parameters are estimated using the remaining data points (Chin, 2010; Hair et al., 2017). These estimations are then used to predict the missing data points which will be compared later with the real omitted data to measure Q^2 value. Blindfolding is considered a sample reuse approach which only applied to endogenous constructs (Henseler et al., 2009). Endogenous constructs are the variables that are affected by other variables in the study model (Götz et al., 2010), such as user susceptibility, involvement, and trust.

3.5.5.2 The Justification For Using Other Statistical Tests

The present research also interested in examining the impact of demographic variables and personality traits on user susceptibility to SE. Using PLS-SEM with binary and nominal variables are possible but not recommended (Hair et al., 2012). As Jakobowicz and Derquenne (2007) pointed out that "When working with continuous data or grades from 1 to 10, PLS does not face any problems, but when working with nominal or binary data it is not possible to suppose there is any underlying continuous distribution". Thus, linear regression analysis, as well as variance tests such as t-test and ANOVA test, have been conducted.

Demographic variables are considered categorical variables. Therefore, the regression test can only indicate if the relationship between particular demographic variable and user susceptibility is significant or not. While to test if different groups of demographics vary in their vulnerability to social engineering, variance tests are needed. Variance tests such as t-test (two groups) and ANOVA (more than two groups) could help identify which group of users are more vulnerable to social engineering.

3.6 Chapter Summary

This chapter explains the methodology that has been followed in this thesis. A sequential exploratory research design with mixed methods (quantitative and qualitative) approach has been adopted with three main phases in the current research. The result of the first phase proposed a user-centric framework that aims to gather the essential perspectives and dimensions of user characteristics that influence users' susceptibility to social engineering in social networks. This chapter has discussed the validation process that has been followed to evaluate the user-centric framework. Chapter 4 and chapter 5 will explain the user-centric framework construction steps and validation results in further detail.

A content validation process has been applied in the second study phase to convert the user-centric framework factors and dimensions to measurable constructs in order to build the conceptual model constructs and relationships. The present chapter explains the content validation procedure while chapter 6 details the process and results of the development and validation for the measurement scales of the study constructs. Chapter 7 presents the conceptual model and its associated hypotheses. A scenario-based experiment has been conducted to empirically test the hypothesised relationships and the prediction ability of the study model. The present chapter has described the evaluation procedures and methods of the proposed conceptual model while the empirical results will be explained in detail in chapter 8.

Chapter 4. USER-CENTRIC FRAMEWORK CONSTRUCTION

4.1 Overview

The present chapter proposes a user-centric framework (UCF) in order to build a cohesive understanding of user vulnerability to social engineering (SE) attack in a social network context. First, the background of the relevant studies that investigated the characteristics of vulnerable users, presented earlier in chapter 2, helped us to elicit the most influential factors. This facilitates developing the UCF, based upon four different perspectives which are: socio-psychological, habitual, perceptual, and socio-emotional. The steps that have been taken to develop the proposed UCF are described in Section 4.2. After that, a comparison of the proposed UCF and the similar and most recent existing models is conducted to identify similarities and differences (Section 4.3). Figure 4.1 summarises the process that has been taken to construct the proposed UCF. Finally, Section 4.4 provides a summary of this chapter.

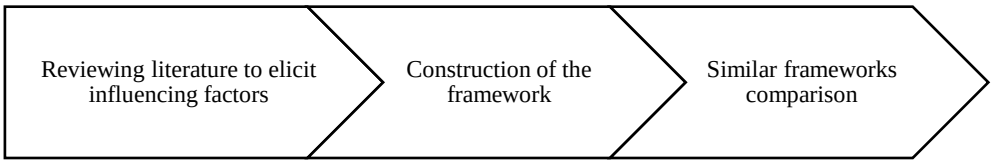


Figure 4.1 Process of Developing the User-Centric Framework

4.2 User Characteristics Framework Construction

Following the literature review on the user characteristics that may influence the user's judgement of online attacks, the present study identifies four critical perspectives to classify user characteristics which are socio-psychological, habitual, perceptual, and socio-emotional. Several attributes and theories have been chosen to develop a UCF. It is worth noting that most of the selected studies were undertaken before 2016 and the present UCF was built and validated later that year. Yet, the proposed UCF has been compared with very recent studies in Section 4.3. Table 4.1 summarises all the attributes that have been extracted from previous empirical research that focused mainly on users' characteristics that influence their susceptibility to social engineering. To construct the framework based on existing studies and theories, the following is a summary of the steps that have been taken.

Table 4.1 Chosen Attributes

Attribute	Author	Attribute	Author
SN frequency of use	(Vishwanath, 2015)	Culture	(Al-Hamar et al., 2010)
SN usage behaviour control		Country-specific factors	
Friendship establishment in SN		Interests	
Concern of privacy		Beliefs	
		Religion	
Individual's trust	(Flores et al., 2014)	Personnel characteristic	
Risk behaviour			
Computer experience at work		Intention to resist	(Flores et al., 2015)
Helpfulness		Security awareness	
Gender		IS policy awareness	
Age		IS training	
Fear		Self-efficacy	
Computer self-efficacy		Computer experience	
		Age	
Commitment	(Workman, 2008b)	Gender	
Trust		Culture	
Obedience			
Reactance		Personality traits	(Halevi et al., 2013)
Age		Gender	
Gender		Facebook activity engagement	
Education		Perceived vulnerability	
Previous victimisation		Internet pessimism	
		Computer expertise	
Gender	(Jagatic et al., 2007)	Privacy settings	
Age			
Education major		Personality traits	(Alseadoon et al., 2015)
		Disposition to trust	
Gender	(Sheng et al., 2010)	Submissiveness	
Age		Email experience	
Anti-phishing education		Email richness	
Familiarity with computer	(Pattinson et al., 2012)	Computer self-efficacy	(Wright & Marett, 2010)
Personality traits		Web experience	
Cognitive impulsivity		knowledge of security policies	
Age		Disposition to trust	
Gender		Perceived risk	
Education level		Suspicion of humanity	
Area of study			
Language		Threat vulnerability	(Workman, 2008a)
		Threat severity	
		Trust	
		Commitment	
		Fear	

4.2.1 Step 1: Selected Attributes Grouped Under Perspectives

In an attempt to build a focused and coherent framework, the selected attributes have been categorised and grouped under four perspectives in regard to the attribute's nature. Repeated attributes have been mentioned once while all the corresponding studies have been cited in the author column. For instance, gender has been reported in 7 different studies (see Table 4.2), age in 6 studies, personality traits, mentioned three times, while each of computer self-efficacy, Trust, fear, education, the area of study, commitment, disposition to trust, and culture has been reported two times. Therefore, the total number of attributes has been reduced from 72 to 51 in this step.

Table 4.2 Attributes Grouped Under Four Perspectives

Perspective	Attributes	Authors
Socio-psychological	Helpfulness Fear Commitment Obedience Reactance Personnel characteristic Personality traits Submissiveness Gender Age Education Email experience Computer experience at work Computer expertise Computer experience Web experience Culture Country-specific factors Religion Beliefs Familiarity with computer Cognitive impulsivity Area of study Language	(Flores et al., 2014) (Workman, 2008b) (Al-Hamar et al., 2010) (Halevi et al., 2013) (Alseadoon et al., 2015) (Sheng et al., 2010) (Jagatic et al., 2007) (Flores et al., 2015) (Workman, 2008a) (Wright & Marett, 2010) (Pattinson et al., 2012)
Habitual	SN frequency of use SN usage behaviour control Friendship establishment in SN Email richness Facebook activity engagement	(Vishwanath, 2015) (Alseadoon et al., 2015) (Halevi et al., 2013)
Perceptual	Risk behaviour Perceived risk Anti-phishing Education Security awareness IS policy awareness IS training Knowledge of security policies Concern for privacy Computer self-efficacy Self-efficacy Previous victimisation Threat severity Intention to resist Threat vulnerability Perceived vulnerability Internet pessimism Privacy settings	(Flores et al., 2014) (Sheng et al., 2010) (Flores et al., 2015) (Vishwanath, 2015) (Workman, 2008b) (Halevi et al., 2013) (Workman, 2008a) (Wright & Marett, 2010)
Socio-emotional	Individual's trust Trust Disposition to trust Interests Suspicion of humanity	(Flores et al., 2014) (Workman, 2008b) (Alseadoon et al., 2015) (Al-Hamar et al., 2010) (Workman, 2008a) (Wright & Marett, 2010)

4.2.2 Step 2: Removing and Merging Overlapping Concepts

When the attributes have been grouped in four perspectives, similar and overlapping terms were obvious, and this allowed for the merging of some terms to form a single factor (see Table 4.3). For example, computer experience, web experience, and email experience are related attributes and can be represented under the single factor 'computer knowledge'. Furthermore, country-specific factors and religion can be represented together by 'culture'. This step converted 51 attributes to 14 factors.

Table 4.3 Attributes Merged into Factors

Perspective	Factor	Attributes	Authors
Socio-psychological	Personality traits	Helpfulness Fear Commitment Obedience Reactance Personnel characteristic Personality trait Submissiveness Cognitive impulsivity	(Flores et al., 2014) (Workman, 2008b) (Al-Hamar et al., 2010) (Halevi et al., 2013) (Alseadoon et al., 2015) (Workman, 2008a) (Pattinson et al., 2012)
	Demographics	Gender Age Education Area of study	(Flores et al., 2014) (Halevi et al., 2013) (Sheng et al., 2010) (Jagatic et al., 2007) (Workman, 2008b) (Flores et al., 2015) (Pattinson et al., 2012)
	Computer knowledge	Email experience Computer experience at work Computer expertise Computer experience Web experience Familiarity with computer	(Alseadoon et al., 2015) (Flores et al., 2014) (Halevi et al., 2013) (Flores et al., 2015) (Wright & Marett, 2010) (Pattinson et al., 2012)
	Culture	Culture Country-specific factors Religion Beliefs Language	(Flores et al., 2015) (Al-Hamar et al., 2010) (Pattinson et al., 2012)
Habitual	Level of Involvement	SN frequency of use SN usage behaviour control Friendship establishment in SN Email richness Facebook activity engagement	(Vishwanath, 2015) (Alseadoon et al., 2015) (Halevi et al., 2013)
Perceptual	Risk perception	Risk behaviour Perceived risk	(Flores et al., 2014) (Wright & Marett, 2010)
	Perceived severity of threats	Intention to resist Threat severity	(Flores et al., 2015) (Workman, 2008a)
	Perceived likelihood of threats	Perceived vulnerability Threat vulnerability Internet pessimism	(Halevi et al., 2013) (Workman, 2008a)
	Security awareness	Anti-phishing Education Security awareness IS policy awareness IS training Knowledge of security policies	(Sheng et al., 2010) (Flores et al., 2015) (Wright & Marett, 2010)
	Privacy awareness	Concern for privacy Privacy settings	(Vishwanath, 2015) (Halevi et al., 2013)
	Self-efficacy	Computer self-efficacy Self-efficacy	(Flores et al., 2014) (Flores et al., 2015) (Wright & Marett, 2010)
	Experience with cybercrime	Previous victimisation	(Workman, 2008b)
Socio-emotional	Trust	Individual's trust Trust Disposition to trust Suspicion of humanity	(Flores et al., 2014) (Workman, 2008b) (Workman, 2008a) (Alseadoon et al., 2015) (Wright & Marett, 2010)
	Motivation	Interests	(Al-Hamar et al., 2010)

4.2.3 Step 3: Substituting and Incorporating Factors to Fit the Study Context

As most of the previous studies were conducted in an email context, some of the elements need to be replaced by contextual factors that would be more related to the social network's environment. For instance, trust in a social network context can include trusting the network provider as well as trusting other members of the network (Dwyer et al., 2007).

Therefore, trust has been replaced by these two factors. Privacy awareness is a crucial factor in social network settings as suggested by (Vishwanath, 2015) while email phishing studies focused only on security awareness. Therefore, the present study will consider social network-related privacy awareness as a factor in the framework along with security awareness.

The success rate of email phishing was found to be higher if the target's interests has been exploited (Al-Hamar et al., 2010). Yet, to use personal interests as a factor to predict behaviour in a social network context, measuring personal motivation to use the network could be more useful. Furthermore, risk perception is a very general term that is defined by ISO (the international organization for standardization) as "stakeholder's (either organization's or individual's) assessment of the outcome of uncertainty on different aspects of objectives" (ISO/IEC 27000, 2018). However, the present research is more concerned with the perceived risk of social network activities. All the perceptual factors will be associated with social network threats. For instance, perceived severity of social network threats, and perceived likelihood of social network threats as presented in the factors' definition in Section 4.2.5.

4.2.4 Framework Construction

Based on the previous classification process, the framework was constructed after converting 72 terms into 15 factors. Figure 4.2 shows the proposed UCF. The next section presents the definition of each factor in detail.

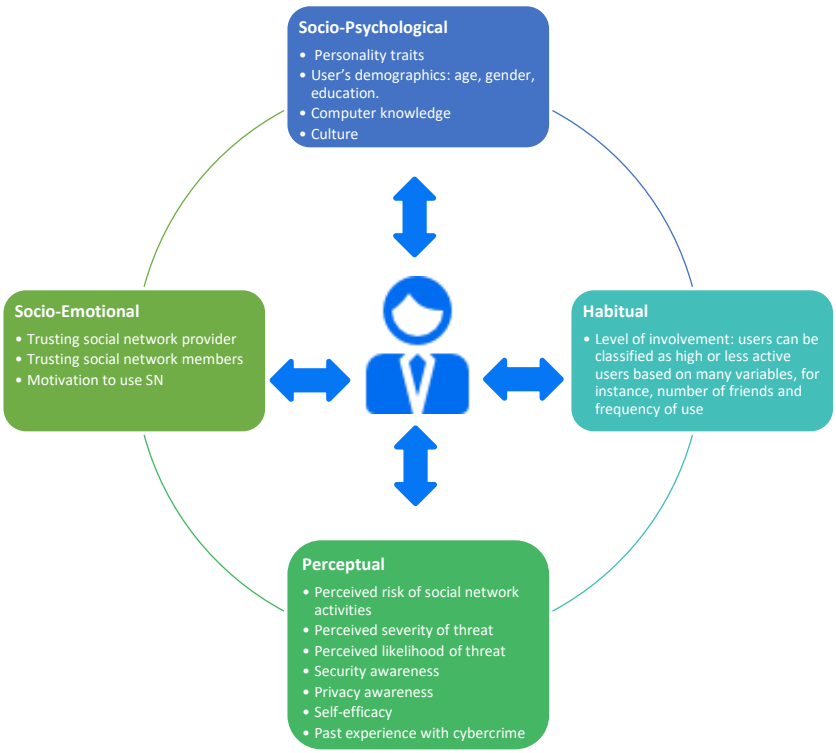


Figure 4.2 User-Centric Framework (UCF)

4.2.5 Factors' Definitions

This section displays the framework's four perspectives and their selected attributes with a brief description of each attribute. In addition, a summary of the selected characteristics' definitions is presented in Table 4.4.

4.2.5.1 Socio-Psychological Variables

Previous research in social engineering indicated that socio-psychological factors are considered one of the main determinants of social engineering victimisation. The following are the most common factors:

a. Personality Traits

According to the big five personality traits theory (Costa & McCrae, 1992), user behaviour can be patterned and categorised in five different traits which are: neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness.

b. User Demographics

The present study considers the importance of each demographic attribute such as age, gender, education as an independent factor that could affects the user's vulnerability.

c. Computer Knowledge

Computer knowledge can be defined as the level of the individual's expertise in using computers. Computer knowledge could be measured by the number of years the individual user has spent using computer-related services such as email and internet services (Flores et al., 2015).

d. Culture

The user's nationality can identify user's culture. Culture has been indicated to play a critical role in deception detection ability of users. Some research in email phishing has taken the first steps toward measuring the impact of culture on users' susceptibility to response to email phishing (Al-Hamar et al., 2010; Alseadoon et al., 2015). However, the role of culture in social engineering victimisation in the environment of social network needs more research. Therefore, the present study chose Saudi Arabia as a new investigation culture.

4.2.5.2 Habitual Variables

a. Level of Involvement

The individual's level of involvement in a social network can be defined as the extent to which a user engages in social network activities (Halevi et al., 2013). Users can be classified as high or less active users in a social network based on many variables, for instance,

the number of friends, the number of subscribed groups, the number of status updates, the frequency of use, and frequency of commenting in other people posts. However, the present study has adopted the famous Facebook intensity scale that has been proposed by Ellison (2007). In the Facebook intensity scale, the following two attributes are considered an indication of user involvement in the network:

- Number of connections: The number of friends the user has in their social network account.
- Frequency of usage: The number of days per week and the number of hours per day that the user usually spends visiting their social network account.

4.2.5.3 Perceptual Variables

This perspective includes all the factors that require the user to engage in interpretation activities or being aware of these activities' boundaries and dimensions. Such as the following:

a. Perceived Risk of Social Networks

Perceived risk can be defined as the extent to which the user is uncertain whether an online action is worthwhile or not (Wright & Marett, 2010).

b. Perceived Severity of Threat

According to the protection motivation theory, when people expect negative consequences, they tend to be more careful and try to implement protection actions (Inouye, 2014). Individual's perception of the threat is a critical factor against SE because if the user is unaware of the severity of the threat and its negative consequences that may happen in a social network, users will feel safe online and may eventually get easily deceived.

c. Perceived Likelihood of Threat

The individual's perception of the likelihood of threats and the possibility of falling victim to SE attacks in social networks can encourage safe practice and reduce vulnerability to social engineering-based attack.

d. Security Awareness

Users' awareness of attitudes and actions that aim to protect themselves from online security threats (Zolait, Anizi, Ababneh, BuAsalli, & Butaiba, 2014).

e. Privacy Awareness

Users' awareness of attitudes and actions in order to protect their personal information online (Bartsch & Dienlin, 2016).

f. Self-Efficacy

This can be defined by the individuals' confidence in their ability to protect themselves against any undesirable online incidents (Wright & Marett, 2010). Previous research suggested that self-efficacy plays a critical role in users' risky behaviour online as an individual with high self-efficacy is less likely to make risky choices online (Milne, Labrecque, & Cromer, 2009).

g. Past Experience with Cybercrime

Peoples' past cybercrime experience has a substantial impact on their perception of risk associated with using online services such as online banking, online shopping, and online social networks (Riek, Bohme, & Moore, 2016). Experience with cybercrime can be measured by asking if the individual has previously faced or fallen victim to any kind of social engineering attacks, such as identity theft and phishing (Bohme & Moore, 2012).

4.2.5.4 Socio-Emotional Variables

a. Trusting Social Network Provider

In reality, trust is considered a critical factor for people's interaction or friendship development. People naturally trust others until their actions prove that they are not trustworthy. Trusting a social network provider can be defined as the extent to which the individual trusts and relies on the social network's service provider to protect their personal information (Dwyer et al., 2007).

b. Trusting Social Network Members

Trusting social network members can be defined as the extent to which the individual believes that other social network members are trustworthy and not harmful (Dwyer et al., 2007).

c. Motivation to Use Social Networks

The present study will assume that motivation to use the social network in addition to other factors can influence users' vulnerability to social engineering-based attacks. Usage motivation is defined as the motivation that causes the individual to engage more in the social network without applying preventive measures (Chen, 2012).

Table 4.4 Summary of Attributes Definitions

Factor	Definition
Personality Traits	User behaviour can be patterned and categorised into five different traits which are: neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness.
User Demographics	The present study considers the importance of each demographic attribute such as age, gender, and education as an independent factor.
Computer Knowledge	The level of the individual's expertise in using computers.
Culture	The user's nationality.
Level of Involvement	The extent to which a user engages in social network activities.
Perceived Risk of SN	The extent to which the user is uncertain whether an online action is worthwhile or not.
Perceived Severity of Threat	The individual's perception of the severity of threats that might be occurred in social networks and the negative consequences of that threats.
Perceived Likelihood of Threat	The individual's perception of the likelihood of threats and the possibility of falling victim to social engineering attacks in social networks.
Security Awareness	Users' attitude and actions that aim to protect themselves from online security threats.
Privacy Awareness	Users' attitude and actions in order to protect their personal information online.
Self-efficacy	The individuals' confidence in their ability to protect themselves against any undesirable online incidents.
Experience with Cybercrime	Has the individual previously faced or fallen victim to any kind of social engineering attacks such as identity theft and phishing.
Trust in Provider	The extent to which the individual trusts and relies on the social network's service provider to protect their personal information.
Trust in Members	The extent to which the individual believes that other social network members are trustworthy and not harmful.
Motivation to Use SN	It is defined as the motivation that causes the individual to engage more in social networks without conducting preventive measures.

4.3 Comparison of Similar Frameworks

Similarly motivated and empirically tested frameworks in the literature, in email or social network environments, are reviewed in Section 4.3.1. In an attempt to indicate the similarities and differences between the most recent models and the proposed UCF, a detailed comparison is presented in Section 4.3.2.

4.3.1 Similar Frameworks' Review

Predicting user susceptibility to social engineering victimisation has been an area of focus for many years. Various frameworks have been proposed in the past with the objective to find out the most influencing factors to users' decisions in order to prevent the user from falling for social engineering-based attacks in different context. The present study will analyse those frameworks based on the selected attributes to develop a robust UCF.

4.3.1.1 In Email Environment

a. SCAM

The suspicion, cognition, and automaticity model (SCAM) that has been proposed by Vishwanath et al. (2016) focused on examining the effects of four main factors in email phishing vulnerability. These primary factors are cyber-risk beliefs, cognitive-information processing, email habits, and deficient-self regulation. The linkage between these four factors has given a prediction of the user suspicious of email phishing.

b. Alseadoon and Colleagues Model

Alseadoon et al. (2015) propose a model based on deception detection theory to measure user characteristics that influence their email phishing detection behaviour. The model includes limited and focused attributes such as personality trait, disposition to trust, submissiveness, email richness, and email experience.

c. Halevi and Colleagues Framework

This framework provided by Halevi et al. (2013) concentrates on the relation between a specific personality trait and susceptibility to email phishing. Likewise, the framework examined the effects of the perceived likelihood of internet threats as well as the user behaviour on Facebook such as number of posts and adjusting the privacy settings on susceptibility to email phishing. Among the demographic variables, the study examined the gender and computer expertise effects on the phishing response probability. The results revealed that there were significant effects of gender, personality trait, and user Facebook activity on predicting email phishing response. Yet, the likelihood of being phished, as well as computer expertise, were not found to predict the user behaviour toward email phishing attacks.

d. Integrated Information Processing Model

This model proposed by Vishwanath et al. (2011) examined the relationships between media habits, email load, domain-specific knowledge, and self-efficacy and their role in susceptibility to email phishing. They found that habitual pattern and email load both have a strong significant impact on email phishing victimisation, while self-efficacy and domain-specific knowledge had a mitigating role in phishing vulnerability.

e. Wright and Marett Model

This model has covered a variety of behavioural variables and investigated their effects in increasing user vulnerability to comply with phishing requests (Wright & Marett, 2010). The factors under study have been categorised as experiential variables that include self-efficacy, web experience, and security knowledge and dispositional variables that include disposition to trust, perceived risk, and suspicion to humanity. Among these variables, the study results revealed that self-efficacy, web experience, security knowledge, as well as suspicion level, could decrease the user's vulnerability to email phishing attacks.

4.3.1.2 In Social Network Environment

a. Algarni and Colleagues Model

Algarni et al. (2017) propose a model that investigates the impact of different source characteristics on vulnerability to social engineering requests in the Facebook platform. The

model indicated four dimensions of source credibility that humans usually rely on when deciding to accept or decline a risky request in the social network. In addition to the identified Facebook-based source characteristics, the model also proposes four demographic factors believed to influence susceptibility to social engineering, which are age, gender, security knowledge, and time since joining the network.

b. Saridakis and Colleagues Model

The model proposed by Saridakis et al. (2016) was concerned with describing individuals' behaviour on the online social network based on perception from the theory of reasoned action and theory of planned behaviour. The model proposes that peoples' perception of risk, their perception of control over information, their technical IT skills, as well as their usage habits, can affect their attitudes, intentions and behaviour in a social network environment.

c. Vishwanath's Habitual Model

Vishwanath's (2015) model investigated the role of Facebook habitual use in the user's vulnerability to Facebook phishing attacks. The model factors under investigation are the frequency of use, number of friends, deficient self-regulation, attitudinal commitment, and privacy concerns. The study results indicated that frequency of Facebook use, having a large social network, and deficient self-regulation are the main predictors of individual victimisation to phishing attacks on Facebook.

d. Benson and Colleagues' Study

The study by Benson, Saridakis, and Tennakoon (2015) investigates cybercrime victimisation in social network platforms among higher education institutions and the reasons behind the delayed adoption of using social networks platforms in educational institutions. Their study focuses on the usage motivation that encourages students and non-students to engage in social networks and found no significant difference of usage between students and non-students and around 60% of participants using social media for socialising and gathering information motives. However, the study did not investigate whether usage motivation has an impact on cybercrime victimisation. Furthermore, the study found that non-student social network users are more likely to be victims of cybercrime compared to university student users.

e. Iuga and Colleagues' Study

Key factors that influence peoples' ability to distinguish between legitimate and phishing webpages have been investigated in a study conducted by Iuga et al. (2016). Their

research focused on examining the effect of different demographics on phishing susceptibility. Among many tested factors, gender and experience of using computers have a significant impact on people's detection scores. As all the images used to test responses to phishing attacks are based on the login page of Facebook, this study has been considered directly relevant to the social network context and is considered in the frameworks' comparison in the next section.

4.3.2 Frameworks Comparison

Similarly motivated and empirically tested frameworks in the literature, in email or social network environments, have been reviewed to indicate the similarity and differences between them (as presented in Table 4.5 where (√) indicates inclusion of the attribute in the considered model). From the comparison, it was clear that researchers in the field have given the socio-psychological factors great attention. In contrast, most research has limited consideration of perceptual and habitual variables, while the socio-emotional perspective and its dimensions have never been investigated before in relation to their effect on social network victimisation. Yet, in an email environment, Alseadoon et al. (2015) and Wright and Marett (2010) have examined people's disposition to trust others as a personality factor and its impact on email phishing.

In social network models, some variables, such as personality traits, culture, and past experience with cybercrime, have rarely been considered for their influence on victimisation. Furthermore, in the perceptual perspective, the individual's estimation of the severity and likelihood of threats and their privacy and security awareness might be considered insufficiently investigated in previous models. Two models have indirectly studied privacy awareness and its relation to phishing vulnerability. Vishwanath (2015) model has investigated the individual's privacy concerns that indirectly refer to privacy awareness, and has found this to be not significant. Likewise, Halevi et al. (2013) model investigated the privacy awareness indirectly through examining the user's adjustment of Facebook's privacy settings as a pattern of the user-Facebook activity, which proved to be a significant predictor to phishing vulnerability.

The need for a multidimensional perspective has emerged after conducting this comparison. Many important attributes should be considered when examining user vulnerability to social engineering victimisation. In contrast to the existing frameworks, the proposed framework affords a more holistic and robust user-centric model that provides a starting point for understanding user susceptibility to social engineering in social networks.

Table 4.5 Comparison of Similar Frameworks in Email and Social Network Contexts

Attributes	**Context**									
	Social Network Environment					**Email Environment**				
Model (Year)	(Algarni et al., 2017)	(Saridakis et al., 2016)	(Vishwanath, 2015)	(Benson et al., 2015)	(Iuga et al., 2016)	(Vishwanath et al., 2016)	(Alseadon et al., 2015)	(Halevi et al., 2013)	(Vishwanath et al., 2011)	(Wright & Marett, 2010)
Socio-psychological										
Personality trait							√	√		
Age	√			√	√		√			
Gender	√				√			√		
Education				√	√					
Computer knowledge	√	√			√		√	√	√	√
Culture					√					
Habitual										
Level of involvement in SN		√	√			√		√	√	
Perceptual										
Perceived risk		√				√				√
Perceived severity										
Perceived likelihood								√		
Security awareness	√									√
Privacy awareness			√					√		
Self-efficacy									√	√
Cybercrime experience										
Socio-emotional										
Trusting SN provider										
Trusting SN members										
Motivation to use SN										

4.4 Chapter Summary

The proposed user-centric framework is built based on the integration between previous literature and relevant theories after conducting a review study of the existing user characteristics frameworks and the related theories, which facilitate the development of the proposed framework. Proposing the user-centric framework and their attributes and dimensions answered the first sub-question (RQ1.1) of the research question 1 which is as follows:

RQ1.1: What are the dimensions and attributes of the user characteristics framework that would influence user susceptibility to social engineering on social networking sites?

The next chapter discusses the process conducted to evaluate and validate the user-centric framework. A mixed-methods expert review has been chosen as an approach to validate the framework attributes to ascertain if there are any critical factors not included in the framework which will be discussed in detail in the following chapter.

Chapter 5. USER-CENTRIC FRAMEWORK VALIDATION

5.1 Overview

The present chapter demonstrates the approach used to validate the proposed user-centric framework (UCF). It describes the experts' evaluation method, design, and analysis that aim to measure experts' agreement and acceptance toward the framework's dimensions and attributes. Section 5.2 presents the approach that has been used to validate the framework components. Section 5.3 provides details of the participating experts' profiles. Section 5.4 describes the analysis techniques that have been used on the collected data along with the results of the validation study. Section 5.5 presents the amendments and the improvements that have been applied to the UCF as a result of the experts' evaluation. Finally, Section 5.6 draws conclusions from this chapter.

5.2 The Validation Approach

The present study adopted expert reviews as a mixed methods approach to validate the proposed UCF with an objective to confirm or modify the proposed UCF. This approach is important as a means to evaluate the dimensions and attributes of the newly developed framework to get proper feedback and validate the proposed framework in the study context.

The study detailed in the present chapter was composed of two major parts: quantitative and qualitative. In the quantitative section, participants were presented with the proposed framework, asked to read each factor's description carefully and rate the importance of the factors in terms of their effects on users' judgements of social engineering (SE) attacks in social networks. The qualitative part includes open-ended questions that aim to gather the experts' opinions and recommendations toward improving the proposed framework.

Two rounds of experts' review were conducted in the present study to increase the reliability of results by using the inter-rater reliability approach. This approach aims to identify the degree to which the results obtained from both rounds of the evaluation are stable and yield similar results, even though different experts have participated in each round (Aguti et al., 2014). The results of the two rounds have been compared to examine whether there are any differences between the two groups regarding the importance of the framework's factors to identify users' ability to detect online threats. Figure 5.1 summarises the process that has been adopted to validate the proposed UCF. More details on the validation procedure and the analysis techniques used in this chapter can be found in chapter 3.

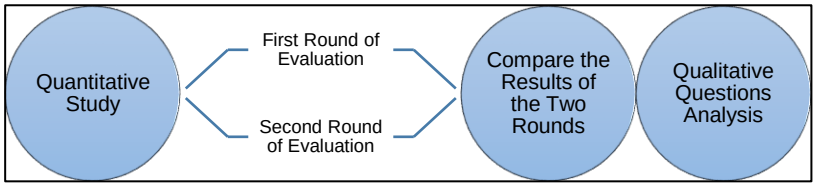


Figure 5.1 Framework Validation Method

5.3 Experts' Profiles

In the two rounds of expert review, participants were diverse in terms of gender, age, education level, and expertise (Table 5.1). As the open-ended questions part was optional, only 11 experts volunteered to complete this part of the questionnaire. Table 5.2 presents the demographics of the experts who participated in the qualitative part of the study. It is worth noting that although experts have different expertise level, their opinion and judgment of the framework factors have the same priority and importance as long as the participants have sufficient experience.

Table 5.1 Experts' Demographics

Demographic		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	17	65.4	65.4	65.4
	Female	9	34.6	34.6	100.0
	Total	26	100.0	100.0	
Age	18-24	1	3.8	3.8	3.8
	25-34	10	38.5	38.5	42.3
	35-44	15	57.7	57.7	100.0
	Total	26	100.0	100.0	
Education Level	High school	3	11.5	11.5	11.5
	Bachelor	5	19.2	19.2	30.8
	Master	11	42.3	42.3	73.1
	PhD	6	23.1	23.1	96.2
	Other	1	3.8	3.8	100.0
	Total	26	100.0	100.0	
Expertise	1-5	6	23.1	23.1	23.1
	6-10	7	26.9	26.9	50.0
	11-15	9	34.6	34.6	84.6
	More than 15	4	15.4	15.4	100.0
	Total	26	100.0	100.0	

Table 5.2 Qualitative Study Experts' Demographics

Expert number	Age	Gender	Education	Expertise (years)
Expert 1	35-44	Male	PhD	Over 15
Expert 2	35-44	Male	PhD	11-15
Expert 3	35-44	Female	PhD	Over 15
Expert 4	35-44	Female	PhD	11-15
Expert 5	35-44	Female	Master	11-15
Expert 6	25-34	Male	Master	6-10
Expert 7	25-34	Female	Master	6-10
Expert 8	25-34	Female	Master	6-10
Expert 9	25-34	Male	Master	1-5
Expert 10	25-34	Male	Bachelor	1-5
Expert 11	25-34	Male	Bachelor	1-5

5.4 Agreement upon the Framework's Factors

Participants were provided with a list of the factors that are included in the framework and were asked to rank them in relation to their effects on users' poor judgements of social engineering-based attacks in social networks, using a Likert-scale from 1 "Not important" to 5 "Very important". This evaluation aims to help eliminate factors considered unimportant from the framework. According to the Likert-scale, any item with an average of less than three is regarded as less important and will be removed from the framework.

In order to measure the agreement level on the framework factors, a sample t-test was carried out. This would determine the importance of each factor and determine whether to keep it or remove it from the framework. Table 5.3 describes the mean from the five-point Likert-scale and the corresponding decision.

Table 5.3 The Scale Mean Description

Mean	Attitude	Description
1.00-1.79	Not important	The item must be excluded from the framework.
1.80-2.59	Slightly important	
2.60-3.39	Moderately important	Item needs revision to be included in the framework (if the item mean is less than 3, exclude the item from the framework).
3.40-4.19	Important	The inclusion of this item is essential for the framework.
4.20-5.00	Very important	

Before starting the validity stage, the data went through several screening steps that will be discussed in further detail in the next subsection.

5.4.1 Data Screening Approach

In self-administered questionnaires, the data has to be checked for any wrong or improper entries. All data should be reviewed before starting the analysis phase. Accordingly, the data has been reviewed as follows.

5.4.1.1 Missing Values

The data has been checked for any missing values. One participant response from the first round of the expert review was removed from the test as the participant missed five sequence items in the rating question, indicating that this particular participant had decided not to complete the questionnaire.

5.4.1.2 Checking the Normality of Distribution

The normality of the data can be checked by two statistical measures, either Kolmogorov-Smirnov test or Shapiro-Wilk, as shown in Table 5.4. The present study relied upon the Shapiro-Wilk test to check the normality of the data as this is considered more

efficient when used with small samples (Razali & Wah, 2011). Data was found to be normally distributed (sig.>0.05) except for the habitual dimension (sig. =.038) in the first round and socio-emotional (sig. =.019) in the second round which were considered slightly deviated from normality. For a graphical representation of the normality of distribution test, the Q-Q plots can be found in Appendix I.

Table 5.4 Tests of Normality

Group Number	First Group						Second Group					
	Kolmogorov-Smirnov[a]			Shapiro-Wilk			Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.	Statistic	df	Sig.	Statistic	df	Sig.
Total_SocioPsychological	.127	14	.200*	.935	14	.363	.262	12	.022	.903	12	.172
Total_Habitual	.205	14	.115	.867	14	.038	.199	12	.200*	.869	12	.064
Total_Perceptual	.120	14	.200*	.966	14	.816	.147	12	.200*	.899	12	.156
Total_SocioEmotional	.157	14	.200*	.942	14	.446	.365	12	.000	.827	12	.019

*. This is a lower bound of the true significance.
a. Lilliefors Significance Correction

5.4.1.3 Careless Responses

In order to check for careless responses, the "user's height" was added as a bogus item to the socio-psychological item set as having an effect on the user's detection ability of online attacks. This item is clearly not important but has been used to reveal inattentive responses. Results showed that all respondents in both phases were giving sufficient attention and ranked the item as "Not important", with means 1.7 and 1.5 respectively.

5.4.1.4 Reliability of the Test

Cronbach's AlphA has been measured to test the internal consistencey of the factors on each perspective. Cronbach's AlphA is a relaibility measure that indicates the extent to which a set of items are related as a group (Hair, Black, Babin, & Anderson, 2010). Table 5.5 shows the reliability test results for both study phases. Cronbach's Alpha for all perspectives was above 0.5 except for the socio-emotional perspective.

Table 5.5 Reliability Statistics

Group number	Perspective	Cronbach's Alpha	Number of Items
1	Socio-Psychological	0.816	6
	Habitual	0.990	2
	Perceptual	0.728	7
	Socio-Emotional	0.549	3
2	Socio-Psychological	0.671	6
	Habitual	0.933	2
	Perceptual	0.893	7
	Socio-Emotional	0.399	3

According to the socio-emotional perspective in the second round, Cronbach's Alpha was only 0.399. Therefore, trusting items should be separated from the motivation item to increase the reliability to 0.855 as observed in the test in Table 5.6. This implication is also

supported by the findings from the expert qualitative study, and this will be discussed further in the next section.

Table 5.6 Socio-Emotional Reliability

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
TrustP	7.667	2.061	0.410	-0.059
TrustM	7.500	1.909	0.535	-0.317
Motivation	8.500	3.545	-0.090	0.855

5.4.2 One-Sample T-Test

After screening and checking, the collected data was ready for the statistical tests. One sample t-test was conducted with the aim of revealing the sample agreement level of each item and thereby determining whether to include or exclude this item from the framework. Items with a mean less than 3 are considered not important and must be excluded from the framework, as detailed earlier in Table 5.3. This decision can be taken after establishing the test hypotheses: H0: the null hypothesis ($\mu=\mu0$); there is no significant difference between the sample mean, and the population mean; which indicates that the mean of each framework factor is equal to 3. H1: the alternative hypothesis ($\mu\neq\mu0$); there is a significant difference between the sample and population mean; which indicates that the factor mean is not equal to 3.

To test these hypotheses alpha ($\alpha=0.05$) has been chosen as support H0 if the item's sig. value is greater than alpha (no difference in means). Support H1 if the item's sig. value is less than or equal alpha (there is a difference in means).

Table 5.7 summarises the one sample t-test results. Generally, the t-test results show that all of the framework's selected factors are considered important in this round. In the following section, each theme will be analysed separately.

Table 5.7 One-Sample T-Test (First Group)

Factor	Sig.	Mean	Attitude	Hypothesis	Factor	Sig.	Mean	Attitude	Hypothesis
Per_T	.002	4.14	Important	Alternative	**Severity**	.165	3.43	Important	Null
Age	.003	4.14	Important	Alternative	**Likelihood**	.045	3.64	Important	Alternative
Gender	.671	3.14	Moderately important	Null	**Sec_aware**	.000	4.43	Very important	Alternative
Education	.000	4.57	Very important	Alternative	**Priv_aware**	.015	4.07	Important	Alternative
Comp_K	.000	4.50	Very important	Alternative	**Self-efficacy**	.045	3.64	Important	Alternative
Culture	.000	4.14	Important	Alternative	**CCEXP**	.008	4.07	Important	Alternative
Num_Con	.045	3.64	Important	Alternative	**TrustP**	.009	3.93	Important	Alternative
Frq_use	.045	3.64	Important	Alternative	**TrustM**	.002	4.07	Important	Alternative
Risk	.003	4.00	Important	Alternative	**Motivation**	.055	3.57	Important	Null

5.4.2.1 Findings and Discussion

a. Socio-Psychological Attributes

As shown in Table 5.7, the significance value in each of the socio-psychological items is less than alpha (α=0.05). Therefore, the null hypothesis will be rejected, except for the gender item. In this case, the alternative hypothesis will be rejected, and the null hypothesis will be accepted. However, the statistical mean for this item is higher than the population mean (μ0=3) and has been ranked as moderately important in the scale, which makes this item hard to exclude from the framework. Surprisingly, the experts did not consider gender as a critical determinant, a result that conflicts with many previous studies (Algarni et al., 2017; Halevi et al., 2013; Iuga et al., 2016). For instance, the experimental study of Algarni et al. (2017) indicated a strong correlation between gender and response to social engineering attacks in social network contexts.

Moreover, Figure 5.2 indicates that education has the highest rank among other considered factors. This result conflicts with a previous study which argued that the level of education is not significantly related to phishing victimisation (Iuga et al., 2016). But most importantly, when comparing university students with people from outside higher education (Benson et al., 2015), both behave similarly in social networks. Yet, the study found that students are less likely to fall victim to cyber-attacks.

Computer knowledge is considered one of the highest rated factors in the experts' assessment (Figure 5.2). Yet, among many studies (Halevi et al., 2013; Iuga et al., 2016; Saridakis et al., 2016; Vishwanath et al., 2011; Wright & Marett, 2010) that have empirically tested the impact of the Internet and computer knowledge in preventing users from getting phished, only two studies (Iuga et al., 2016; Wright & Marett, 2010) found this relationship to be significant. This contradictory result might imply that users' Internet or computer knowledge is a very general concept whose impact on safe or risky behaviour could be hard to measure. In the qualitative study, Expert 5 mentioned that as the targets of the attacks are social network users, there is no need to measure their computer knowledge and instead, measuring the social network literacy is more relevant. Another participant, Expert 6 had a similar view as he mentioned that computer knowledge is not important if Internet security and privacy awareness are measured, as all these attributes are related to each other and could be merged in one construct. Furthermore, Expert 9 stated that nowadays, social network users generally have a basic knowledge of computer usage, but their problem lies with their knowledge of computer security.

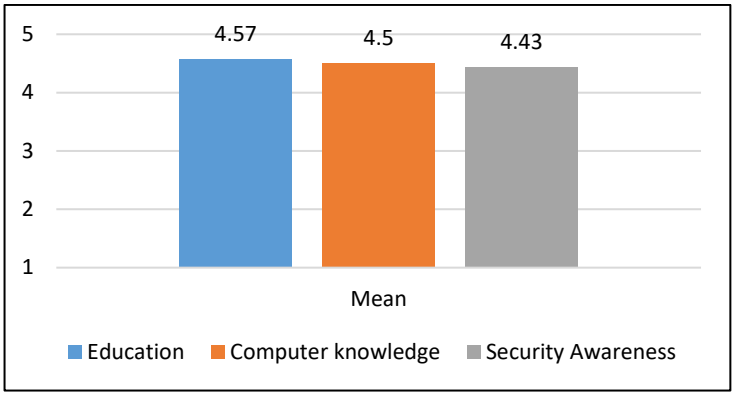


Figure 5.2 The Three Highest Rated Factors

b. Habitual Attributes

It is clear from Table 5.7 that the significance value is less than .05 for all habitual factors. Therefore, the research will reject the null hypothesis and accept the alternative hypothesis. The experts' evaluation revealed that habitual factors are on the importance side to include in the framework. This supports previous findings that presented the critical role of the involvement level of the user on the phishing vulnerability both in the email context (Halevi et al., 2013; Vishwanath et al., 2016, 2011), or in the social network context (Saridakis et al., 2016; Vishwanath, 2015).

c. Perceptual Attributes

The survey results revealed that the perceptual factors are generally crucial factors to consider in relation to user susceptibility to social engineering. Perceptual attributes have not been studied thoroughly before in social network settings. Table 5.7 shows that for all the perceptual factors the null hypothesis will be rejected, and the alternative hypothesis will be accepted as (sig. <0.05) except for the perceived severity the null hypothesis will be accepted as (sig. >0.05). Yet, the perceived severity of threat's mean is still on the importance side, which means it must be included in the framework.

Results shown in Figure 5.2 indicate the importance of security awareness, which has been proven to be significant in previous empirical studies either in an email setting (Wright & Marett, 2010), or a social network environment (Algarni et al., 2017). This importance has been emphasised by the answer of Expert 2 in the qualitative part of the study as he stated that some of the perceptual perspective attributes, such as self-efficacy, security, and privacy awareness, are very critical and can represent the user's defensive ability.

Moreover, perceived severity of threat was given the lowest rank in the experts' assessments, with mean only 3.4 which opposes the findings that this factor is critical in determining the individual's behaviour toward online risks (Alqarni, Algarni, & Xu, 2016;

Workman et al., 2008). Both studies used self-administered questionnaires to measure the severity of threat which might be considered a common way to gauge the individual's perceived threat. Another explanation for the low rank given to perceived severity of threat has been proposed by Expert 1 who suggested that severity of threat and the likelihood of threat could be considered as a multi-attribute that provides an assessment of the user's risk perception. Likewise, Expert 4 commented that user expectation of the threat's occurrence and their perception of risks associated with using the social network are similar and can be combined. The rating results show very close means between the likelihood of threat and the perceived risk which supports Expert 4's comment.

d. Socio-Emotional Attributes

Unlike the context of email, social network members play a vital role in users' trust. Table 5.7 shows that trusting the social network members is the factor ranked highest by the experts as causing users to judge social engineering-based attacks in a social network context poorly. Furthermore, people tend to rely on social network providers to protect them against privacy and security threats, which explains their trusting attitude online. With significant level less than 0.05, the null hypothesis will be rejected while the alternative hypothesis will be accepted for all the factors in this dimension except for motivation where the null hypothesis will be accepted (sig. = 0.055).

The socio-emotional factors, trust in social networks and usage motivation were ranked as important by the experts, and this reflected the gap in the literature, as these two factors have never been encountered in previous frameworks. Although Workman (2008b), Alseadoon et al. (2015), and Wright and Marett (2010) have studied the individual's disposition to trust as a factor to affect the user vulnerability to email phishing, they did not reach the same conclusion. Workman (2008b) and Alseadoon et al. (2015) studies found that individuals who are more trusting would be more vulnerable to social engineering than others. In contrast, Wright and Marett (2010) research found the relationship between trust and deception success to be not significant.

Yet, in this study, two types of trust have been proposed, trusting the social network's provider and trusting the social network's members, which are more specific to the context of social networking. However, Expert 3 suggested combining these two types of trust in one construct. Expert 8 also recommended splitting the motivation factor into multiple sub-factors as there are various types of motivations that persuade users to engage more in social networks. Thus, this study proposes trust as a multi-dimensional construct that includes provider trust and member trust. This also confirms the previous findings of the reliability tests for the second

group that the Cronbach alpha will be raised from 0.399 to 0.855 if the motivation item is deleted and only two types of trust remain.

5.4.3 Independent Samples T-Test

In order to increase the reliability of the framework's validation and the results of the first expert's review, another expert's review phase has been conducted with different experts. An independent samples t-test was performed to examine whether there is a difference between the two groups in the study sample. The grouping variables used in this test are nationality and gender. Therefore, the means of the framework's items have been compared between the multi-national experts' group (first expert review phase) and Saudi experts' group (second expert review phase) to identify any impact of cultural differences on the results, and then between male and female to detect the presence of gender differences. Table 5.8 presents the descriptive statistics of the results of both tests.

To conduct the independent samples test, two steps have been considered. First, testing the homogeneity of variance; using Levene's test for equality of variances. The hypotheses for Levene's test are as follows:

- Support the null hypothesis (H0): if the Levene's test p-value is greater than 0.05 which means the variances of the two groups are equal (equal variances assumed).
- Support the alternative hypothesis (H1): if the Levene's test p-value is less than or equal to 0.05 which means the variances of the two groups are not equal (equal variances not assumed).

The second test step was testing means differences. As can be seen from Table 5.9, the output of the t-test includes two rows: equal variance assumed and equal variance not assumed. The independent samples t statistic is calculated differently in these two rows. Therefore, depending on the level of the variance from the first step the appropriate result will be read from the table. To test the means differences, alpha (α=0.05) has been chosen as support H0 if the significance of the t-test is greater than alpha (no difference in means). Support H1 if the significance of the t-test is less than or equal alpha (there is a difference in means).

Table 5.8 Descriptive Statistics (Culture, Gender)

	Group_no	Culture			Gender		
		N	Mean	STDEV	N	Mean	STDEV
Per_T	group 1	14	4.14	1.1	17	3.94	0.97
	group 2	12	3.75	0.62	9	4	0.87
Age	group 1	14	4.14	1.17	17	3.94	1.2
	group 2	12	3.5	1.31	9	3.67	1.41
Gender	group 1	14	3.14	1.23	17	3.06	1.3
	group 2	12	3.08	1.38	9	3.22	1.3
Education	group 1	14	4.57	0.51	17	4.29	0.85
	group 2	12	3.83	0.94	9	4.11	0.78
Comp_K	group 1	14	4.5	0.65	17	4.53	0.8
	group 2	12	4.33	0.98	9	4.22	0.83
Culture	group 1	14	4.14	0.66	17	3.71	1.1
	group 2	12	3.25	1.36	9	3.78	1.2
Num_Con	group 1	14	3.64	1.08	17	3.18	1.24
	group 2	12	3.42	1.38	9	4.22	0.83
Frq_use	group 1	14	3.64	1.08	17	3.29	1.16
	group 2	12	3.92	1.31	9	4.67	0.5
Risk	group 1	14	4	1.04	17	3.76	1.15
	group 2	12	4	1.04	9	4.44	0.53
Severity	group 1	14	3.43	1.09	17	3.29	1.26
	group 2	12	3.75	1.29	9	4.11	0.78
Likelihood	group 1	14	3.64	1.08	17	3.47	1.18
	group 2	12	3.5	1.17	9	3.78	0.97
Sec_aware	group 1	14	4.43	1.16	17	4.41	1.23
	group 2	12	4.58	1	9	4.67	0.71
Priv_aware	group 1	14	4.07	1.44	17	4.06	1.43
	group 2	12	4.33	1.15	9	4.44	1.01
Self-efficacy	group 1	14	3.64	1.08	17	3.53	1.18
	group 2	12	3.92	1.08	9	4.22	0.67
CCEXP	group 1	14	4.07	1.27	17	4.06	1.43
	group 2	12	4	1.35	9	4	1
TrustP	group 1	14	3.93	1.14	17	3.76	1.15
	group 2	12	4.17	1.03	9	4.56	0.73
TrustM	group 1	14	4.07	1.07	17	3.94	1.14
	group 2	12	4.33	0.98	9	4.67	0.5
Motivation	group 1	14	3.57	1.02	17	3.24	1.03
	group 2	12	3.33	1.07	9	3.89	0.93

5.4.3.1 Findings and Discussion

a. Culture Comparison

To examine if the experts' culture or nationality had an effect on the framework's factors' validation, independent samples t-test have been conducted on two different groups. While the first group includes information security experts from various nationalities, the second group comprises only Saudi experts. Both groups have similar demographics, such as gender, age, and education level. Table 5.9 shows the independent samples t-test results.

It can be seen from Table 5.9 that the Levene's test p-value for most of the items is greater than alpha (sig.>0.05), which means that the null hypothesis is supported and the variances of the two groups are equal. However, one item that has rejected the null hypothesis is culture. Therefore, the alternative hypothesis is supported for this item, as the variances of the two groups are not equal and indicate that the homogeneity of the variance has been violated. Yet, the independent samples t-test includes t statistics based on both assumptions

(equal variances assumed, and equal variances not assumed). Thus, when comparing the means in the second step of the t-test for the culture item, we must rely on the t statistics that assumed not equal variances.

When comparing the means in the second part of the t-test, it was clear that most of the items supported the null hypothesis (sig.>0.05) as there were no differences in means between the two groups, except for one item which is education (sig. =.018). For this item, there was a difference in means between the two groups as the significance value was less than 0.05. Therefore, the alternative hypothesis has been supported. The difference of opinion here was on the importance level of the education factor, which causes the difference in means between the two groups. Yet, both groups have rated education as being on the importance side to be included in the framework. Furthermore, there was an agreement among experts in both groups with regard to the low importance of gender differences in the user's poor judgement of social engineering-based attacks in social networks. Generally, all items in both groups were ranked on the importance side, which means that both groups of experts have confirmed the framework's items.

Table 5.9 Independent Samples T-Test (Culture)

		Levene's Test		t-test for Equality of Means		Supported hypothesis			Levene's Test		t-test for Equality of Means		Supported hypothesis
		F	Sig.	t	Sig.				F	Sig.	t	Sig.	
Per_T	Equal variances assumed	2.96	.098	1.095	.284	Null	Severity	Equal variances assumed	.874	.359	-.690	.497	Null
	Equal variances not assumed			1.141	.267			Equal variances not assumed			-.681	.503	
Age	Equal variances assumed	.181	.674	1.321	.199	Null	Likelihood	Equal variances assumed	.491	.490	.324	.749	Null
	Equal variances not assumed			1.309	.204			Equal variances not assumed			.322	.751	
Gender	Equal variances assumed	.345	.562	.116	.908	Null	Sec-Awar	Equal variances assumed	.174	.680	-.362	.721	Null
	Equal variances not assumed			.115	.909			Equal variances not assumed			-.366	.717	
Education	Equal variances assumed	2.41	.134	2.540	.018	Alternative	Priv-Awar	Equal variances assumed	.282	.600	-.506	.618	Null
	Equal variances not assumed			2.432	.027			Equal variances not assumed			-.515	.612	
Comp_K	Equal variances assumed	1.52	.229	.516	.610	Null	Self-efficacy	Equal variances assumed	.150	.702	-.643	.526	Null
	Equal variances not assumed			.500	.623			Equal variances not assumed			-.643	.527	
Culture	Equal variances assumed	6.41	.018	2.182	.039		CCEXP	Equal variances assumed	.047	.830	.139	.891	Null
	Equal variances not assumed			2.077	.055	Null		Equal variances not assumed			.138	.891	
Num_Con	Equal variances assumed	.770	.389	.469	.644	Null	TrustP	Equal variances assumed	.271	.607	-.554	.584	Null
	Equal variances not assumed			.460	.650			Equal variances not assumed			-.559	.581	
Frq_use	Equal variances assumed	.172	.682	-.584	.565	Null	TrustM	Equal variances assumed	.167	.686	-.645	.525	Null
	Equal variances not assumed			-.575	.571			Equal variances not assumed			-.649	.523	
Risk	Equal variances assumed	.542	.469	.000	1.000	Null	Motivation	Equal variances assumed	.243	.626	.580	.567	Null
	Equal variances not assumed			.000	1.000			Equal variances not assumed			.578	.569	

b. Gender Comparison

Since the previous section has revealed that both groups have given similar responses regarding the framework's items, this means that the data gathered from the two groups can now be combined and tested together to examine if the experts' gender influenced the framework's factors' validation. To this end, the independent samples t-test has been conducted on two gender groups (male and female). This comparison aims to find out if participants with different gender have a different level of agreement across the framework items. Table 5.10 presents the independent samples t-test results.

Table 5.10 Independent Samples T-Test (Gender)

		Levene's Test		t-test for Equality of Means		Supported hypothesis			Levene's Test		t-test for Equality of Means		Supported hypothesis
		F	Sig.	t	Sig.				F	Sig.	t	Sig.	
Per_T	Equal variances assumed	.002	.964	-.153	.880	Null	Severity	Equal variances assumed	7.75	.010	-1.76	.091	
	Equal variances not assumed			-.158	.876			Equal variances not assumed			-2.03	.054	Alternative
Age	Equal variances assumed	.121	.731	.523	.606	Null	Likelihood	Equal variances assumed	.826	.372	-.669	.510	Null
	Equal variances not assumed			.496	.628			Equal variances not assumed			-.711	.486	
Gender	Equal variances assumed	.269	.609	-.305	.763	Null	Sec_awar	Equal variances assumed	1.72	.202	-.571	.573	Null
	Equal variances not assumed			-.305	.764			Equal variances not assumed			-.671	.509	
Education	Equal variances assumed	.126	.725	.537	.596	Null	Priv_awar	Equal variances assumed	1.23	.278	-.714	.482	Null
	Equal variances not assumed			.551	.588			Equal variances not assumed			-.795	.435	
Comp_K	Equal variances assumed	.185	.671	.919	.367	Null	Self-efficacy	Equal variances assumed	6.52	.017	-1.62	.118	
	Equal variances not assumed			.907	.378			Equal variances not assumed			-1.91	.068	Null
Culture	Equal variances assumed	.040	.843	-.153	.879	Null	CCEXP	Equal variances assumed	1.70	.204	.109	.914	Null
	Equal variances not assumed			-.149	.883			Equal variances not assumed			.122	.904	
Num_Con	Equal variances assumed	.604	.445	-2.27	.033	Alternative	TrustP	Equal variances assumed	3.77	.064	-1.87	.074	Null
	Equal variances not assumed			-2.56	.018			Equal variances not assumed			-2.14	.043	
Frq_use	Equal variances assumed	3.66	.068	-3.36	.003	Alternative	TrustM	Equal variances assumed	1.68	.208	-1.80	.084	Null
	Equal variances not assumed			-4.19	.000			Equal variances not assumed			-2.24	.035	
Risk	Equal variances assumed	7.23	.013	-1.67	.107		Motivation	Equal variances assumed	.341	.565	-1.59	.126	Null
	Equal variances not assumed			-2.07	.050	Alternative		Equal variances not assumed			-1.64	.118	

Table 5.10 shows that the Levene's test p-values for most of the items are higher than alpha (sig.>0.05) which means that the null hypothesis is supported, and the variances of the two groups are equal, except for three items which have rejected the null hypothesis and accepted the alternative hypothesis (perceived risk, self-efficacy, and perceived severity of threat). As the variances of the two groups are not equal for these three items, the homogeneity of the variance has been violated. Yet, the independent samples t-test includes t statistics based on both assumptions (equal variances assumed, and equal variances not assumed). Therefore, when comparing the means in the second step of the t-test for perceived risk, self-efficacy, and perceived severity of threat, we must rely on the t statistics that assumed not equal variances.

When comparing the means in the second step, it was clear that four items rejected the null hypothesis (number of friends, frequency of use, perceived risk, and perceived severity of threat). For these four items, there was a difference in means between the two groups (male and female) as can be seen in Figure. 5.3.

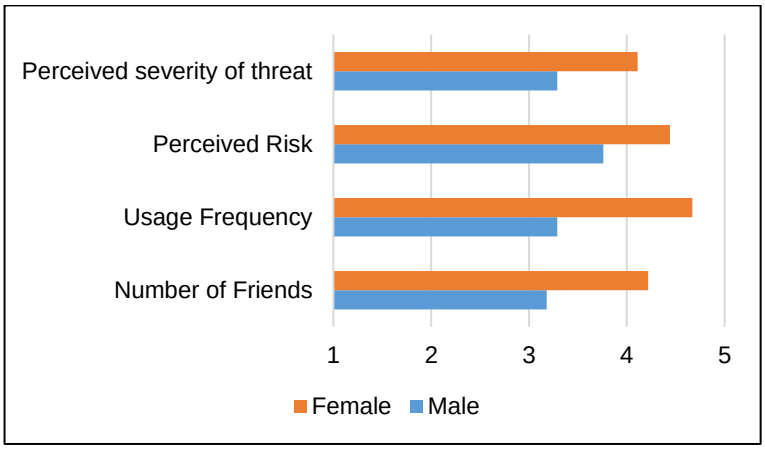


Figure 5.3 Gender Comparison

According to the socio-psychological attributes, both male and female participants agree that gender is not a very important factor to predict social engineering victimisation. Also, Figure 5.3 indicates that there were some opposing views among the two genders about habitual items and their effect on the user's vulnerability to social engineering. Male experts agreed that the number of friends and the usage frequency of a social network are not very important factors that affect the users' judgement of social engineering attacks in the social network. However, female experts have the opposite opinion, as they ranked these as significant factors. Additionally, female experts are agreed about the importance of perceived risk and perceived severity of threat while, in contrast, male experts believed that perceived risk and perceived severity of threat are not very important factors to consider. Once again, these disagreements were regarding the importance level of the items while both groups ranked all items as important and should be included in the framework.

5.4.4 Expert Recommendations (Qualitative Study Results)

The first and the second questions of the qualitative part of the study have been discussed earlier with the quantitative part. This section will address the third question which asked the experts if they think other attributes should be included in the framework. Expert 2 suggested adding more attributes regarding the users' knowledge of social networks, applications, and settings. In addition, Expert 7 suggested looking at the uncertainty level of the user, which might be considered under the culture factor. Expert 10 has stated, "There are

many factors that can be added here but might not explain the behaviour of all social media users. However, some young people are careless and they did not deal with the social media seriously they communicate with anybody either known or not with the goal to enjoy and pass time". Expert 11 agreed with this point of view and said, "People use social media to entertain themselves and do not want to bother use them with high concentration and full attention, they usually click on any video or image without even reading the post". The suggestions from Expert 10 and Expert 11 can be categorised under the personality trait of the user and their motivation for using social media, factors that are already present in the framework.

5.5 The Validation Impact on the Framework

The proposed UCF was the result of integrating previous research, after conducting a comprehensive study of existing human-centric frameworks and related theories. The expert evaluation has been designed to validate the framework's attributes, and the results demonstrate that there is a significant agreement among experts in both study phases with regard to the importance of the framework's factors. However, there were some controversial opinions about some factors. All of these factors' means show that they are considered important by the experts, and this allows us to include them in the framework. Yet, some amendments have been made to the framework according to the experts' recommendations.

In the socio-psychological perspective, computer knowledge has been replaced by social network knowledge. Most social network users should already have basic computer knowledge, but their knowledge of social networking sites and applications is more critical to the study purpose. Therefore, users experience of social networks could be measured by the time elapsed since the user opened his/her social network account and will be moved to the habitual perspective.

In the perceptual perspective, two dimensions are included which are risk perception and user competence. The risk perception consists of the severity of threat and the likelihood of threat while user competence includes security awareness, privacy awareness, self-efficacy, and past experience with cybercrime. In the socio-emotional perspective, two dimensions are included which are the motivation dimension, and the trust dimension which consists of the attributes of trusting social network provider and trusting social network members. Figure 5.4 presents the validated UCF.

Figure 5.4 The Validated User-Centric Framework

5.6 Chapter Summary

The present chapter highlights the riskiest factors that impact users' vulnerabilities, particularly in social network settings. Yet, how these factors interact with each other and how we can mitigate their influence is still unclear and will be discussed further in subsequent chapters. Incorporating experts' opinion on identifying the reasons behind the failure of cyber-attack resistance is a fundamental step toward understanding why people still succumb to cyber-attacks. Detecting the prime interventions between people and the likelihood of victimisation is important for social network providers in order to protect their users. For example, providing security and privacy tutorials that cover the four proposed perspectives would be helpful for the normal user. Classifying the users based on their habitual and socio-psychological attributes to identify vulnerable users is another area that network providers should consider. In chapter 10, a service scenario is provided that can enable extracting user's vulnerabilities based on the proposed UCF.

The previous chapter has discussed the proposed user-centric framework which was developed based on four perspectives: socio-psychological, habitual, perceptual, and socio-emotional. Previous research tends to rely on part of these perspectives and to the best of the

researcher knowledge, have never tried to combine them for a more cohesive understanding of user's susceptibility, relevant factors and dimensions. Subsequently, this chapter focused on the experts' evaluation which has been used as an approach to validate the proposed framework dimensions and components. The results of this validation indicate a general agreement among the experts about the UCF which reflects their confirmation and acceptance of the framework's components. This chapter has answered the second sub-question of the first research question (RQ1.2) as the framework has been validated.

RQ1.2: What is the evaluation method that could be used to validate the proposed user-centric framework?

By the end of this chapter, the user-centric framework has been developed based on four perspectives: socio-psychological, habitual, perceptual, and socio-emotional and validated using mixed-methods experts' evaluation. Therefore, the first phase of the present research has been finished by answering the two sub-questions of the first research question (RQ1).

RQ1: What framework can be used as a basis for the user characteristics that influence user susceptibility to social engineering victimisation on social networking sites?

Next chapter will focus on developing and validating the measurement scales that will be used to empirically test the impact of the framework factors in the third quantitative phase of the current research. The third phase aims to provide objective support to the findings of the present chapter and to examine further the validity of the user-centric framework for predicting people vulnerability.

Chapter 6. CONSTRUCTS MEASUREMENT AND VALIDATION

6.1 Overview

The effect of the different constructs and their dimensions that had emerged from the first phase of the present research needs to be measured in the third phase of the study. These constructs and their dimensions are mostly drawn from the literature. However, some of them were suggested by the participants in the experts' review. Therefore, validating the suitability of the identified dimensions to measure their intended constructs is fundamental before building the conceptual model of the empirical study that will be evaluated in the third phase of the current research. For example, the user competence construct has been suggested by the experts to be measured by four dimensions which are security awareness, privacy awareness, self-efficacy, and experience with cybercrime. These four factors had not been previously measured in the literature as dimensions of user competence. Thus, they need to be validated to ensure their efficacy to measure user competence before developing the conceptual model. Accordingly, the recommendations and guidelines of Mackenzie et al. (2011) have been followed. This method facilitates conducting the content validity test as well as building a robust study instrument.

This chapter is organised as follows. Section 6.2 provides definitions of the study constructs. The constructs in the user-centric framework (UCF) that have been defined as potential factors must be converted into measurable variables in Section 6.3. The content validity test result is discussed in Section 6.4. Section 6.5 draws conclusions from this chapter.

6.2 Constructs Identification

Each construct has been conceptually defined based on previous literature. As suggested by Mackenzie et al. (2011), the definition must reflect precisely the nature and the conceptual domain of the construct. Then, the construct dimensionality must be examined as some constructs might consist of multiple sub-dimensions. Furthermore, the relationship between these sub-dimensions and their higher-order constructs should be identified.

In the proposed UCF, the socio-psychological factors, such as user demographics and personality traits, are considered nominal variables where their values are identified categories, see Table 6.1. The factors of the other three perspectives (habitual, perceptual, and socio-emotional) are measured using ordinal scales. In such measurement scales, the

relationship between the construct and their indicators must be identified as formative or reflective (Henseler et al., 2009).

The proposed framework includes three types of constructs: 2 categorical constructs (Table 6.1), 13 reflective constructs (Table 6.2), and 4 second-order formative constructs and their definitions are listed in Table 6.3. Categorical constructs such as user demographics are usually measured using predefined basic categories. Reflective constructs are measured by a number of observed variables which can be represented by the flow of headed arrows from the construct to its observed items (Finn & Wang, 2014). This can imply that a change in reflective constructs causes a change in observed items. Formative constructs are formed by a number of not necessarily correlated observed items where headed arrows flow from observed items to formative latent variables which imply that a change in any observed item will cause a change in the formative construct (Finn & Wang, 2014). The second-order formative construct can be defined as a construct that is formed by a number of sub-constructs (Hair et al., 2017; Petter et al., 2007). The sub-construct can be reflective or formative constructs. In the second-order formative construct, the headed arrow flows from sub-constructs to the second-order construct which implies that a change in sub-constructs causes a change in the second-order construct.

Table 6.1 Categorical Constructs

Categorical Construct	Definition
User Demographics	The present study considers the importance of each demographic attribute such as age, gender, education level, and major as an influencing factor.
Personality Traits	User behaviour can be patterned and categorised into five different traits which are: neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness.

Table 6.2 Reflective Constructs

Reflective Construct	Definition
Level of Involvement	The extent to which a user engages in social network activities.
Social Network Experience	The amount of time elapsed since the user opened his/her SN account.
Perceived Severity of Threat	The individual's perception of the severity of threats that might be occurred in social networks and the negative consequences of those threats.
Perceived Likelihood of Threat	The individual's perception of the likelihood of threats occurrence and the possibility of falling victim to social engineering attacks in social networks.
Security Awareness	The individuals' awareness of actions and behaviour to protect themselves from online security threats.
Privacy Awareness	The individuals' awareness of actions and behaviour required to protect their personal information online.
Self-efficacy	The individuals' confidence in their ability to protect themselves from any undesirable online incidence.
Experience with Cybercrime	Has the individual previously faced or fallen victim to any kind of social engineering attacks such as identity theft, phishing.
Trust in Provider	The extent to which the individual trusts and relies on the social network's service provider to protect their personal information.

Trust in Members	The extent to which the individual believes that other social network members are trustworthy and not harmful.
Social Motivation	The extent to which social network mediums are perceived to improve the relationship and the impression of friends and family.
Information Motivation	The extent to which social network mediums are perceived to satisfy the desire of expression and information seeking and sharing.
Hedonic Motivation	The extent to which participating in social network mediums is considered enjoyable and pleasurable.

Table 6.3 Second-Order Formative Constructs

Formative Construct	Definition
Perceived Risk	The extent to which the user is uncertain whether an online action is worthwhile or not.
User Competence	The individual's knowledge of social networks and its related risk and ability to use it effectively.
Trust	The extent to which the individual trusts social networks providers and members.
Motivation	It is defined as the motivation that causes the individual to engage more in social networks without conducting preventive measures.

6.3 Constructs Measurement

The constructs in the UCF that have been defined as potential factors must be converted into measurable variables so that we can examine their effects. The study constructs are convertible into measurable variables if we can quantify them by a scale or score (Kimberlin & Winterstein, 2008). The goal of this step is to generate a set of items that adequately represent each conceptual construct. For the second-order formative constructs, it was recommended to develop a set of items that measure each factor in their first-order sub-dimensions individually (Mackenzie et al., 2011). For validity motives, this study has mainly adopted previous scales and measures with some modification needed to reflect the study context and purpose. However, some measurement scales have been developed in this study based on similar instruments used in previous studies. The following are descriptions of each construct and their measurement scales.

6.3.1 Categorical Constructs

6.3.1.1 Demographic Variables

Different demographics have been proposed by the framework to affect user susceptibilities such as gender, age, and education level. Basic and direct demographics questions have been used in the present study.

6.3.1.2 Personality Traits

User personality has a critical role in user online behaviour as revealed by a considerable number of social networks studies (Amichai-Hamburger & Vinitzky, 2010;

Seidman, 2013). The user personality can be divided into five broad categories which group certain traits together in the following five dimensions (Costa, Terracciano, & McCrae, 2001):

- Neuroticism which refers to a personality that has a tendency to show disconcerting emotions such as anxiety and anger.
- Extraversion which means a character that can easily communicate with others.
- Openness to experience which implies a personality that likes the adventure and the new experience.
- Agreeableness which means a personality that shows good deeds and kindness.
- Conscientiousness which refers to a character that has a high level of commitment.

One of the objectives of this research is to find out if certain personality traits influence user vulnerability to social engineering (SE) attacks. Therefore, the participant's personality traits need to be measured and identified. After taking into consideration the other constructs that must be measured in the same survey as well as the time required to complete the scenario-based experiment, a short version of the personality test has been adopted from Rammstedt and John (2007) study to save participants time and to increase the completion rate. Each trait's scale consists of one positive item and one negative coded item. For instance, the two items that measure extraversion are "… Is outgoing, sociable" and "… Is reserved" and the two items that measure agreeableness are "… Is generally trusting" and "… Tends to find fault with others". Participants are asked to rate how each item is related to their personalities using a 5 Likert-scale from 1 (strongly disagree) to 5 (strongly agree).

6.3.2 Reflective Constructs

6.3.2.1 Level of Involvement

Level of involvement has been proposed to be measured using the scale of Facebook intensity which mainly relies on measuring number of friends connections and frequency of use (Ellison et al., 2007). Number of connections can be directly measured by asking participants about the number of friends connected to their social network account. However, when measuring the number of connected friends, it could be worthwhile to ask participants to estimate the percentage of the connected friends that they know personally as suggested by Alqarni et al. (2016) study.

While when developing the measurement of frequency of usage, previous literature recommend different measures for this variable such as calculating the time spent on the network (Saridakis et al., 2016) and checking how often the individual interact with other users in the network such as posting comments (Cao & Lin, 2015; Dwyer et al., 2007). Therefore, both scales were used to measure the frequency of usage. All the scales used to measure the user level of involvement in social networks has been adopted from (Fogel & Nehmad, 2009).

6.3.2.2 Social Networks Experience

When measuring personal experience with information technology, it is common practice to rely on years of experience of using a particular technology, such as computer experience (Flores et al., 2015), or mobile device experience (Arachchilage et al., 2016). People who spent years using social networks usually have more experience than those who started to use the network recently. Furthermore, previous SE research found that the time elapsed since users joined the network to be a significant predictor of susceptibility of SE (Algarni et al., 2017). Therefore, years since joining the network will be used to measure user experience with social networks.

6.3.2.3 Perceived Severity of Threat, and Likelihood of Threat

The scales used to measure these two constructs were adapted from Milne et al. (2009), with some modification and changes to fit the present study context.

6.3.2.4 Security Awareness

The information security literature lacked a validated and accepted measure or technique that can assess individual security awareness in the context of social networks. Organisation practitioners always rely on a variety of methods to measure their users' security awareness, such as counting the number of reported calls to the helpdesk or measuring the number of accesses to unauthorised websites from their network (Khan, Alghathbar, Nabi, & Khan, 2011). However, while such techniques might work for limited and closed environments, they could not measure the users' security awareness for other contexts such as the Internet or social networks. For Internet users, there are other proposed techniques in the literature such as measuring the complexity of passwords used (Kiss & Szasz, 2016) or the amount and type of shared sensitive information in social networks such as real name, workplace, and address (Abdul Molok, Ali, Talib, & Mahmud, 2014). However, the most common technique used by information security researchers is gauging the users' security knowledge by their familiarity with the definitions of computer security terms such as phishing, virus, and malware (Sheng et al., 2010).

Notably, there is no specific scale in the literature to measure users' security awareness in the social network context. This makes it important to generate a scale to measure social network-specific information security awareness. The present study has built a scale based on literature recommendations to social network users to increase their awareness of the security risks associated with social media usage. Users' knowledge and behaviour can be reflections of their awareness. If the user practices safe behaviour in social networks, this could be an

indication of high-security awareness. Thus, this study created a scale to measure user awareness based on the amount of user knowledge about safe security practice. Thereby, a large number of good security practices indicates a high level of user security awareness. Security awareness scale items have been taken partially from recommendations and guidelines in information security training programs (Kim, 2013) supported by a scale created to measure secure behaviour in social networks (Zolait et al., 2014).

6.3.2.5 Privacy Awareness

The items used to measure privacy awareness are adapted from Bartsch and Dienlin's (2016) study. Yet, the previous research did not include a direct scale that measures user privacy awareness. Instead, it focused mainly on online privacy literacy and investigated factors that affect it or are affected by it. Online privacy literacy is a general and complex concept that aims to gauge people's knowledge from many dimensions such as laws and legal aspects of data protection, and the technical issues of online privacy and data protection (Trepte et al., 2015). Peoples' privacy knowledge does not always reflect in their online behaviour, but it is important to measure user awareness based on an assessment of online behaviour. Consequently, the adapted items used in the present study aimed to measure the individual's awareness of safe privacy practices in the social network.

6.3.2.6 Self-efficacy

Previous research has indicated that self-efficacy, which was defined in table 6.2, can contribute to explaining users' risky behaviour online. As a high level of self-efficacy is more likely to prevent the individual from engaging in risky behaviour online (Milne et al., 2009; Vishwanath et al., 2011). In the present study, the self-efficacy scale is adopted from Milne et al. (2009) study, with minor modification to fit the present study context.

6.3.2.7 Cybercrime Experience

Cybercrime experience can be determined by knowing if the individual has previously faced or fallen victim to any SE attacks such as identity theft, phishing. The scale used to measure this factor has been adopted from Bohme and Moore (2012). However, the fourth item in the latter study, which was "Not being able to access online services", has been found to be not significant and removed from the analysis of their research. Therefore, it has also been excluded from the present study and replaced by cyber-harassment, which is one of the most common social network attacks that has been used and found significant in social network studies (Benson et al., 2015).

6.3.2.8 Social Motivation

Social motivation dimension was measured using a four-item scale adopted from previous studies (Al Omoush, Yaseen, & Atwah Alma'aitah, 2012; Basak & Calisir, 2015; Brandtzæg & Heim, 2009; Orchard, Fullwood, Galbraith, & Morris, 2014; Yang & Lin, 2014). This motivation is defined as the extent to which social network mediums are perceived to improve the relationship and the impression of friends and family (Al Omoush et al., 2012; Yang & Lin, 2014).

6.3.2.9 Information Motivation

Information motivation means the extent to which social network mediums are perceived to satisfy the desire of expression and information seeking and sharing which are also reflected by a four-item scale derived from previous literature (Al Omoush et al., 2012; Basak & Calisir, 2015; Brandtzæg & Heim, 2009; Orchard et al., 2014; Yang & Lin, 2014).

6.3.2.10 Hedonic Motivation

Hedonic motivation can be defined as the extent to which participating in social network mediums is considered enjoyable and pleasurable. A four-item scale reflecting this dimension was adopted from the literature (Al Omoush et al., 2012; Basak & Calisir, 2015; Brandtzæg & Heim, 2009; Orchard et al., 2014; Yang & Lin, 2014).

6.3.2.11 Trust in Provider

The scale used to measure the user's trust in a social network provider was adopted from Fogel and Nehmad's (2009) study with minor modification to enhance clarity.

6.3.2.12 Trust in Members

The scale used to measure the user's trust in social network members was adapted from Chiu, Hsu, and Wang (2006) study.

6.3.3 Second-Order Formative Constructs

6.3.3.1 Perceived Risk

People are likely to vary in their perception of the potential risk associated with using social networking sites. High risk perception is assumed to prevent people from being easily deceived by social engineering attempts. Risk perception is a multi-dimensional construct that is measured by two sub-factors (perceived severity of threat and perceived likelihood of threat) which have been defined and discussed in more details earlier in Section 6.3.2.

6.3.3.2 User Competence

In the realm of information systems, user competence can be defined as the individual's knowledge of the intended technology and ability to use it effectively (Munro, Huff, Marcolin, & Compeau, 1997). User competence is a critical construct in previous research and has been widely examined either as a single-dimension or multi-dimensional construct (Koo, Chung, & Kim, 2015). However, end-user competence cannot be measured based upon one type of skill or knowledge. Accordingly, Marcolin, Compeau, Munro, and Huff (2000) have investigated various user competence dimensions and their relation to the knowledge domain. Those dimensions can range between *skills-oriented*, which is related to the individual performance in a specific task, *cognitive-oriented*, which is related to knowledge about a specific task, and *affective-oriented*, which is associated with the individual's attitude toward the particular task including self-efficacy (Kraiger, Ford, & Salas, 1993). Marcolin et al. (2000) have concluded that user competence is a multidimensional construct and the research domain determines its dimensions.

Existing information system research has widely discussed the importance of examining user competence toward increasing user satisfaction and the usage effectiveness of various technologies (Koo et al., 2015). However, little research has investigated its importance in an information security setting. Therefore, based on the user competence conceptualisation that has been suggested by previous research (Marcolin et al., 2000), the present study proposes examining user competence based on four dimensions which are: security and privacy awareness (skills-oriented), self-efficacy (affective-oriented), and cybercrime experience (cognitive-oriented). These four dimensions, as shown in Figure 6.1, provide good breadth of conceptualisation of user competence regarding online risks, such as social engineering attacks. For example, if the social network user is aware of social network privacy issues and the benefits of adjusting privacy settings, such as restricting access to their profile, the user would be more competent in avoiding social engineering threats. In the previous reflective constructs section (6.3.2), the dimensions of user competence were described in detail with the measurements that would formulate user competence level.

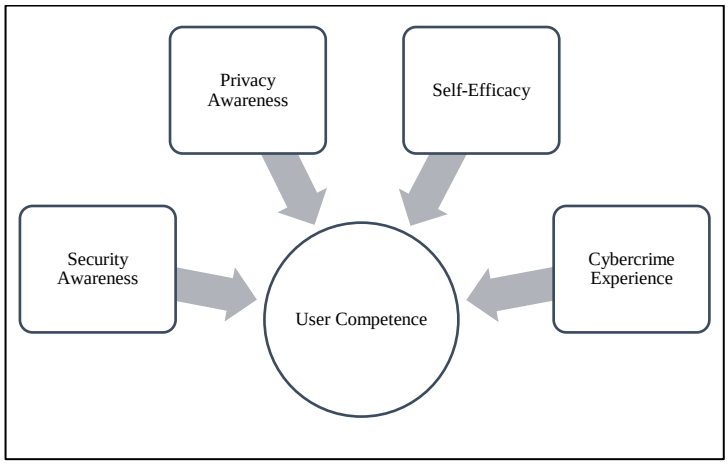


Figure 6.1 Dimensions of the User Competence in Detecting Security Threats on Social Networks

6.3.3.3 Trust

Trust is a context-driven construct that can be defined and classified differently in different settings. In computer science discipline, trust can be classified into two main types: user trust and system trust (Sherchan et al., 2013). Social networks sites are using several strategies to increase the user's trust in their systems and their members. However, increasing the user's trust sometimes leads to risky online behaviour. Therefore, this study investigates the effects of the two types of trust on the user vulnerability to social engineering as the user who trusts social network provider and members would likely be vulnerable to social engineering attacks. The measurement scales for these two dimensions of trust were provided earlier in Section 6.3.2.

6.3.3.4 Motivation

Using social networks services have many motivations and sub-motivations that have been studied in the literature. Yet, there is no agreement about a unique or specific measurement scale that can be used to measure the individual motivation to engage in social networks. Thus, the present research adopted and incorporated the scales from a number of researches scales (Al Omoush et al., 2012; Basak & Calisir, 2015; Brandtzæg & Heim, 2009; Orchard et al., 2014; Yang & Lin, 2014) to form the study scale which consists of three motivations dimensions: social, information, and hedonic. These three dimensions have been defined and discussed in more details earlier in Section 6.3.2.

6.4 Content Validity Test

The current study involves measuring multidimensional constructs and most dimension scales used were adopted from previous studies with some adapted scales. Yet, the

adopted scales have been developed in different fields than the current field of study, which required the addition of some items and change to some of the descriptors to fit the present context. This emphasised the importance of conducting a content validation test not only for the adapted scales but also, for the adopted ones.

The content validity test will examine only the factors that are measured using multiple items scales (12 reflective factors). The formative factors validity will be examined later in the pilot test because their latent scores will be measured based on a number of formative indicators after collecting a sample of data. Therefore, to test the content validity of the reflective measurement scales, Schriesheim and Hinkin (1990) item-categorisation approach has been followed due to its suitability and robustness even with a small sample of participants (Hornsby et al., 2013). More details about this approach can be found in Chapter 3.

Participants have been asked to complete a short survey, which consists of three parts. The first part is asking about some demographic factors such as age, gender, and field of study. The second part includes two content validation matrixes. Participants have been asked to judge and align each item in the matrixes with its relevant constructs as the following:

- If participants think the item represents one construct, participants can assign or tick "√" the intended construct.
- If participants think the item can indicate more than one construct, participants should rank-order the constructs in which the item measures from the highest relevance to the lowest relevance from 1 to 3.

In the third part, participants have been asked to list the numbers of any statements that they found unclear and to write down any concept or term that they read in the statements that they think needs more clarification.

6.4.1 Participants' Profiles

All Participants were PhD students in computer and information sciences departments from two universities in the UK. Almost 60% of the participants are specialised in the information security (IS) field while the rest are specialised in different disciplines, such as cloud computing, digital health, and information sciences. 17 responses have been collected, of which 12 are female and ages range from 25 to 44 years old.

6.4.2 Results and Discussion

After collecting the data, the answers have been coded as follows. Any tick "√" or "1" answer has been weighted as 3. Any "2" answer has been weighted as 2. Any "3" answer has been weighted as 1. Items will be only retained if the percentage of the points assigned by the

experts to the intended construct exceeded 60% (Hornsby et al., 2013; Schriesheim & Hinkin, 1990).

Table 6.4 contains the items for the six constructs in the perceptual perspective and shows the results of content validity for each item. Among the 29 items, there were five items (item 7, item 10, item 11, item 16, and item 18) with insufficient content validity, as each of these had a percentage of the total points below the 60% threshold. The self-efficacy, the perceived likelihood of threat, and the cybercrime experience items were all scored highly by the participants and no items needed to be changed or removed from their scales. While items 26, 27, and 28 of the cybercrime experience scale have been adopted from an earlier study (Bohme & Moore, 2012), their validity is also supported by the result of the current research. These items received high validity scores of 81.82%, 63.16%, and 81.82% respectively. The new item (item 29) that was added by the current study to the past experience with cybercrime scale has been given a relatively low score (60.38%).

The participants generally accept the privacy awareness items as they fulfilled the required retention criterion to be included in the scale. In contrast, item 7 failed to exceed the retention cut point as its score was quite low (42.37%). Therefore, this item must be removed from the privacy awareness scale. Similarly, item 18 failed to measure the perceived severity of threat (49.25) and thus was removed from the scale. Likewise, the consensus among participants regarding item 10, item 11, and item 16 was relatively evident as their low percentages proved that they could not represent security awareness. Therefore, these three items must be removed from the security awareness scale.

It is also worth noting that item 11 (the individual usually reports any malicious accounts to SN provider) was nearly transferred to represent self-efficacy. As 45.61% of the total points assigned by participants to this item were in the self-efficacy dimension which was higher than the points assigned to its intended dimension, security awareness, which was only 31.58%. However, this item can’t be transferred as it still did not reach the recommended threshold (60%) to be adequate to represent self-efficacy.

Table 6.4 Content Validity Result (Perceptual Perspective)

Statements	The percentage of the total points					
	SEF	PA	SA	ST	LT	CCEXP
Self-efficacy (SEF): The individuals' confidence in their ability to protect themselves from any undesirable online incidence.						
1. The individual is confident that they can avoid any hazards while using Facebook.	**72.13**	8.20	14.75	4.92	0.00	0.00
2. The individual is skilled at avoiding dangers while using Facebook.	**64.71**	14.71	14.71	2.94	2.94	0.00
3. The individual has the knowledge and the ability to secure their Facebook account by adjusting the account settings.	**71.43**	6.35	15.87	3.17	0.00	3.17
4. The individual has the ability to protect themselves from any online threats while using Facebook.	**66.67**	13.64	9.09	4.55	0.00	6.06
Privacy Awareness (PA): The individuals' awareness of actions and behaviour required to protect their personal information online.						
5. The individual reviewed the SN privacy policy and they know how to configure it.	20.69	**60.34**	15.52	3.45	0.00	0.00
6. The individual restricts access to their account by adjusting the privacy setting.	16.67	**73.33**	10.00	0.00	0.00	0.00
7. On Facebook, the individual does not feel safe regarding their personal data, who can contact them, and the exchange of thoughts and feelings.	0.00	**42.37**	23.73	18.64	10.17	5.08
8. The individual does not share personal information in SN such as birthdate, phone number, workplace or address.	10.77	**70.77**	10.77	4.62	3.08	0.00
9. The individual does not share their current or future location in SN, for example, images for their current vacation, or plans for future vacation.	11.11	**62.50**	25.00	0.00	1.39	0.00
Security Awareness (SA): The individuals' awareness of actions and behaviour to protect themselves from online security threats.						
10. The individual does not use third party apps (apps that offer new features that are not available in the official version) to access their social networks accounts.	14.04	19.30	**52.63**	10.53	3.51	0.00
11. The individual usually reports any malicious accounts to SN provider.	45.61	12.28	**31.58**	10.53	0.00	0.00
12. The individual uses a password for their SN account different from the passwords they use to access other sites	23.73	0.00	**76.27**	0.00	0.00	0.00
13. The individual uses a specific new email for their SN account different from their personal or work email.	19.67	0.00	**63.93**	8.20	8.20	0.00
14. The individual updates their password on a regular basis	16.92	7.69	**75.38**	0.00	0.00	0.00
15. The individual always reads and pays attention to the security warning messages on Facebook.	6.56	9.84	**72.13**	11.48	0.00	0.00
16. The individual does not use similar usernames for different social media accounts.	9.84	18.03	**52.46**	9.84	9.84	0.00
Perceived Severity of Threat (ST): The individual's perception of the severity of threats that might be occurred in social networks and the negative consequences of those threats.						
17. The individual believes that losing financial information while using Facebook would be harmful to them.	6.78	8.47	13.56	**61.02**	10.17	0.00
18. The individual believes that having strangers eavesdropping on their Facebook account would be a severe problem for them.	14.93	26.87	8.96	**49.25**	0.00	0.00
19. The individual believes that having their messages and chats seen or listened to on Facebook would be a severe problem for them.	0.00	14.93	5.97	**62.69**	16.42	0.00
20. The individual believes that losing their data privacy while using Facebook would be a severe problem for them.	0.00	24.62	0.00	**75.38**	0.00	0.00
21. The individual believes that having their identity stolen on Facebook would be a severe problem for them.	0.00	12.70	6.35	**80.95**	0.00	0.00
Perceived Likelihood of Threat (LT): The individual's perception of the likelihood of threats occurrence and the possibility of falling victim to social engineering attacks in social networks.						
22. The individual's opinion about how likely it is for one's financial information to be stolen in Facebook.	0.00	0.00	22.03	10.17	**67.80**	0.00
23. The individual's opinion about how likely it is for one's personal information to be secure while using Facebook.	0.00	15.79	15.79	7.02	**61.40**	0.00
24. The individual's opinion about how likely it is for one's privacy to be invaded without their knowledge while using Facebook.	0.00	24.56	0.00	10.53	**64.91**	0.00
25. The individual's opinion about how likely it is that one's identity can be stolen in Facebook.	0.00	19.05	14.29	0.00	**66.67**	0.00
Cybercrime Experience (CCEXP): Has the individual previously faced or fallen victim for any kind of social engineering attacks such as identity theft, phishing...etc.						
26. Has the individual ever experienced somebody stealing their personal data and impersonating them, e.g. shopping under their name, open SN account in their name.	7.27	0.00	10.91	0.00	0.00	**81.82**
27. Has the individual ever experienced online fraud where goods purchased were not delivered, counterfeit or not as advertised	8.77	0.00	19.30	8.77	0.00	**63.16**
28. Has the individual ever received emails fraudulently asking for money or personal details (including banking or payment information).	7.27	10.91	0.00	0.00	0.00	**81.82**
29. Has the individual ever received harassing messages, inappropriate comments, or other persistent behaviours that endanger their safety?	0.00	11.32	0.00	11.32	16.98	**60.38**

Table 6.5 shows the result of the content validity of the habitual and the socio-emotional factors measurement scales. Most of scales items have successfully represented their intended constructs. However, some items have failed to reach the acceptance threshold. The UCF in Chapter 5 claimed that number of connections in users' networks could also reflect users' involvement in the network. However, the experts have a different opinion as the

content validity test results revealed that the number of connections (item 2) could not measure a person's level of involvement in the network as the total points assigned to the item (58.18) is less than the threshold of 60%. Therefore, this item has been eliminated from the level of involvement scale and will be treated individually as an independent factor in the conceptual model.

In the social motivation, item 4 has failed to reach the threshold of 60%. Therefore, it has been removed from the factor measurement scale. Furthermore, item 8 and item 9 of the measurement scale of information motivation have also been removed due to the low points that have been given by the experts. However, experts have given item 15 in the hedonic motivation a high number of points as to represent the information motivation (60.66) instead of the hedonic motivation (16.39). Therefore, item 15 has been transferred from the hedonic motivation scale to the information motivation scale.

Table 6.5 Content Validity Result (Habitual and Socio-Emotional Perspectives)

Statements	The percentage of the total points					
	LOI	**SM**	**IM**	**HM**	**TP**	**TM**
Level of Involvement (LOI): The extent to which a user engages in social network activities.						
1. How often does the individual comment on other people's status update or pictures?	**61.02**	10.17	10.17	18.64	0.00	0.00
2. Approximately how many ''friends" does the individual have on their account?	**58.18**	36.36	5.45	0.00	0.00	0.00
3. On a typical day, how many minutes does the individual spend on Facebook?	**69.49**	0.00	0.00	30.51	0.00	0.00
Social Motivation (SM): The extent to which social network mediums are perceived to improve the relationship and the impression of friends and family.						
4. The individual believes that using social networks makes a good impression on other people.	15.79	**57.89**	0.00	15.79	0.00	10.53
5. The individual uses Facebook to maintain their popularity and prestige among peers.	18.64	**64.41**	6.78	10.17	0.00	0.00
6. The individual uses Facebook to keep in touch with friends and family.	0.00	**86.44**	6.78	6.78	0.00	0.00
7. The individual uses Facebook to meet and connect with new people with similar interests.	0.00	**81.82**	7.27	10.91	0.00	0.00
Information Motivation (IM): The extent to which social network mediums are perceived to satisfy the desire of expression and information seeking and sharing.						
8. The individual uses Facebook to express and share their opinion freely.	9.84	24.59	**52.46**	6.56	0.00	6.56
9. The individual uses Facebook to share information, photos, or videos with others.	12.31	12.31	**47.69**	7.69	7.69	12.31
10. The individual uses Facebook to stay up to date with news and current events	6.35	25.40	**68.25**	0.00	0.00	0.00
11. The individual could obtain useful information from Facebook.	12.28	0.00	**87.72**	0.00	0.00	0.00
Hedonic Motivation (HM): The extent to which participating in social network mediums is considered enjoyable and pleasurable.						
12. The individual enjoys using the wide range of applications in Facebook such as games.	10.17	10.17	6.78	**62.71**	10.17	0.00
13. The individual believes that using social networks is enjoyable and entertaining.	14.75	8.20	0.00	**68.85**	0.00	8.20
14. The individual uses Facebook to pass the time.	10.17	16.95	6.78	**66.10**	0.00	0.00
15. The individual uses Facebook out of curiosity; they want to know what their friends and other people are doing on Facebook.	0.00	22.95	**60.66**	**16.39**	0.00	0.00
Trust in Provider (TP): The extent to which the individual trusts and relies on the social network's service provider to protect their personal information.						
16. The individual believes that Facebook can be relied on to keep its promises and commitment to its members.	0.00	7.27	0.00	0.00	**81.82**	10.91
17. The individual can count on Facebook to protect their personal information from unauthorised use.	0.00	0.00	0.00	0.00	**92.73**	7.27
18. The individual believes that Facebook is a trustworthy social network.	0.00	0.00	0.00	0.00	**88.24**	11.76
19. The individual can count on Facebook to protect their privacy.	0.00	0.00	0.00	0.00	**100.00**	0.00
Trust in Members (TM): The extent to which the individual believes that other social network members are trustworthy and not harmful.						
20. The individual believes that Facebook members will always keep the promises they make to one another.	10.53	0.00	7.02	0.00	0.00	**82.46**
21. The individual believes that Facebook members will not misuse the information they found about them in their account.	0.00	0.00	0.00	0.00	11.76	**88.24**
22. The individual believes that Facebook members will not take advantage of others even when the opportunity arises.	0.00	7.27	0.00	0.00	10.91	**81.82**
23. The individual believes that Facebook members are truthful in dealing with one another.	0.00	0.00	0.00	0.00	0.00	**100.00**

In the qualitative comments, some participants mentioned that they had difficulty distinguishing between the items for security and privacy awareness. Others also suggested that self-efficacy, security, and privacy awareness items could be overlapping as they are very similar to each other. This was clearly seen in the results from Table 6.4 that for most items, participants have assigned them to those three constructs: self-efficacy, security awareness, and privacy awareness with different relevance. This can remarkably reflect the proposed idea that those items are dimensions that measure the same concept, which is user competence. However, experts' comments and the content validity results make us reconsider including past experience with cybercrime to be a dimension with self-efficacy, security, and privacy awareness to form user competence. Cybercrime experience has been treated as a stand-alone factor to influence SE vulnerability as will be discussed further in Chapter 7. This conclusion has also been supported later by the result of the pilot study where user competence has been tested by the four dimensions. The results of the pilot test revealed that cybercrime experience has no impact on user competence. Table 6.6 and Figure 6.2 show the result of the bootstrapping test of user competence dimensions.

Table 6.6 Bootstrapping Test of the Four Dimensions of User Competence (Pilot Study)

Relationship	Path coefficient	T-value	P-value	Sig.?
Security → Competence	0.416	14.138	<0.001	Yes
Privacy → Competence	0.374	11.660	<0.001	Yes
Self-efficacy → Competence	0.376	15.938	<0.001	Yes
CCEXP → Competence	0.106	1.352	0.177	No

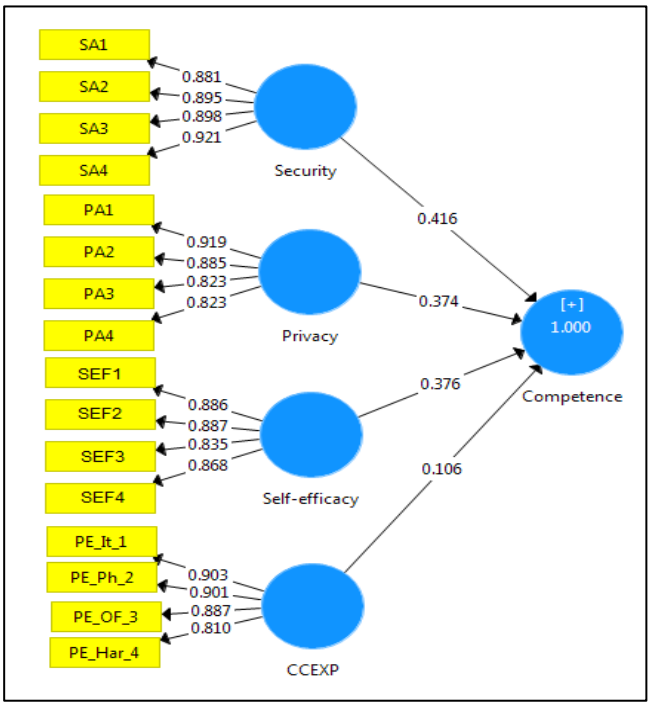


Figure 6.2 Pilot Study Result of the User Competence Dimensions

Regarding the wording of the items, most of the participants found them to be clear. However, two participants indicated one item in the privacy awareness scale which is "I reviewed Facebook privacy policy and I know how to configure it" to be not clear enough. One of them mentioned precisely that the word "configure" is ambiguous here and should be replaced by a more specific word. Therefore, it was replaced with "manage" to remove the ambiguity. Another term that also has been found difficult and unclear by respondents is "third party apps" in item 10 in the security measurement scale, so it has been declared with an example for more clarity. Yet, this item has been removed from the security scale due to low validity. Other than that, the responses indicated that the questionnaire was clear and easy to complete.

6.5 Chapter Summary

The present chapter has focused on validating the measurement scales that were used to quantify the reflective constructs (Table 6.2). While the second-order formative constructs such as user competence and trust will be verified later in the pilot study in the third study phase as these types of constructs are formed and calculated based on a number of dimensions (reflective constructs). One of the main results of the content validity test is that cybercrime experience could not be treated as a dimension of user competence. Therefore, cybercrime experience will be included as an independent variable in the conceptual model that directly affects the user vulnerability to social engineering. Similarly, number of connections has not been found to reflect users' involvement in the network. Thus, this factor will also be considered as a stand-alone factor in the conceptual model.

The next chapter will concentrate on building a conceptual model that facilitates empirically testing the impact of framework factors and dimensions on the social engineering victimisation in the social network context.

Chapter 7. CONCEPTUAL MODEL DEVELOPMENT (THE CASE OF FACEBOOK)

7.1 Overview

Previous chapters have proposed and validated a user-centric framework that includes different perspectives and factors to predict users' vulnerability toward social engineering (SE) attacks in social networks context. Previous research tends to treat factors that affect user victimisation as being simple and straightforward constructs. However, most of the factors that influence human behaviour are complex and multifaceted which needs further effort to measure. For example, if user competence to deal with online threats was measured using a single dimension, that measure will not adequately cover the full concept of the user competence. Thus, the present research used multi-dimensional variables to measure the study constructs in order to provide a clear and comprehensive view of the concepts under investigation. Yet, before developing the conceptual model based on the proposed framework, all of the dimensionality and the feasibility of the framework's constructs have been validated, and the result of this validation is presented in Chapter 6.

This chapter investigates the relationship between each factor in the user-centric framework and user susceptibility to SE as well as examining the relationships among those identified factors. In order to propose a conceptual model, Facebook social network has been selected to be the case study of the present research as justified in Section 7.2. The study hypotheses will be presented in Section 7.3. The conceptual model of the present research is illustrated in Section 7.4. Finally, Section 7.5 provides a summary of the current chapter.

7.2 The Facebook Case

Facebook has been chosen as an example social network due to its popularity and a vast number of active profiles, with almost 2.2 billion monthly active users communicating on the network (Statista, 2018). Given this number of profiles, Facebook has not attracted only legitimate users, cybercriminals have also given this media special attention. As the online social network has expanded and produced various advanced tools and technologies that cybercriminals managed to use to their advantage (Tsikerdekis & Zeadally, 2014). A study conducted in 2014 revealed that around 22% of phishing scam targeted Facebook network

(Stern, 2014). According to Sophos's Security threat report (2011), Facebook is by far the most targeted social network platform by cybercriminals.

Privacy and security researchers have recently focused on the challenges and issues associated with Facebook usage. Some researchers have classified Facebook security threats into three different classes which are multimedia content threats, traditional threats, and social threats (Rathore, Sharma, Loia, et al., 2017). Furthermore, Fokes and Li (2014) have surveyed the most common security vulnerabilities in Facebook and found that most weaknesses are either platform-related or user-related. Likewise, Kayes and Iamnitchi (2017) provided an overview of security and privacy challenges and issues that could face social network users and outlined that solutions to overcome these privacy and security issues are hard to separate when their goal is the same, that is to protect the end user.

Most of Facebook issues are related to unauthorised access to users' accounts (security violation) or unpermitted access to users' private information such as users' image and location (privacy violation) (Van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018). Uncontrolled user behaviour can cause both of these violations in regards to information sharing (Van Schaik et al., 2018). However, in social network behavioural research, huge attention has been given to privacy-related issues while limited research has focused on the social network's information security problems (Saridakis et al., 2016). Therefore, the present study investigated user characteristics in social networks, particularly Facebook, from different angles such as people's perceptions and behaviour, in an attempt to identify the factors that could predict individuals' vulnerability to social engineering threats. People's vulnerability level will be identified based on their response to a variety of social engineering scenarios. The following section will address in detail the relationship between each factor of the four perspectives and user vulnerability to social engineering victimisation.

7.3 The Study Hypotheses

To develop the study model, first, it was essential to identify the nature and direction of the relationship between every factor of each perspective and user vulnerability to SE victimisation (these hypotheses will be represented with the letter a). Second, the relationships among the factors themselves need to be clarified (these hypotheses will be represented with the letter b). However, socio-psychological factors are measured using nominal scales which make them hard to include in the measurement model. Therefore, their hypotheses will be represented using (the letter c), and their effect on user victimisation will be examined using other statistical tests in chapter 8.

7.3.1 Habitual Perspective

Due to the importance of understanding the impact of a person's habitual factors on their susceptibility to social engineering in social networks, this study aims to measure the effect of level of involvement, number of social network connections, percentage of known friends among the network's connections, and social network experience on predicting user susceptibility to social engineering in the conceptual model.

7.3.1.1 Level of Involvement

This construct is intended to measure the extent to which a user engages in Facebook activities. When people are highly involved with a communication service, they tend to be relaxed and ignore any cues associated with such service that warn of deception risk (Vishwanath et al., 2016). User involvement in a social network can be measured by the number of minutes spent on the network every day and the frequency of commenting on other people's status updates or pictures (Vishwanath, 2015). Time spent on Facebook is positively associated with disclosing highly sensitive information (Chang & Heo, 2014). Furthermore, people who are more involved in the network are believed to be more exposed to social engineering victimisation (Saridakis et al., 2016; Vishwanath, 2015).

Conversely, highly involved users are supposed to have more experience with the different types of threat that could occur online. Yet, it has been observed that active Facebook users are less concerned about sharing their private information as they usually have less restrictive privacy settings (Halevi et al., 2013). Users' tendency to share private information could relate to the fact that individuals who spend more time using the network usually exhibit high trust in the network (Sherchan et al., 2013). Therefore, the following hypotheses have been proposed.

- **Ha1.** Users with a higher level of involvement will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
  - **Hb1.** The user's level of involvement positively influences the user's experience with cybercrime.
  - **Hb2.** The user's level of involvement positively influences the user's trust.

7.3.1.2 Number of Connections

Despite of the fact that having a large number of social network connections could increase a person's life satisfaction if he/she is motivated to engage in the network to maintain friendships (Rae & Lonborg, 2015), this high number of contacts in the network is claimed to increase vulnerability to online risks (Buglass et al., 2016; Vishwanath, 2015). Risky behaviour such as disclosing personal information in Facebook is closely associated with users' desire to maintain and increase the number of existing friends (Chang & Heo, 2014;

Cheung, Lee, & Chan, 2015). Users with a high number of social network connections are motivated to be more involved in the network by spending more time sharing information and maintaining their profiles (Madden et al., 2013).

Furthermore, a high number of connections might suggest that users are not only connected with their friends but also with strangers. Vishwanath (2015) has claimed that connecting with strangers on Facebook can be considered as the first level of cyber-attack victimisation, as those individuals are usually less suspicious of the possible threats that can result from connecting with strangers in the network. Furthermore, Alqarni et al. (2016) have adopted this view to test the relationship between severity and vulnerability of phishing attacks and connection with strangers (as assumed to present the basis for phishing attacks). Their study indicated a negative relationship between the number of strangers that the user is already connected to and the user's perception of the severity and their vulnerability to phishing attacks in Facebook. Therefore, if users are connected mostly with known friends on Facebook, this could be seen as a mark of less vulnerable individuals. With all of these points in mind, the following hypotheses are generated.

- **Ha2.** Users with a higher number of connections will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
    - **Hb3.** The user's number of connections positively influences the user's level of involvement.
- **Ha3.** Users with higher connections with known friends will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).

7.3.1.3 Social Network Experience

People's experience in using information communication technologies makes them more competent to detect online deception in social networks (Tsikerdekis & Zeadally, 2014). For instance, it has been found that the more time elapsed since joining Facebook makes the user more capable of detecting social engineering attacks (Algarni et al., 2017). Furthermore, despite the fact that some researchers argue that computer experience has no significant impact on phishing susceptibility (Halevi et al., 2013; Saridakis et al., 2016; Vishwanath et al., 2011), other research on email phishing found positive impact from number of years of using the Internet and number of years of using email on a person's detection ability of email phishing (Alseadoon, 2014; Sheng et al., 2010). Therefore, the present study suggests that the more experienced are the users with social networks, the less vulnerable they are to social engineering victimisation.

Additionally, in the context of the social network, Internet experience has been found to predict precautionary behaviour, and further causes greater sensitivity to associated risks in

using Facebook (Van Schaik et al., 2018). Thus, years of experience in using the network could increase the individual's awareness of the risk associated with connecting with strangers. Accordingly, the present study postulates that more experienced users would have a high percentage of connections with known friends in the network.

- **Ha4.** Users with a higher level of experience with social network will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).
    - **Hb4.** The user's social network experience positively influences the user's connections with known friends.

7.3.2 Perceptual Perspective

People's risk perception, competence, and cybercrime experience are the three perceptual factors that are believed to influence their susceptibility to social engineering attacks. The strength and direction of these factors' impact will be discussed as follows.

7.3.2.1 Risk Perception

Facebook users have a different level of risk perception that might affect their decision in times of risk. Vishwanath et al. (2016) has described risk perception as the bridge between users' previous knowledge about the expected risk and their competence to deal with that risk. Many studies have considered perceiving the risk associated with engaging in online activities as having a direct influence on avoiding using online services (Riek et al., 2016) and more importantly as decreasing their vulnerability to online threats (Vishwanath et al., 2016).

Facebook users' perceived risk of privacy and security threats significantly predict their strict privacy and security settings (Van Schaik et al., 2018). Thus, if online users are aware of the potential risks and their consequences that might be encountered on Facebook, they will probably avoid clicking on malicious links and communicating with strangers on the network. This indicates that risk perception contributes to the user's competence in dealing with online threats and should lead to a decrease in susceptibility to SE. Therefore, the following relationships have been proposed.

- **Ha5.** Users with a higher level of risk perception will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).
    - **Hb5.** The user's perceived risk positively influences the user's competence.

7.3.2.2 Competence

User competence has been considered an essential determinant of end-user capability to accomplish tasks in many different fields. To gain insight into user competence in detecting security threats in the context of online social networks, investigating the multidimensional space that determines this user competence level is fundamental. The role of user competence

and its dimensions in facilitating the detection of online threats is still a controversial topic in the information security (IS) field. The dimensions used in the present study to measure the concept are security awareness, privacy awareness, and self-efficacy. The scales used to measure these factors can determine the level of user competence in evaluating risks associated with social network usage.

User competence in dealing with risky situations in a social network setting is a major predictor of the user's response to online threats. When individuals feel competent to control their information in social networks, they are found to be less vulnerable to victimisation (Saridakis et al., 2016). Furthermore, Self-efficacy, which is one of the user's competence dimensions, has been found to play a critical role in users' safe and preservative behaviour online (Milne et al., 2009). People who have confidence in their ability to protect themselves online as well as having high-security awareness can be perceived as highly competent users when facing cyber-attacks (Wright & Marett, 2010). This study hypothesised that highly competent users are less susceptible to cyber-attack victimisation.

- **Ha6.** Users with a higher level of competence will be less susceptible to social engineering attacks (i.e., there will be a negative relationship).

7.3.2.3 Cybercrime Experience

Cybercrime experience has been identified as a competence measure at the start of this study. Yet, the content validity test, as well as the result of the pilot test that has been discussed in chapter 6, reveal that this construct should be measured separately. Past victimisation is observed as profoundly affecting the person's view of happiness and safety in general (Mahuteau & Zhu, 2016). Also, such unpleasant experience is inclined to change behaviour, for example, reducing the likelihood of engagement in online-shopping (Bohme & Moore, 2012) or even increasing antisocial behaviour (Cao & Lin, 2015).

Furthermore, previous email phishing victimisation is claimed to raise user awareness and vigilance and thus prevent them from being victimised again (Workman, 2007). Yet, recent studies found this claim to be not significant (Iuga et al., 2016; Wang et al., 2017). As experience with cybercrimes could also be used as a determinant of a person's limitations in protecting themselves from such threats.

Experience with cybercrime has been found to increase a person's perceived risk of social network services (Riek et al., 2016). Those who are knowledgeable and have previous experience with online threats could be assumed to have high-risk perception (Vishwanath et al., 2016). However, unlike the context of email phishing, little is known about the role of prior knowledge and experiences with cybercrime in preventing people from being vulnerable

to social engineering attacks in the context of social networks. Therefore, this study proposes that past experience could raise the user's risk perception but also could be used as an indicator of the user's susceptibility. To this extent, the following hypotheses have been assumed.

- **Ha7.** Users with a previous experience with cybercrime will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
    - **Hb6.** The user's experience with cybercrime positively influences the user's perceived risk.

7.3.3 Socio-Emotional Perspective

Little is known regarding the impact that this perspective has on social engineering victimisation in a social network context. However, previous research has highlighted the positive effect of a person's general trust or belief in their victimisation in email phishing context (Alseadoon et al., 2015) which encourages the present research to investigate more socio-emotional factors such as the dimensions of user trust and motivation, in order to consider their possible impact on user's risky behaviour.

7.3.3.1 Trust

Some studies in email phishing (e.g., Alseadoon et al., 2015; Workman, 2008a) stress that the disposition to trust is a predictor of the user's probability of being deceived by cyber-attacks. In the context of social networks, trust can be derived from the members' trust for each other as well as trusting the network provider. These two dimensions of trust have been indicated to negatively influencing a person's perceived risk of the likelihood of disclosure of personal information (Cheung et al., 2015). Trust has also been found to strongly increase the disclosure of personal information among social network users (Beldad & Hegner, 2017; Chang & Heo, 2014). With all of this in mind, the present study hypothesised that trusting the social network provider as well as other members may cause higher susceptibility to SE.

- **Ha8.** Users with a higher level of trust will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).

7.3.3.2 Motivation

According to the uses and gratification theory, people are using the communication technologies that fulfil their needs (Joinson, 2008). Users' motivation to use communication technologies must be taken into consideration in order to understand online user behaviour. This construct has been acknowledged by researchers in many fields such as marketing (Chiu, Wang, Fang, & Huang, 2014), and mobile technology (Kim, Kim, & Wachter, 2013) in order to understand their target users. However, IS research has limited the adoption of this view toward understanding the online users' risky behaviour. Users can be motivated by different

stimuli to engage in social networks such as entertainment or information seeking (Basak & Calisir, 2015).

Additionally, people use Facebook for social reasons such as maintaining existing relationships and making new friends (Rae & Lonborg, 2015). According to social engineering victimisation, these motivations can shed light on understanding the user's behaviour at times of risk. For example, hedonically motivated users who usually seek enjoyment are assumed to be persuaded to click on links that provide new games or apps. While socially motivated users are generally looking to meet new people online, which makes them more likely to connect with strangers. Such connections with strangers are considered risky behaviour nowadays (Alqarni et al., 2016). Therefore, this study predicts that the users' vulnerability to social engineering-based attacks will be different based on their motives to access social networks.

User's differing motivation to use social networking sites can explain their attitude online, such as tendency to disclose personal information in social networks (Chang & Heo, 2014). Additionally, a person's perceived benefit of network engagement has a positive impact on their willingness to share their photos online (Beldad & Hegner, 2017). Thus, the present study assumes that motivated users are more vulnerable to cyber-attack victimisation than others. Additionally, motivated users could be inclined to be more trusting when using technology (Baabdullah, 2018). This motivation could lead the individual to spend more time and show higher involvement in social networks (Ross et al., 2009). This involvement could ultimately lead motivated individuals to experience or at least be familiar with different types of cybercrime that could happen in the network. Hence, the following hypotheses have been postulated.

- **Ha9.** Users with a higher level of motivation will be more susceptible to social engineering attacks (i.e., there will be a positive relationship).
    - **Hb7.** The user's motivation positively influences the user's trust.
    - **Hb8.** The user's motivation positively influences the user's level of involvement.
    - **Hb9.** The user's motivation positively influences the user's experience with cybercrime**.**

7.3.4 Socio-Psychological Perspective

The nature of the measurement scales of the socio-psychological variables is a nominal categorical scale which means that these variables are not recommended to be included in the measurement and structural model (Hair et al., 2012). The socio-psychological factors impact on user vulnerability to social engineering attacks will be hypothesised in this chapter and will be tested separately on Chapter 8.

7.3.4.1 Personality Traits

According to the big five personality traits theory (Costa & McCrae, 1992), there are five distinct traits (neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness) that explain the pattern of human personality regarding their reactions, behaviours, feelings, and thoughts. Personality traits are commonly known as the driver of human behaviour and have been recognised by researchers from diverse fields, such as marketing (Leong, Jaafar, & Sulaiman, 2017), learning and education (Di Giunta et al., 2013), as predictors of user reactions to different phenomena. Previous IS research has anticipated the relationship between the big five personality traits and the user's possible victimisation to cyber-attacks such as social engineering-based attacks. Some studies have empirically investigated personality traits' impact on email phishing responses (Alseadoon et al., 2015; Halevi et al., 2013). However, Halevi et al. (2013) state that neuroticism is the only trait that correlates to phishing email responses, while Alseadoon et al. (2015) study presented opposing findings that openness, extraversion, and agreeableness are personality traits that increase user tendency to comply with phishing email requests. One potential reason for such inconsistent results is the existence of mediation factors that control the relationship between personality traits and SE victimisation.

With this in mind, this study takes a different approach when dealing with the effects of personality traits on victimisation and proposes that personality traits have indirect effects on a user's vulnerability to cyber-attack. Other factors are mediating this relationship such as the individual's perceptual and socio-emotional factors. More detail of the mediation model components and hypotheses will be discussed in the following chapter.

- **Hc1.** Certain personality traits are indirectly associated with the user's susceptibility to social engineering attacks.

7.3.4.2 User Demographics

One of the proposed solutions to deal with enduring online threats is to understand the victim's demographics and education background and examine their reaction by conducting a real attack, such as the case of sending phishing emails to a particular group of users (Alseadoon et al., 2015; Vishwanath et al., 2016). In contrast, due to ethical considerations, the majority of studies (e.g., Algarni et al., 2017; Iuga et al., 2016; Sheng et al., 2010) have used scenario-based experiments to examine people's vulnerabilities. Among the many identified characteristics that are believed to predict potential victims, demographic factors are the most controversial variables. For instance, female users have been repeatedly indicated as the weakest gender to detect online threats (Algarni et al., 2017; Halevi et al., 2013; Iuga et

al., 2016; Sheng et al., 2010), while in other studies either females have shown a high detection accuracy compared to males (Wang et al., 2017), or even found this relation between gender and susceptibility to being not significant (Alseadoon, 2014; Diaz, Sherman, & Joshi, 2018; Griffin, 2018).

Moreover, most of the earlier mentioned studies are focused on one type of attack although criminals have several ways to perform social engineering attacks. This has indicated the need for further investigation of the impact of a person's demographics on their vulnerability to different types of cyber-attack and the need to explore which groups of users are more vulnerable to specific kinds of cyber-attack in a social network context. Therefore, the present study hypothesised the existence of direct effects of demographic variables on a person's vulnerability to social engineering attacks that have been considered in the study.

- **Hc2.** Certain user's demographics (age, gender, education level, major) are directly associated with the user's susceptibility to social engineering attacks.

7.3.5 Summary of the Study Hypotheses

Table 7.1 presents a summary of the 18 relationships that will be included in the conceptual model. The present research assumes that the relationships among the constructs on the proposed conceptual model could accurately predict users' susceptibility to SE.

Table 7.1 Summary of Research Hypotheses

H	Sub-H	
Ha1		Users with a higher level of involvement will be more susceptible to SE attacks.
	Hb1	The user's level of involvement positively influences the user's experience with cybercrime.
	Hb2	The user's level of involvement positively influences the user's trust.
Ha2		Users with a higher number of connections will be more susceptible to SE attacks.
	Hb3	The user's number of connections positively influences the user's level of involvement.
Ha3		Users with higher connections with known friends will be less susceptible to SE attacks.
Ha4		Users with a higher level of experience with social network will be less susceptible to SE attacks.
	Hb4	The user's social network experience positively influences the user's connections with known friends.
Ha5		Users with a higher level of risk perception will be less susceptible to SE attacks.
	Hb5	The user's perceived risk positively influences the user's competence.
Ha6		Users with a higher level of competence will be less susceptible to SE attacks.
Ha7		Users with a previous experience with cybercrime will be more susceptible to SE attacks.
	Hb6	The user's experience with cybercrime positively influences the user's perceived risk.
Ha8		Users with a higher level of trust will be more susceptible to SE attacks.
Ha9		Users with a higher level of motivation will be more susceptible to SE attacks.
	Hb7	The user's motivation positively influences the user's trust.
	Hb8	The user's motivation positively influences the user's level of involvement.
	Hb9	The user's motivation positively influences the user's experience with cybercrime.

7.4 The Proposed Conceptual Model

The previous section provides an explanation of the nature and the directions of the relationships among the constructs of the present study. Based on these 18 proposed hypotheses, a novel conceptual model has been developed in this study and presented in Figure 7.1. This conceptual model relies on four different perspectives which are believed to predict user behaviour toward social engineering victimisation in Facebook. Developing and validating such a holistic model provides a clear indication of the contribution of the present study.

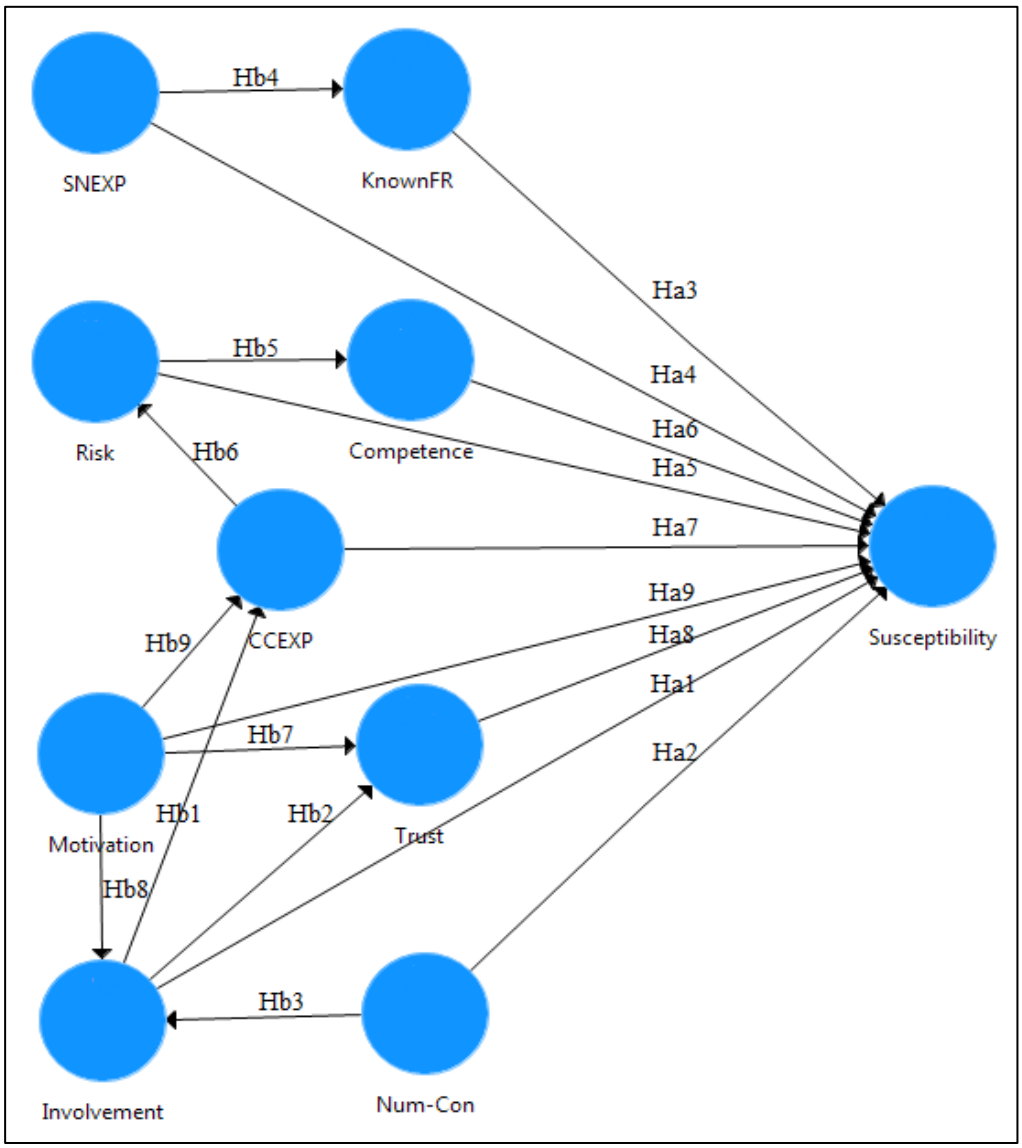


Figure 7.1 The Research Conceptual Model

7.5 Chapter Summary

The objective of developing the conceptual model in this chapter is to examine to what extent the framework factors and dimensions that have been identified in the first phase of the current research are integrated to predict users' vulnerability to social engineering attacks. However, the proposed conceptual model and hypothesised relationships need to be examined and evaluated to answer the second research question which is "RQ2: How can the selected factors in the user-centric framework be tested in order to indicate whether these factors and dimensions can predict the user's poor judgement of social engineering attacks on social networking sites?"

If users' vulnerability could be predicted using the proposed model, the present study can then be extended further by focusing on semi-automatically classifying social network users based on their Facebook features and habits. This classification will define less competent users, which can be protected by either targeting them by focused to need training or incorporating additional layers of countermeasures to their social network accounts. The next chapter will discuss the empirical study that has been conducted to examine if the proposed conceptual model can predict user vulnerability to social engineering attacks in social networks.

Chapter 8. SCENARIO-BASED EXPERIMENT RESULT

8.1 Overview

In the previous chapter, a research model has been proposed that aims to predict user vulnerability to social engineering (SE) victimisation. The model was empirically examined using a scenario-based experiment that has been conducted on 316 participants (after the mandatory screening steps were performed). This chapter will explain the approaches used to analyse the collected data to test the proposed model. Descriptive statistical results were obtained via statistical package for social sciences (SPSS v24) while partial least squares structural equation modelling (PLS-SEM) was used as a statistical modelling technique to test the model and its associated hypotheses using SmartPLS v3 as a software tool.

Section 8.2 provides a description of the data preparation methods. Section 8.3 gives an overview of the participants' profile and demographics. After that, the analysis phase started by conducting a reliability test on the constructs measurements as shown in Section 8.4, followed by the result of the exploratory factor analysis which presented in Section 8.5. The approach used to deal with second-order factors is explained in Section 8.6. Section 8.7 presents the assessment of the conceptual model which starts by the evaluation of the measurement model in Section 8.8, followed by the structural model assessment which includes the research hypotheses testing as described in Section 8.9. After that, the results of the impact of demographic variables and personality traits on user vulnerability are reported in Section 8.10.

Additionally, to provide a more in-depth analysis of the proposed model, a mediation test has been conducted and described in Section 8.11. Section 8.12 presents a brief assessment of the role of the type of social engineering-based attacks in people vulnerability. Finally, Section 8.13 concludes the chapter by highlighting the most significant findings.

8.2 Data Preparation Methods

In total, 580 responses were collected from two universities in Saudi Arabia. The first step of the data analysis is to make sure that the received data aligns with the conditions of structural equation modelling (Hair et al., 2010). As recommended by Hair et al. (2017), the collected data should be scrutinised before starting the analysis stage in order to guarantee that

the results of the analysis are as valid and reliable as possible. Next is the screening process that has been followed in the present study.

8.2.1 Cases Screening

8.2.1.1 Missing Data in Rows

According to Hair et al. (2017), if the amount of the missing data, in any case, exceed 15%, the observation should be removed from the dataset. Therefore, 236 responses have been identified and deleted due to the high percentage of missing data as clearly those respondents started the questionnaire but didn't complete it. The remaining dataset includes 344 responses.

8.2.1.2 Unengaged Responses

Potential unengaged responses or suspicious response patterns are identified when a respondent answers all 5-point-scale questions with "1" or either with the middle response "3" (Hair et al., 2017). These responses affect the validity and reliability of the study results negatively and thus needs to be eliminated. To find and deleted these responses, the standard deviation for each row has been calculated, and a low standard deviation can indicate answers with repeated values. For Example, respondents who answer all questions with "disagree" which was represented with "1" in the 5-point-scale. Therefore, 6 cases in the dataset have been deleted due to suspicious response patterns. Thus, the remaining responses in the dataset were 338 cases in total.

8.2.1.3 Outliers

Most of the survey collected data were on the form of a 5-point Likert-scale which hardly include outliers. Yet, the demographic variables have been tested for outliers. As the present study focuses on Saudi culture only, 22 participants have been indicated to be from other nationalities, therefore, removed from the dataset. Apart from that, no outliers have been found. The remaining dataset contains 316 responses.

8.2.2 Variables Screening

8.2.2.1 Missing Data in Columns

It has been observed that the dataset has some random missing data. Calculating a replacement value from a set of observations is the most common remedy for such limited missing data (Hair et al., 2010). When calculating the replacement value, Zhang (2016) recommended using mean substitution with continuous variables while mode substitution is more suitable with ordinal variables such as Likert-scale. Therefore, all the missing values in the following variables, attack_4a (2 values), attack_4b (3 values), Safe 2 (1 value), the personality trait number 4 (1 value), and the personality trait number 10 (1 value), have been

replaced by the most frequent observation, the mode value, of the surrounding items of the latent variable for the particular respondent.

8.2.2.2 Variable Coding

All the variables measurement items are designed to be in the same direction as (1) represents a low score while (5) represents a high score. Therefore, no reverse coding is needed in the dataset. Yet, one involvement variable (number of connections) is collected as a continuous number with the objective to not constraint the participants to a specific scale. Therefore, this continuous variable needs to be transformed into a scale. Based on the collected data, the number of connections has been categorised into 5-point-scale as follows: from 0 to 100 connections represents level "1", 101-200 → "2", 201-300 → "3", 301-400 → "4", more than 400 → "5".

8.2.2.3 Skewness and Kurtosis (Normality)

Skewness and kurtosis index were used to test if the collected data is normally distributed. Any violation of normality might affect the future test of means. Skewness test examines to what extent the distribution of the data is symmetrical while kurtosis measures the extent to which the data is too peaked or too flat (Hair et al., 2017). The observed result of the normality assessment in Table 8.1 showed a slight deviation from normality as the value of skewness and kurtosis for some items were slightly above and below the recommended criteria of – 1/+1. For instance, freq-min and con_scale have a skewness of 2.098 and 2.386 respectively which exhibit a slight degree of violation. Kurtosis index was mostly between the recommended criteria except for one item (IM1= 5.543) which considered too peaked. However, some researchers such as Hair et al. (2010) and Stevens (2009) argued that normal distribution of data is met if Skewness is between -2 to +2 and Kurtosis is between -7 to +7.

Moreover, Hair et al. (2010) stated that with a larger sample size (200 and more) researchers should be less concerned with non-normal data as their impact on study results are minimal. However, following the strict guideline of testing the normality of the data as suggested by Hair et al. (2017), it was concluded that the study data slightly deviate from being normal. Therefore, PLS-SEM is the structural equation modelling technique that will be used to analyse the present study dataset and model as unlike CB-SEM, this approach could be applied even with some violation of normality of distributions.

Table 8.1 Normality of the Distribution Assessment

			Skewness		Kurtosis	
Dimension	**Factor**	**Items**	**Statistic**	**Std. Error**	**Statistic**	**Std. Error**
Socio-psychological	Personality Traits	Neuroticism	0.148	0.137	-0.238	0.273
		Extraversion	-0.309	0.137	0.274	0.273
		Openness	0.269	0.137	-0.603	0.273
		Agreeableness	-0.036	0.137	-0.101	0.273
		Conscientiousness	-0.149	0.137	-0.073	0.273
Perceptual	Self-efficacy	SEF1	-0.200	0.137	-0.501	0.273
		SEF2	-0.353	0.137	-0.186	0.273
		SEF3	-0.622	0.137	-0.273	0.273
		SEF4	-0.331	0.137	-0.762	0.273
	Security Awareness	SA1	-0.415	0.137	-0.783	0.273
		SA3	0.546	0.137	-0.678	0.273
		SA2	-0.141	0.137	-1.115	0.273
		SA4	0.000	0.137	-1.271	0.273
	Privacy Awareness	PA1	0.158	0.137	-1.084	0.273
		PA2	-0.507	0.137	-0.620	0.273
		PA3	-0.624	0.137	-0.679	0.273
		PA4	-0.764	0.137	-0.370	0.273
	Cybercrime Experience	PE1_It	1.264	0.137	0.500	0.273
		PE3_OF	0.470	0.137	-0.986	0.273
		PE2_Ph	0.445	0.137	-1.076	0.273
		PE4_Har	0.411	0.137	-1.012	0.273
	Likelihood of threat	LT1	-0.158	0.137	-1.172	0.273
		LT2	-0.406	0.137	-0.891	0.273
		LT3	-0.542	0.137	-0.488	0.273
		LT4	-0.346	0.137	-0.531	0.273
	Severity of threat	ST1	-0.485	0.137	-0.829	0.273
		ST2	-0.626	0.137	-0.529	0.273
		ST3	-0.412	0.137	-0.728	0.273
		ST4	-0.913	0.137	0.133	0.273
Habitual	Involvement	Freq_com	0.478	0.137	-0.118	0.273
		Freq_min	2.098	0.137	3.482	0.273
	Number of connections	CON_SCALE	2.386	0.137	4.802	0.273
	Percentage of known Friends	KnownFriends	0.670	0.137	-1.059	0.273
	Social Network Experience	SN_exp	-0.497	0.137	-1.223	0.273
Socio-emotional	Hedonic Motivation	HM1	-1.124	0.137	1.539	0.273
		HM2	-1.115	0.137	1.370	0.273
		HM3	-0.505	0.137	-0.769	0.273
	Information motivation	IM1	-1.879	0.137	5.543	0.273
		IM2	-1.540	0.137	2.601	0.273
		IM3	0.163	0.137	-1.121	0.273
	Social Motivation	SM1	-0.354	0.137	-0.962	0.273
		SM2	-0.910	0.137	0.306	0.273
		SM3	0.156	0.137	-0.896	0.273
	Trust Provider	TP1	0.368	0.137	-0.396	0.273
		TP2	0.622	0.137	-0.106	0.273
		TP3	0.381	0.137	-0.472	0.273
		TP4	0.059	0.137	-0.485	0.273
	Trust Members	TM1	0.187	0.137	-0.295	0.273
		TM2	-0.043	0.137	-0.584	0.273
		TM3	0.019	0.137	-0.151	0.273
		TM4	-0.104	0.137	-0.213	0.273
SE Susceptibility	SE Attack 1	Attack_1a	1.390	0.137	0.763	0.273
		Attack_1b	1.162	0.137	-0.006	0.273
	SE Attack 2	Attack_2	0.984	0.137	-0.257	0.273
	SE Attack 3	Attack_3	0.828	0.137	-0.486	0.273
	SE Attack 4	Attack_4a	0.794	0.137	-0.784	0.273
		Attack_4b	0.800	0.137	-0.743	0.273

8.3 Participants' Demographics

This section summaries the profile of the participants of the scenario-based experiment which include diverse demographics regarding age, gender, education level, and academic major as explained in Section 8.3.1 and variance personality patterns as described in Section 8.3.2. Respondents' demographic characteristics and personality traits were further analysed in Section 8.10 in order to find out which demographics and personality traits are more associated with the issue of people vulnerability to social engineering victimisation in social networks.

8.3.1 Participants' Profiles

The descriptive analysis of participants' demographics in Table 8.2 revealed a variety of profiles in terms of gender (39% male, 61% female), education level, and education major. The majority of participants in the study were younger adults (age 18-24), representing 76% of the total participants. However, this was expected as the survey was undertaken on two universities in Saudi Arabia where students considered vital members of the higher education environment.

Table 8.2 Participants' Demographics

Demographic		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	123	38.9	38.9	38.9
	Female	193	61.1	61.1	100.0
	Total	316	100.0	100.0	
Age	18-24	240	75.9	75.9	75.9
	25-34	57	18.0	18.0	94.0
	35-44	14	4.4	4.4	98.4
	45-55	5	1.6	1.6	100.0
	Total	316	100.0	100.0	
Education Level	High school	187	59.2	59.2	59.2
	Bachelor's degree	112	35.4	35.4	94.6
	Master's degree	14	4.4	4.4	99.1
	Other, please specify	3	.9	.9	100.0
	Total	316	100.0	100.0	
Major	Computer Science/IT	124	39.2	39.2	39.2
	Engineering	32	10.1	10.1	49.4
	Business/ Administrative Sciences	38	12.0	12.0	61.4
	Medical Sciences	5	1.6	1.6	63.0
	Science	15	4.7	4.7	67.7
	Humanities and Arts	6	1.9	1.9	69.6
	Other, please specify	96	30.4	30.4	100.0
	Total	316	100.0	100.0	

8.3.2 Personality Traits

Participants were asked to rate 10 items related to their personalities on a 5-point Likert-scale (Table 8.3). The received answers to these 10 measurement items then summarised and calculated to form scores which supposed to identify participants' personality traits among 5 distinct personality patterns which are neuroticism, extraversion, openness to

experience, agreeableness, and conscientiousness. The guidelines of Rammstedt and John (2007) have been followed to compute the scores for the five personality traits. All negatively worded items must be reverse scored first. These items are item 1, item 3, item 4, item 5, and item 7. Then, for every single trait, the mean of its two items was calculated. For instance, this equation has been used to calculate the score of extraversion.

Extraversion = MEAN (Pert1_Ext(R), Per6_Ext)

After computing all the scores of the 5 personality traits, they are ready now for the analysis. Table 8.4 presents that the study participants were more likely to agree that they were conscientious, mostly agreeable, open to new experience, and slightly extroverted while appeared to be least likely to agree that they were neurotic and experienced negative or anxious states.

Table 8.3 Personality Traits Measurement Scale

ID	Questions	Trait
1	I am reserved	Ext(R)
2	I am generally trusting	Agr
3	I tend to be lazy	Con(R)
4	I am relaxed, handle stress well	Neu(R)
5	I have few artistic interests	Ope(R)
6	I am outgoing, sociable	Ext
7	I tend to find fault with others	Agr(R)
8	I do a thorough job	Con
9	I get nervous easily	Neu
10	I have an active imagination	Ope

R-(reverse scored items)

Table 8.4 Descriptive Statistics of the Five Personality Traits

	N	Minimum	Maximum	Mean	Std. Deviation
Neuroticism	316	1	5	2.82	0.821
Extraversion	316	1	5	3.19	0.642
Openness	316	2	5	3.39	0.800
Agreeableness	316	1	5	3.51	0.703
Conscientiousness	316	1	5	3.53	0.726

8.4 Reliability Tests

The reliability test is needed to measure the internal consistency of items to measure the intended construct. The most common measure to test the reliability of research constructs is Cronbach's alpha which should exceed 0.70 to represent an acceptable value of reliability (Hair et al., 2010). Table 8.5 shows that all the constructs in the study have sufficient and satisfactory reliability measures that exceeded the threshold of 0.70.

Table 8.5 Reliability Test of the Conceptual Model Constructs

Construct	Number of items	Cronbach's Alpha
Social Motivation	3	0.709
Hedonic Motivation	3	0.710
Information Motivation	3	0.728
Trust Provider	4	0.921
Trust Members	4	0.885
Self-efficacy	4	0.826
Security Awareness	4	0.820
Privacy Awareness	4	0.858
Perceived Severity of Threat	4	0.828
Perceived Likelihood of Threat	4	0.712
Cybercrime Experience	4	0.776
Involvement	3	0.749
Susceptibility	6	0.921

8.5 Exploratory Factor Analysis Using SPSS

Exploratory factor analysis (EFA) was carried out after confirming the reliability of the constructs. The goal of conducting the factor analysis was to examine the interrelationships among the study variables to identify the group of variables that are highly correlated to form and represent a single factor (Hair et al., 2010). This process could help guarantee that the used measurement items would highly load on its intended construct which ultimately leads to extract their matching theoretical factor. SPSS v24 tool was used to analyse the study items, and the principal component approach was employed as an extraction method with varimax rotation. This method is considered the default and the most widely used approach when the objective of the study is to summarise the variables to the minimum number of factors for prediction purposes (Costello & Osborne, 2005; Hair et al., 2010).

While factor analysis is mostly performed only on variables that are measured by scales (Hair et al., 2010), the socio-psychological factors are not included in the EFA as they are categorical variables and not measured by Likert-scales. Thus, three perspectives (habitual, perceptual, and socio-emotional) and 13 factors are involved in the factor analysis. Due to this large number of factors, it was easier to start the exploratory factors analysis for each perspective separately first. Then, analysing the remaining factors together to make sure the loading and cross loading is valid. Moreover, Even though the factor loadings of 0.50 and higher is generally considered acceptable (Hair et al., 2010), a more restricted threshold of 0.70 was considered in the current study. Furthermore, any item with cross-loadings greater than 0.40 was eliminated from the dataset as suggested by Ferguson and Cox (1993).

8.5.1 Initial Factor Analysis

The result of the initial factor analysis, which can be found in Appendix J, indicated six factors in the perceptual perspective. The result revealed that some items have low loadings on their intended factors such as the case of SA1, PA1, PA2, and LT4. Additionally, some very high cross-loadings were found in PA1 (0.778), and PA2 (0.596). Therefore, these items have been deleted from the dataset.

According to the socio-emotional perspective, the result of the initial factor analysis indicated five factors and revealed that some items have low loadings (less than 0.70) on their intended items such as HM3, SM2, TP1, and TP4. In addition, other elements have been noticed to have high cross-loadings on other factors such as HM3, IM3, SM2, and TP4. Since TP4 have two issues related to low and cross loading, TP1 has been kept and TP4 was deleted first. The result of the final factor analysis in Table 8.6 shows that deletion of TP4 has fixed the low loading of TP1. In the habitual aspect, level of involvement is the only factor with multiple measurement items. Therefore, the items of this factor will be analysed together with all the other factors in the final factor analysis test.

8.5.2 Final EFA Test

The final factor analysis was conducted on all the constructs of the three perspectives (habitual, perceptual, and socio-emotional) in the study. The result of the final factor analysis in Table 8.6 shows that all items loadings are above the threshold of 0.7 in their intended factors. The Cronbach's alpha for all the factors were 0.7 or higher, except for information motivation factor (0.494) where it has not met the criteria of reliability. Therefore, information motivation factor has been removed from the study model. The remaining number of factors that were measured using multiple-items are 12 in the model.

Table 8.6 The Final Factor Analysis Test

	Susceptibility	Involvement	Hedonic	Info	Likelihood	Privacy	CCEXP	Security	Self-efficacy	Social	Severity	TrustM	TrustP
Cronbach's Alpha	**0.877**	**0.706**	**0.727**	**0.494**	**0.829**	**0.710**	**0.777**	**0.745**	**0.800**	**0.709**	**0.854**	**0.886**	**0.862**
Attack_1a	0.866												
Attack_1b	0.839												
Attack_2	0.806												
Attack_3	0.739												
Attack_4a	0.725												
Attack_4b	0.721												
Freq_com		0.908											
Freq_min		0.847											
HM1			0.854										
HM2			0.915										
IM1				0.820									
IM2				0.810									
LT1					0.822								
LT2					0.914								
LT3					0.853								
PA3						0.882							
PA4						0.879							
PE1_It							0.862						
PE2_Ph							0.704						
PE3_OF							0.736						
PE4_Har							0.723						
SA2								0.849					
SA3								0.761					
SA4								0.828					
SEF1									0.719				
SEF2									0.837				
SEF3									0.762				
SEF4									0.843				
SM1										0.905			
SM3										0.852			
ST1											0.724		
ST2											0.924		
ST3											0.851		
ST4											0.834		
TM1												0.833	
TM2												0.831	
TM3												0.886	
TM4												0.894	
TP1													0.842
TP2													0.923
TP3													0.890

8.6 Second-Order Constructs

Our proposed conceptual model includes four second-order formative constructs which are risk, competence, trust, and motivation. Repeated indicator approach was used to measure the formative constructs values. This method recommends using the same number of items on all the first order factors in order to guarantee that all first-order factors have the same weight on the second order factors and to ensure no weight bias are existed (Ringle, Sarstedt, & Straub, 2012). Therefore, before testing the measurement model, it is mandatory to make sure that all first-order factors have the same number of items and delete any extra items based on the lowest loading first and see the effects on the loading of the other items before removing the rest. For example, Risk has two first order dimensions which are likelihood of threat that has three items and severity of threat which has four items. Therefore, ST1 the lowest loading among the severity items has been removed.

Also, Competence has three first-order factors which are self-efficacy (4 items), security (3 items), and privacy (2 items). SA3 was deleted as it has the lowest loading on the security items. Similarly, among the self-efficacy items, SEF1 was removed first, and then the deletion effect was checked on the other items' loadings and then decided to delete SEF2 as it has the lowest loading among the remaining items. Finally, the factor of trusting social network members has four items while trusting social network provider has three items only, therefore, TM2 has also been removed as it represents the lowest loading item.

8.7 The Conceptual Model Assessment

Structural equation modelling is the statistical technique that has been used to examine the study's conceptual model. The SmartPLS v3 software package (Ringle et al., 2015) was used to analyse the present study model. The part of the conceptual model that includes the relations between the measurement items and their associated factors is called the measurement model, while the hypothesised relationships among the different factors is called the structural model (Tabachnick & Fidel, 2013). Each one of these models has a particular set of assessment criteria that should be checked. Section 8.8 will show the result of the assessment of the measurement model while section 8.9 will present the structural model evaluation result.

It is worth noting that the study model includes 15 reflective factors (in which 12 are measured using multiple-items, three are measured using single-item). Nine of the 12 multiple-

item reflective factors are treated as first-order factors (dimensions) that form four second-order formative constructs. Table 8.7 summarises the factors that are included in the model.

Table 8.7 Types of the Model Factors

Formative factors	First-order Reflective factors (multiple-items)	Reflective factors (multiple-items)	Reflective factors (single-item)
Perceived risk	Perceived likelihood of threat	Involvement	Percentage of known friends
	Perceived severity of threat		
Competence	Security	Cybercrime experience	Number of connections
	Privacy		
	Self-efficacy		
Trust	Trust provider	Susceptibility	Social network experience
	Trust members		
Motivation	Hedonic		
	Social		

8.8 Measurement Model's Assessment

The measurement model assessment is mainly conducted to ensure the reliability and validity of the model constructs. These reliability and validity tests should only apply to constructs that are measured by multiple items. These tests are not considered appropriate to be used with single-item constructs, e.g., number of connections in the model, where the indicator's outer loading is normally fixed at 1.00 (Hair et al., 2017).

Figure 8.1 shows the study's measurement model, which includes all the constructs along with their indicators' outer loadings. In the present study, two types of measurement models exist which are reflective measurement model and formative measurement model. Each model has a different criterion to be assessed. This study has followed all the steps of reflective and formative measurement model assessment as suggested by Hair et al. (2017). It is also worth noting that in the measurement model, no connections were established between the constructs to test the relationships between the independent variables. As the four formative constructs values will be estimated in this stage, and the relationships between the constructs will be demonstrated in the structural model in Section 8.9.

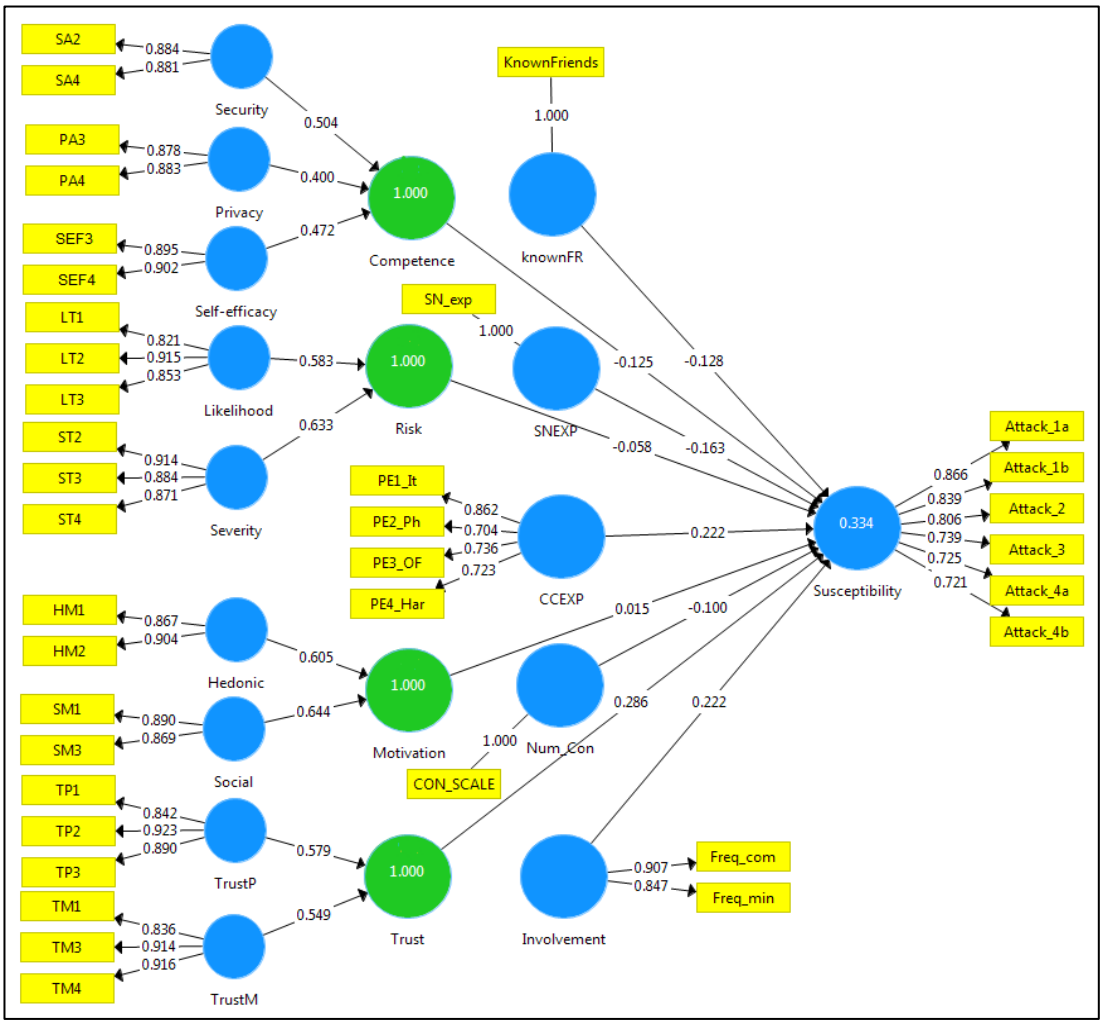


Figure 8.1 The Measurement Model

8.8.1 Reflective Measurement Model Assessment

8.8.1.1 Internal Consistency Reliability

Internal consistency is the test that is used to ensure that all the items of a particular instrument measure the same latent concept (Sekaran & Bougie, 2010). As recommended by Hair et al. (2017), both composite reliability and Cronbach Alpha should be measured as these two tests could be considered as the upper and lower bound of internal consistency reliability. The cut-off value for the acceptable reliability to evaluate the internal consistency should be above 0.70, even though the present research is considered exploratory where the reliability of 0.60 would be regarded as acceptable (Hair et al., 2017).

The result of the model analysis in Table 8.8 reveals that the composite reliability was acceptable for all constructs as they were above the threshold of 0.70. Additionally, the Cronbach Alpha which is the traditional standard for assessing internal reliability was also above 0.70 for most constructs.

8.8.1.2 Convergent Validity

Convergent validity is established when a particular item highly correlates with the other items that measure the same concept (Sekaran & Bougie, 2010). Convergent validity can be assessed by two different measures which are indicators' outer loadings on their intended construct that should be above 0.70, and average variance extracted (AVE) which should be above 0.50 (Hair et al., 2017).

Figure 8.1 presented all the constructs along with their indicators' outer loadings which showed that all the indicators' outer loadings for all the constructs were above 0.70. Furthermore, the result in Table 8.8 revealed that the AVE for all constructs was above the threshold of 0.5. Thus, the convergent validity of the model's reflective constructs was confirmed.

Table 8.8 Convergent Validity Tests

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
CCEXP	0.777	0.923	0.843	0.576
Hedonic	0.727	0.738	0.879	0.784
Involvement	0.706	0.733	0.870	0.771
Likelihood	0.829	0.834	0.898	0.746
Num_Con	1.000	1.000	1.000	1.000
Privacy	0.710	0.710	0.873	0.775
SNEXP	1.000	1.000	1.000	1.000
Security	0.715	0.715	0.875	0.778
Self-efficacy	0.762	0.763	0.894	0.808
Severity	0.868	0.868	0.919	0.792
Social	0.709	0.712	0.873	0.774
Susceptibility	0.877	0.896	0.905	0.616
TrustM	0.867	0.868	0.919	0.791
TrustP	0.862	0.862	0.916	0.784
knownFR	1.000	1.000	1.000	1.000

8.8.1.3 Discriminant Validity

Discriminant validity is the extent to which a particular construct is distinctly different from other constructs (Sekaran & Bougie, 2010). Hair et al. (2017) recommended using three criteria to assess discriminant validity which are Fornell-Larcker criterion, Heterotrait monotrait ratio (HTMT), and Cross loadings.

a. Fornell-Larcker criterion

This criterion relies upon the comparison between the square root of the AVE for a construct and its correlations with other constructs in the model (Hair et al., 2017). Discriminant validity is established if the square root of AVE is higher than the construct's other correlations. The result in Table 8.9 indicates that all constructs are valid as the square

root of AVE (bold values) for each reflective construct appeared to be higher than the construct's correlation with other constructs.

Table 8.9 Fornell-Larcker Criterion

	CCEXP	Hedonic	Involve	Likelihood	Num_Con	Privacy	SNEXP	Security	Efficacy	Severity	Social	Suscept	TrustM	TrustP	knownFR
CCEXP	**0.759**														
Hedonic	0.046	**0.886**													
Involve	0.198	0.013	**0.878**												
Likelihood	0.237	-0.057	0.077	**0.864**											
Num_Con	0.096	0.018	0.210	-0.024	1.000										
Privacy	-0.042	-0.036	-0.060	0.129	-0.136	**0.880**									
SNEXP	-0.129	-0.002	-0.100	0.022	0.104	-0.068	1.000								
Security	0.099	-0.023	0.134	0.026	0.041	0.300	-0.019	**0.882**							
Efficacy	-0.011	0.023	0.059	-0.109	0.133	0.173	0.076	0.371	**0.899**						
Severity	0.065	0.084	-0.011	0.351	-0.013	0.256	0.092	0.115	0.187	**0.890**					
Social	0.244	0.281	0.269	-0.060	0.107	-0.220	-0.109	0.087	0.120	-0.002	**0.880**				
Suscept	0.298	0.010	0.330	0.066	-0.044	-0.101	-0.303	0.026	-0.039	-0.104	0.296	**0.785**			
TrustM	-0.022	0.119	0.161	-0.041	0.033	0.058	-0.073	0.193	0.194	0.071	0.210	0.196	**0.889**		
TrustP	0.183	0.144	0.305	0.026	0.039	-0.010	-0.145	0.244	0.286	0.082	0.345	0.434	0.571	**0.886**	
knownFR	-0.044	-0.047	-0.012	-0.069	0.044	-0.102	0.302	0.021	0.173	0.098	-0.104	-0.221	-0.042	-0.073	1.000

b. Heterotrait monotrait ratio (HTMT)

As suggested by Hair et al. (2017), HTMT is the most critical discriminant validity criteria where all HTMT ratios should be below the most conservative threshold of 0.85. Table 8.10 provides evidence that discriminant validity was confirmed for all reflective constructs.

Table 8.10 HTMT Ratio

	CCEXP	Hedonic	Involve	Likelihood	Num_Con	Privacy	SNEXP	Security	efficacy	Severity	Social	Suscept	TrustM	TrustP	knownFR
CCEXP															
Hedonic	0.161														
Involve	0.248	0.102													
Likelihood	0.316	0.086	0.108												
Num_Con	0.141	0.021	0.254	0.043											
Privacy	0.123	0.056	0.079	0.170	0.162										
SNEXP	0.114	0.050	0.114	0.106	0.104	0.081									
Security	0.139	0.033	0.199	0.050	0.072	0.422	0.022								
efficacy	0.119	0.046	0.090	0.139	0.152	0.236	0.088	0.502							
Severity	0.125	0.107	0.055	0.414	0.013	0.327	0.099	0.146	0.231						
Social	0.316	0.383	0.378	0.094	0.131	0.310	0.129	0.124	0.165	0.043					
Suscept	0.293	0.080	0.405	0.131	0.056	0.121	0.315	0.045	0.077	0.131	0.358				
TrustM	0.063	0.144	0.205	0.067	0.086	0.074	0.079	0.246	0.240	0.082	0.269	0.226			
TrustP	0.198	0.175	0.394	0.065	0.043	0.026	0.157	0.311	0.353	0.095	0.439	0.489	0.662		
knownFR	0.091	0.054	0.056	0.100	0.044	0.122	0.302	0.055	0.198	0.105	0.125	0.239	0.045	0.078	

c. Cross Loadings

Discriminant validity is established if each indicator loads higher on its intended construct compared to its cross-loadings with other constructs. The cross loadings table in

Appendix K shows the loading and cross-loadings for each item in the present study model. Overall, the result of the indicators' cross-loadings together with the earlier findings of the Fornell-Larcker criterion and HTMT provide clear evidence for the reflective constructs' discriminant validity.

8.8.2 Formative Measurement Model Assessment

8.8.2.1 Collinearity of Formative Indicators

Examining the existence of multicollinearity among the formative dimensions is considered one of the critical evaluations of the formative measurement model. Unlike the case with reflective indicators, a high level of correlations among formative indicators (dimensions) is not predicted and considered a sign of a collinearity problem (Hair et al., 2017), as high levels of multicollinearity disclose the low level of contribution of the dimensions to form the second-order formative construct (Diamantopoulos & Winklhofer, 2001).

To avoid collinearity issues, the variance inflation factor (VIF) value should be below the suggested threshold of 5 (Hair et al., 2017), or, preferably, below the strict cut-off point of 3.3 (Petter et al., 2007). Table 8.11 shows that the multicollinearity level is very small among the dimensions of Risk, Competence, Trust, and Motivation. This distinction among the dimensions of each construct makes it clear that these constructs are undoubtedly formative and that there is no violation to the multicollinearity assumption.

Table 8.11 Collinearity Test (VIF) of Formative Indicators

	Risk	Competence	Trust	Motivation
Likelihood	1.141			
Severity	1.141			
Security		1.242		
Privacy		1.104		
Self-efficacy		1.165		
TrustP			1.484	
TrustM			1.484	
Hedonic				1.086
Social				1.086

8.8.2.2 The Significance of Formative Indicators

An indicator's outer weight is an important criterion to assess the importance and relevance of each indicator on forming its latent formative factor. Table 8.12 provides a summary of the bootstrapping results which can be used to evaluate the formative indicators' importance and relevance as suggested by Hair et al. (2017). The result shows that all the formative indicators are significant ($p<0.05$) and none of their confidence intervals has a zero

value between the lowest and highest levels. Thus, the result provides empirical evidence to retain all formative indicators in the model.

Table 8.12 Formative Constructs Outer Weights Significance Results

Construct	Indicators	Outer weights	Outer loadings	T-Value	P-Value	95% Bca Confidence Interval		Sig.?
Risk	LT1	0.209	0.649	17.244	<0.001	0.185	0.233	Yes
	LT2	0.237	0.733	23.758	<0.001	0.220	0.257	Yes
	LT3	0.228	0.703	25.352	<0.001	0.213	0.248	Yes
	ST2	0.238	0.749	24.669	<0.001	0.222	0.261	Yes
	ST3	0.235	0.738	23.389	<0.001	0.219	0.258	Yes
	ST4	0.239	0.749	25.454	<0.001	0.223	0.260	Yes
Competence	PA3	0.225	0.552	9.307	<0.001	0.167	0.266	Yes
	PA4	0.230	0.563	8.105	<0.001	0.164	0.275	Yes
	SA2	0.287	0.709	14.067	<0.001	0.254	0.335	Yes
	SA4	0.284	0.701	15.641	<0.001	0.254	0.325	Yes
	SEF3	0.259	0.644	13.207	<0.001	0.223	0.297	Yes
	SEF4	0.267	0.665	12.190	<0.001	0.227	0.317	Yes
Trust	TM1	0.202	0.760	25.393	<0.001	0.188	0.220	Yes
	TM3	0.207	0.791	34.338	<0.001	0.196	0.220	Yes
	TM4	0.209	0.796	29.712	<0.001	0.197	0.223	Yes
	TP1	0.214	0.778	26.504	<0.001	0.201	0.235	Yes
	TP2	0.222	0.803	28.424	<0.001	0.208	0.239	Yes
	TP3	0.217	0.789	28.267	<0.001	0.205	0.235	Yes
Motivation	HM1	0.312	0.641	14.697	<0.001	0.271	0.348	Yes
	HM2	0.370	0.746	23.901	<0.001	0.340	0.402	Yes
	SM1	0.382	0.745	20.360	<0.001	0.348	0.418	Yes
	SM3	0.350	0.686	18.801	<0.001	0.316	0.387	Yes

8.8.3 Summary of the Measurement Model Assessment Results

In the measurement model, the reliability and validity of the reflective and formative variables have been tested. Table 8.13 summarises the assessment results of the reflective and formative measuerment models which indicate that all validity and reliability assessment criteria have been met. However, the model includes four second-order formative constructs that were formed from multiple first-order reflective constructs using the repeated indicator approach. In this case, the four formative constructs in the model will have an R^2 value of 100% as the explained variation from their first-order variables. This prevents exploring whether other constructs in the model have any relationships with these second-order constructs (Ringle et al., 2012). To solve this problem, Hair et al. (2017) suggested acquiring the latent variable scores for the first-order reflective constructs from the measurement model and using them as indicators of the second–order formative constructs in the structural model when estimating the constructs' relationship significance.

Table 8.13 Summary of the Measurement Model Assessment Results

Measurement Model	Assessment Tests	Met Assessment Criteria?
Reflective measurement model	Internal Consistency Reliability	Yes
	Convergent Validity	Yes
	Discriminant Validity	Yes
Formative measurement model	Collinearity of Formative Indicators	Yes
	The Significance of Formative Indicators	Yes

8.9 Structural Model's Assessment

After analysing and evaluating the measurement model, the structural model should be assessed according to the guidelines of the PLS analysis. The structural model would be evaluated based upon the results obtained from the standard PLS-SEM algorithm, bootstrapping procedure, and blindfolding procedure (Hair et al., 2017). Figure 8.2 shows the structural model path coefficient results of this study which include nine independent variables (IVs) and one dependent variable (DV). In the study model, the nine independent variables consist of three exogenous variables and six endogenous variables. The endogenous variables mean that some other variables within the Model are influencing their values, while the exogenous variables are those independent variables that are not affected by other variables in the model (Götz et al., 2010). The structural model is able to assess the model's predictive ability and to examine the significance of relationships between the model's constructs. The assessment of the structural model involves the following testing steps.

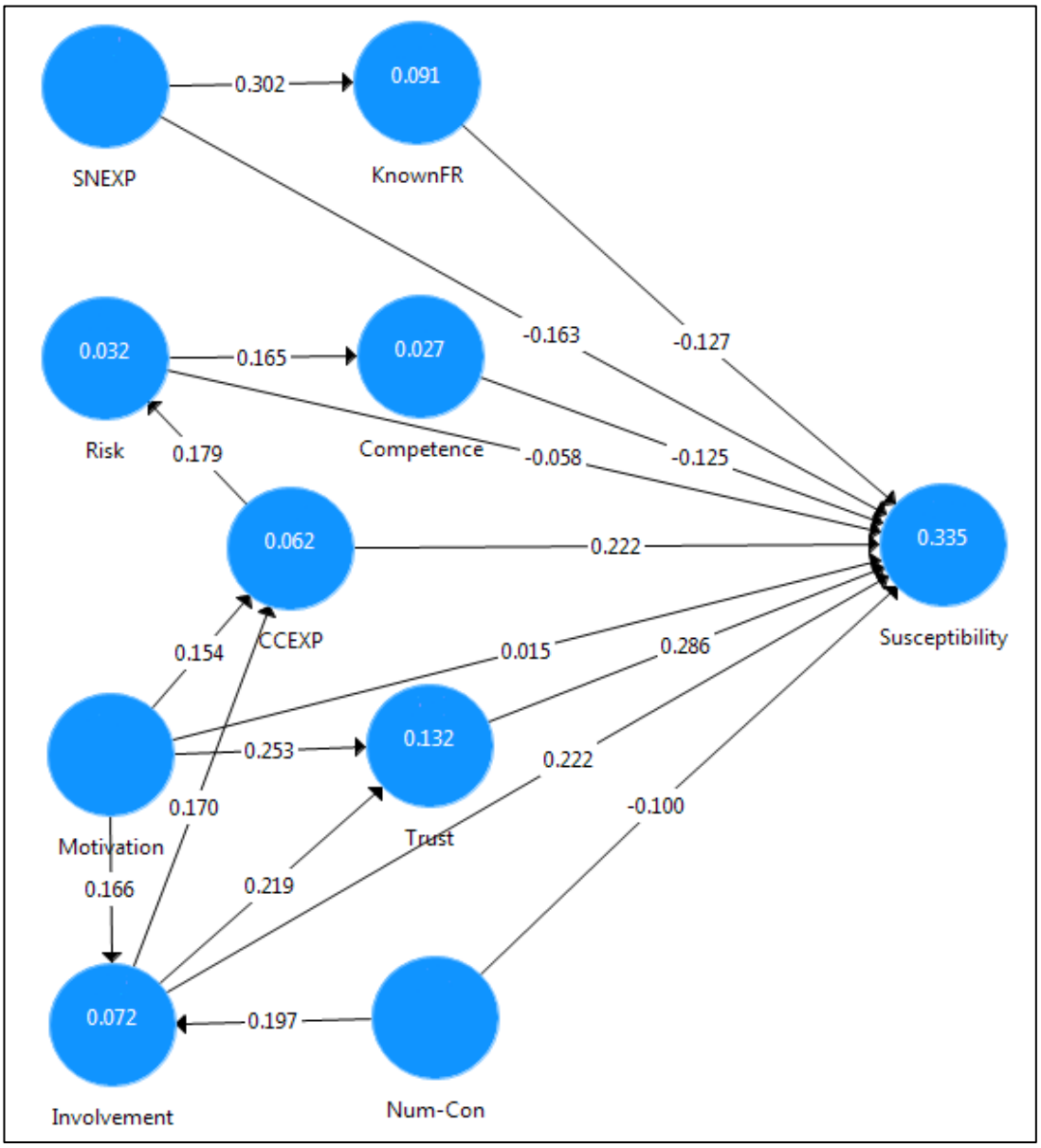


Figure 8.2 The Structural Model with Path Coefficients

8.9.1 Assessing Collinearity

This step is vital to determine if there are any collinearity issues among the predictors of each endogenous construct. Failing to do so could lead to a biased path coefficient estimation if a critical collinearity issue exists among the construct predictors (Hair et al., 2017). Table 8.14 presents all the endogenous constructs (represented by the columns) which indicate that VIF values for all predictors of each endogenous construct (represented by the rows) are below the threshold of 5. Thus, no collinearity issues exist in the structural model.

Table 8.14 Collinearity Assessment (VIF) of the Structural Model

	CCEXP	Competence	Involvement	KnownFR	Risk	Susceptibility	Trust
CCEXP					1.000	1.125	
Competence						1.115	
Involvement	1.034					1.170	1.034
KnownFR						1.112	
Motivation	1.034		1.006			1.152	1.034
Num-Con			1.006			1.075	
Risk		1.000				1.077	
SNEXP				1.000		1.162	
Trust						1.255	

8.9.2 Assessing Path Coefficients (Hypotheses Testing)

The structural model relationships are examined by running the PLS-SEM algorithm which provides the estimates (i.e., path coefficients) that are used to determine the direction and strength of the hypothesised relationships. The standardized value of path coefficient usually ranges between -1 and +1, where an estimated value close to 0 generally represents a not significant relationship (Hair et al., 2017). A path coefficient close to +1 represents a strong positive correlation, while an estimated value close to -1 represents a strong negative correlation.

Yet, to statistically examine if a relationship is significant, a bootstrapping algorithm must be running using SmartPLS as this procedure provides an empirical calculation of test statistic (t-value) and probability value (p-value) for all the structural model relationship paths (Hair et al., 2017). A t-value of 2.57 or more reflects a statistically significant relationship at 1% error probability, while a t-value of 1.96 or more is considered significant at 5% error probability, as suggested by Hair et al. (2017).

Table 8.15 presents a summary of the study's proposed hypotheses whose significance will be assessed in this section using the PLS-SEM algorithm and bootstrapping algorithm. To examine the assumptions, the first nine hypotheses (group a) will be tested with regards to the direct and total effects of the independent variables on the dependent variable, which is the user's susceptibility to social engineering victimisation. Then, the direct impact of each path among constructs will be examined in order to test group b hypotheses by considering the estimates of path coefficient for each relationship.

Table 8.15 Summary of Study Hypotheses

H	Sub-H	
Ha1		Users with a higher level of involvement will be more susceptible to SE attacks.
	Hb1	The user's level of involvement positively influences the user's experience with cybercrime.
	Hb2	The user's level of involvement positively influences the user's trust.
Ha2		Users with a higher number of connections will be more susceptible to SE attacks.
	Hb3	The user's number of connections positively influences the user's level of involvement.
Ha3		Users with higher connections with known friends will be less susceptible to SE attacks.
Ha4		Users with a higher level of experience with social network will be less susceptible to SE attacks.
	Hb4	The user's social network experience positively influences the user's connections with known friends.
Ha5		Users with a higher level of risk perception will be less susceptible to SE attacks.
	Hb5	The user's perceived risk positively influences the user's competence.
Ha6		Users with a higher level of competence will be less susceptible to SE attacks.
Ha7		Users with a previous experience with cybercrime will be more susceptible to SE attacks.
	Hb6	The user's experience with cybercrime positively influences the user's perceived risk.
Ha8		Users with a higher level of trust will be more susceptible to SE attacks.
Ha9		Users with a higher level of motivation will be more susceptible to SE attacks.
	Hb7	The user's motivation positively influences the user's trust.
	Hb8	The user's motivation positively influences the user's level of involvement.
	Hb9	The user's motivation positively influences the user's experience with cybercrime**.**

8.9.2.1 Testing Constructs Impact on Users' Susceptibility

The path coefficient provides estimates of the direct impact that each construct has on user susceptibility to cyber-attack. The result of the direct effect test in Table 8.16 shows that trust ($t=5.202$, $p<0.001$) is the highest variable that predicts the user's susceptibility to SE victimisation, followed by user's involvement ($t=5.002$, $p<0.001$), cybercrime experience ($t=3.736$, $p<0.001$), social network experience ($t=-3.015$, $p<0.01$), and percentage of known friends among Facebook connections ($t=-2.735$, $p<0.01$). The direct effects of user competence to deal with threats ($t=-2.474$, $p<0.05$) and the number of connections ($t=-2.428$, $p<0.05$) were relatively small, they were still statistically significant in explaining the target variable. However, the impact of the number of connections on users' susceptibility was negative which opposes hypothesis (Ha2) that claims that this relationship is positive.

Most importantly, the result indicated that perceived risk and motivation have no direct effect on a user's vulnerability ($p>0.05$). This could be caused by the fact that both factors are second-order formative variables, while their first order factors have different direction effects on a user's susceptibility. As can be seen from the result of the regression analysis in Table 8.17, perceived risk is the second order factor of perceived severity of threat which has a significant negative effect on the user's susceptibility and perceived likelihood of threat which has a positive impact on user's susceptibility. Therefore, their joint effect logically will be not significant, because the opposite effects of the two dimensions of

perceived risk have cancelled each other. Thus, Ha5 could be considered as partially supported.

Table 8.16 Path Coefficient Results (Significance Test- Group a)

Hypo	Relationship	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Decision
Ha1	Involvement → Susceptibility	0.222	0.063	5.002	<0.001	0.098	0.344	Supported***
Ha2	Num-Con → Susceptibility	-0.100	0.041	2.428	0.015	-0.181	-0.019	Rejected [a]
Ha3	KnownFR → Susceptibility	-0.127	0.047	2.735	0.006	-0.222	-0.037	Supported**
Ha4	SNEXP → Susceptibility	-0.163	0.054	3.015	0.003	-0.268	-0.053	Supported**
Ha5	Risk → Susceptibility	-0.058	0.051	1.142	0.254	-0.157	0.041	Rejected
Ha6	Competence → Susceptibility	-0.125	0.050	2.474	0.013	-0.224	-0.029	Supported*
Ha7	CCEXP → Susceptibility	0.222	0.059	3.736	<0.001	0.105	0.340	Supported***
Ha8	Trust → Susceptibility	0.286	0.055	5.202	<0.001	0.177	0.392	Supported***
Ha9	Motivation → Susceptibility	0.015	0.043	0.346	0.729	-0.068	0.099	Rejected

Statistically significant at ***p<0.001, **p<0.01, *p<0.05; [a] statistically significant but in the opposite direction to that hypothesised

Table 8.17 Regression Analysis of Perceived Risk and Motivation Dimensions

Factors	Dimensions	Std. Beta	t	Sig.
Perceived Risk	Severity	-0.146	-2.446	0.015
	Likelihood	0.117	1.958	0.051
Motivation	Hedonic	-0.080	-1.423	0.156
	Social	0.319	5.680	<0.001

Dependent Variable: Susceptibility

The situation with Motivation is similar as it is also a second-order formative factor and its first order factors (hedonic and social) have an opposite effect on users' susceptibility. Table 8.17 presents the result of the regression analysis of first-order factors for the motivation construct. The result provides evidence that hedonic motivation is negatively related to the user's susceptibility while social motivation is positively associated with user's susceptibility. However, when the two dimensions of motivation were aggregated to create one index to measure the total effect of a user's motivation (both direct and indirect), as illustrated in Table 8.18, the model revealed a significant predictor of users' susceptibility ($t=3.854$, $p<0.001$). Thus, the direct effect of motivation on user susceptibility is statistically rejected, while the total effect of motivation on users' susceptibility is statistically significant and considered one of the strongest predictors in the study model.

Evaluating the total effect of a particular construct on user susceptibility is considered useful, especially if the goal of the study is to explore the impact of the relationships between different drivers to predict one latent construct (Hair et al., 2017). The total impact includes both the construct's direct effect and indirect effects through mediating constructs in the model.

The total effect analysis in Table 8.18 revealed that most of the constructs have a significant overall impact on user susceptibility ($p<0.05$). Although the number of connections has been proven to have a significant negative direct effect on user susceptibility, its total effect when considering all the direct and indirect relationships seems to be very low and not significant ($t=-0.837$, $p>0.05$). Furthermore, both the direct and total effect of perceived risk has been found to be not substantial ($t=-1.559$, $p>0.05$).

Table 8.18 Total Effects Significance Testing Results

Hypo	Relationship	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Sig.?
Ha1	Involvement → Susceptibility	0.320	0.064	5.002	<0.001	0.188	0.441	Yes***
Ha2	Num-Con → Susceptibility	-0.037	0.044	0.837	0.403	-0.122	0.050	No
Ha3	KnownFR → Susceptibility	-0.127	0.047	2.735	0.006	-0.224	-0.041	Yes**
Ha4	SNEXP → Susceptibility	-0.201	0.050	4.028	<0.001	-0.302	-0.105	Yes***
Ha5	Risk → Susceptibility	-0.078	0.050	1.559	0.119	-0.176	0.024	No
Ha6	Competence → Susceptibility	-0.125	0.050	2.474	0.013	-0.218	-0.023	Yes*
Ha7	CCEXP → Susceptibility	0.208	0.059	3.552	<0.001	0.090	0.322	Yes***
Ha8	Trust → Susceptibility	0.286	0.055	5.202	<0.001	0.180	0.395	Yes***
Ha9	Motivation → Susceptibility	0.173	0.045	3.854	<0.001	0.082	0.257	Yes***

Statistically significant at ***p<0.001; **p<0.01; *p<0.05.

8.9.2.2 Testing Constructs Impact On Each Other

The rest of the hypotheses (group b) aim to examine the relationships between the independent constructs of the study model, which will be tested according to estimates of the path coefficient between the related constructs. Table 8.19 shows that all nine hypotheses are statistically significant ($p<0.05$). This also shows that the most substantial relationship was between social network experience and the percentage of known friends among Facebook connections ($t=6.091$, $p<0.001$), followed by the favourable impact motivation and level of involvement have on increasing users trust (with t-value=4.821, and t-value=3.914, respectively).

Furthermore, motivation ($t=3.640$, $p<0.001$) and the number of connections ($t=3.106$, $p<0.01$) are two factors found to increase users' level of involvement in the network. Level of involvement also plays a notable role in raising people's previous experience with cybercrime ($t=2.532$, $p<0.05$), while past cybercrime expertise significantly increases people's perceived risk associated with using Facebook ($t=2.968$, $p<0.01$). Nevertheless, the contribution of perceived risk in raising user competence level to deal with online threats was not very strong, although considered statistically significant ($t=2.241$, $p<0.05$).

Table 8.19 Path Coefficient Results (Significance Test- Group b)

Hypo	Relationship	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Decision
Hb1	Involvement → CCEXP	0.170	0.067	2.532	0.011	0.031	0.295	Supported*
Hb2	Involvement → Trust	0.219	0.056	3.914	<0.001	0.105	0.327	Supported***
Hb3	Num-Con → Involvement	0.197	0.063	3.106	0.002	0.080	0.324	Supported**
Hb4	SNEXP → KnownFR	0.302	0.050	6.091	<0.001	0.201	0.394	Supported***
Hb5	Risk → Competence	0.165	0.074	2.241	0.025	0.020	0.311	Supported*
Hb6	CCEXP → Risk	0.179	0.060	2.968	0.003	0.062	0.294	Supported**
Hb7	Motivation → Trust	0.253	0.053	4.821	<0.001	0.150	0.353	Supported***
Hb8	Motivation → Involvement	0.166	0.046	3.640	<0.001	0.078	0.256	Supported***
Hb9	Motivation → CCEXP	0.154	0.055	2.795	0.005	0.046	0.264	Supported**

Statistically significant at ***p<0.001; **p<0.01; *p<0.05.

8.9.3 The Coefficient of Determination - R^2

The coefficient of determination is a traditional criterion that is used to evaluate the structural model's predictive power. In this study, this coefficient measure will represent the joint effect of all the model variables in explaining the variance in a person's susceptibility to SE attacks. According to Hair et al. (2017), the acceptable R^2 value is hard to determine as it might vary depending on the study discipline and the model complexity. Cohen (1988) has suggested a rule of thumb to assess the R^2 values for models with several independent variables which are: 0.26, 0.13, and 0.02 to be considered substantial, moderate, and weak respectively. Table 8.20 illustrates the coefficient of determination for the endogenous variables in the study model. The R^2 values indicate that the nine prediction variables together have substantial predictive power and explain 33.5% of the variation in users' susceptibility to SE attacks. Furthermore, users' involvement and motivation combined effect on users' trust is considered moderate as it explains 13.2% of the variation in users' trust.

Table 8.20 Coefficient of Determination (R^2)

Construct	R Square	R Square Adjusted	Interpretation
Susceptibility	0.335	0.315	**substantial**
Involvement	0.072	0.066	**weak**
KnownFR	0.091	0.088	**weak**
Risk	0.032	0.029	**weak**
Competence	0.027	0.024	**weak**
CCEXP	0.062	0.056	**weak**
Trust	0.132	0.127	**Moderate**

8.9.4 Effect Size – f^2

After assessing the combined effect of all independent variables in explaining endogenous variables, the impact of each variable in the model's endogenous constructs was also evaluated via measuring the effect size. This measure estimates the particular variable impact on a specific endogenous variable by observing the change in R^2 value if the variable

was omitted from the model (Hair et al., 2017). According to Cohen (1988) criteria, the interpretation of the effect size of 0.02, 0.15, and 0.35 signify small, medium, and large effects respectively. However, any value below this threshold ($f^2 < 0.02$) represents no effect size (Hair et al., 2017).

Table 8.21 presents the effect sizes (f^2) for all the structural model's exogenous constructs (IVs) on their corresponding endogenous constructs (DVs). The result indicated that most of the model independent variables have a small individual effect on their corresponding dependent variables. The result also aligns with the findings of the path coefficient test where trust has been found to have the highest effect size on users' susceptibility (f^2=0.098), followed by prior experience with cybercrime and users' involvement (f^2=0.066; f^2=0.063 respectively). While no individual effect has been found between the number of connections, risk, and motivation on users' susceptibility (f^2<0.02).

Table 8.21 Effect Size (f^2)

Relationship	f^2	Interpretation
Involvement → Susceptibility	0.063	Small effect
Num-Con → Susceptibility	0.014	No effect
KnownFR → Susceptibility	0.022	Small effect
SNEXP → Susceptibility	0.034	Small effect
Risk → Susceptibility	0.005	No effect
Competence → Susceptibility	0.021	Small effect
CCEXP → Susceptibility	0.066	Small effect
Motivation → Susceptibility	<0.001	No effect
Trust → Susceptibility	0.098	Small effect
Involvement → CCEXP	0.030	Small effect
Involvement → Trust	0.054	Small effect
Num-Con → Involvement	0.042	Small effect
SNEXP → KnownFR	0.100	Small effect
Risk → Competence	0.028	Small effect
CCEXP → Risk	0.033	Small effect
Motivation → Trust	0.070	Small effect
Motivation → Involvement	0.029	Small effect
Motivation → CCEXP	0.024	Small effect

8.9.5 Predictive Relevance – Q^2

To measure the model's predictive capabilities, a blindfolding procedure has been used to obtain the model's predictive relevance (Q^2 value). Blindfolding is a sample reuse technique which only applied to endogenous constructs (Henseler et al., 2009). Stone-Geisser's Q^2 value, which is a measure to assess how well a model predicts the data of omitted cases, should be higher than zero in order to indicate that the path model has a cross-validated predictive relevance (Hair et al., 2017). Table 8.22 presents results of the predictive relevance

test and shows that all of the endogenous constructs in the research model have predictive relevance (Q^2) greater than zero, which means that the structural model has appropriate predictive ability.

Table 8.22 Predictive Relevance (Q^2)

Construct	SSO	SSE	Q^2 (=1-SSE/SSO)
Susceptibility	316.00	222.74	0.295
Involvement	316.00	297.18	0.060
KnownFR	316.00	288.18	0.088
Risk	316.00	306.36	0.031
Competence	316.00	309.17	0.022
CCEXP	316.00	300.16	0.050
Trust	316.00	277.69	0.121

8.9.6 Model Fit

The assessment of the structural model does not only rely upon testing the model relationships significance but also examining the model fit is a vital part of the evaluation (Hair et al., 2010). Various indices could determine if the model fits the data. However, few model fitting parameters have been recommended to be used in PLS-SEM context (Hair et al., 2017). Four model fit indices have been considered in this research to evaluate the structural model fit which are the standardized root mean square residual (SRMR), the root mean square residual covariance (RMS_{theta}), the normed fit index (NFI), and the exact model fit.

Hair et al. (2017) and Henseler et al. (2014) have recommended using SRMR and RMS_{theta} as indices to test a model's goodness of fit. While, SRMR represents the discrepancy between the observed correlations and the model's implied correlations where its cut-point value should be less than 0.08 (Hu & Bentler, 1998), RMS_{theta} value of less than 0.12 represents an appropriate model fit (Hair et al., 2017; Henseler et al., 2014).

Normed Fit Index (NFI) is an incremental model fit evaluation approach which compares the structural model with a null model of entirely uncorrelated variables, whereby an NFI value of more than 0.90 represents good model fit (Bentler & Bonett, 1980). Additionally, Dijkstra and Henseler (2015), recommend using the squared euclidean distance (d_{LS}) and the geodesic distance (d_G) as measures to assess model fit by comparing the distance between the sample covariance matrix and a structured covariance matrix. Comparing the original values of d_{LS} and d_G with their confidence intervals could indicate a good model fit if their values are less than the upper bound of the 95% confidence interval.

Table 8.23 illustrates the result of the model fit indices that was obtained from the SmartPLS report. The empirical test of the structural model revealed a good model fit as the SRMR value was 0.05, the RMS_{theta} value was 0.099, the NFI was 0.858, which, if rounded,

will be 0.9, and the values of d_{LS} and d_G were less than the upper bound of their confidence interval. Thereby, the results of all the considered model fit indices reflect a satisfactory model fit when considering the complexity of the present research model.

Table 8.23 Model Fit Criteria

	Estimated Model	95% Confidence interval	
SRMR	0.053	-	-
rms Theta	0.099	-	-
NFI	0.858	-	-
d_{LS}	0.154	0.041	0.155
d_G	0.030	0.009	0.031

8.9.7 Summary of the Structural Model Assessment Results

The assessment tests that have been considered to evaluate the structural model show satisfactory results. Table 8.24 presents a summary of the assessment criteria that have been followed and their results.

Table 8.24 Summary of the Structural Model Assessment Results

Assessment Criteria	Threshold	Result	Met Assessment Criteria?
Collinearity Assessment	VIF<5	No collinearity issues exist	Yes
Path Coefficient Assessment	P<0.05	All the study's hypotheses were supported except Ha2, Ha5, and Ha9 were rejected.	Partially
Coefficient of Determination-R^2	0.26 (substantial), 0.13 (moderate), 0.02 (weak)	0.335 (substantial)	Yes
Effect Size-f^2	0.35 (large), 0.15 (medium), 0.02 (small)	Most of the independent variables have small effect size on users' susceptibility. Yet, num-con, risk, and motivation have no effect on users' susceptibility.	Partially
Predictive Relevance – Q^2	$Q^2>0$	0.295	Yes
Model Fit	SRMR<0.08	0.053	Yes
	RMS_{theta}<0.12	0.099	Yes
	NFI>0.90	0.86	Yes
	d_{LS} and d_G < the upper bound of the 95% confidence interval	d_{LS}=0.154, d_G =0.030	Yes

8.10 Demographics and Personality Traits Assessment

8.10.1 Demographic Variables Effect

One of the present study goals is to examine if specific users' demographics (age, gender, education, and major) are associated with users' susceptibility to social engineering attacks. To explore this relationship, regression analysis, as well as variance tests such as t-test and ANOVA test, have been conducted. Table 8.25 summarises these tests results.

Gender has been found to affect the user's susceptibility to SE victimisation (Std. beta=0.133, p<0.05) and the t-test indicates that women are more vulnerable to victimisation (t(271.95)=2.415, p<0.05). Also, the user's major has a significant effect on the user's

vulnerability (Std. beta=0.112, p<0.05). When comparing the groups' behaviour via ANOVA test, users who are specialised in technical majors such as computer and engineering have been indicated as less susceptible to social engineering attacks than those specialised in humanities and business (F(6)=5.164, p<0.001). Furthermore, the results show that age has no significant impact on user vulnerability (Std. beta=0.096, p>0.05). However, when comparing the means of age groups, it can be seen that younger adults (M=1.97, SD=0.99) are less susceptible than older adults (M=2.56, SD=0.92). Moreover, the educational level has no significant impact on users' vulnerability as revealed by the result of the regression analysis (Std. beta=0.068, p>0.05).

Table 8.25 Demographic Factors Impact on User Susceptibility to SE

Demographic Variable	Regression Analysis			Variance Test		Means						
	Std. Beta	t	Sig.	t-value/ f-value	Sig.							
Gender	0.133	2.381	0.018	-2.415	0.016	**Male**			**Female**			
						1.87			2.14			
Age	0.096	1.714	0.088	1.932	0.124	**18-24**	**25-34**		**35-44**		**45-55**	
						1.97	2.28		1.95		2.56	
Education	0.068	1.201	0.231	0.919	0.432	**High school**	**Bachelor**		**Master**		**Other**	
						1.98	2.12		1.93		2.7	
Major	0.112	1.990	0.047	5.164	<0.001	**Comp/ IT**	**Eng**	**Bus**	**Med**	**Sci**	**Hum**	**Other**
						1.78	1.89	2.72	2.46	2.23	2.57	2.05

8.10.2 Personality Traits Effect

This study is also interested in examining if a specific personality trait is related to users' vulnerability to social engineering victimisation. To test this relationship, multiple linear regression analysis has been conducted. Furthermore, multiple regression has also been used to examine whether the five personality traits have any relationships with other constructs in the model.

Table 8.26 presents the results of the regression analysis which show that no personality traits have direct effect on users' susceptibility to social engineering attacks (p>0.05). The results also pointed out that neuroticism has a strong negative effect on both user competence and trust with t-value equals to -3.48, and -2.77 respectively. Extraversion has a strong positive effect on the user's motivation to use Facebook (t=4.66, p<0.001). Agreeableness has a negative effect on the user's experience with cybercrime (t=-2.33, p<0.05). Conscientiousness has a strong positive effect on the user's competence (t=3.89, p<0.001) but has negative effect on motivation (t=-2.02, p<0.05). However, openness to experience has been found to have no significant relationships at all with any construct in the model (p>0.05).

Table 8.26 Personality Traits Regression Analysis

Personality Trait	Susceptibility			Competence			Motivation			Trust			CCEXP		
	Std. Beta	t	Sig.	Std. Beta	t	Sig.	Std. Beta	t	Sig.	Std. Beta	t	Sig.	Std. Beta	t	Sig.
Neuroticism	0.02	0.261	0.80	**-0.20**	**-3.48**	**<0.001**	0.05	0.94	0.35	**-0.16**	**-2.77**	**0.01**	0.02	0.26	0.80
Extraversion	0.05	0.836	0.40	0.04	0.80	0.42	**0.26**	**4.66**	**<0.001**	0.02	0.29	0.77	0.01	0.17	0.87
Openness	-0.07	-1.183	0.24	-0.02	-0.31	0.76	0.06	1.10	0.27	-0.06	-0.99	0.33	-0.01	-0.11	0.92
Agreeableness	0.04	0.774	0.44	-0.05	-0.91	0.36	0.07	1.19	0.24	0.04	0.70	0.48	**-0.13**	**-2.33**	**0.02**
Conscientiousness	0.10	1.801	0.07	**0.22**	**3.89**	**<0.001**	**-0.12**	**-2.02**	**0.04**	0.09	1.52	0.13	0.00	-0.05	0.96

In this context, the present study proposes an extended version of the structural model that includes mediation relationships. This model estimates how personality traits affect the mediation factors (the individual's competence level, the individual's motivation to use the social network, the individual's trust in social network's members and provider, and the individual's experience with cybercrime) and thereby indirectly influence the user's possible victimisation. The proposed mediation hypotheses have been validated in the next section using a PLS-SEM technique which allow this research to test the relationships between the constructs as well as the mediations' significance.

8.11 Mediation Effects Assessment

Mediator variables are generally used to explain why there is a relationship between an independent variable and a dependent variable as mediators can intervene in this relationship. The reason behind conducting the mediation analysis in this study is twofold. First, to investigate if there are constructs that might have indirect effects on users' susceptibility to social engineering victimisation. Given the fact that several constructs have failed to predict users' susceptibility such as personality traits and users' motivation. However, it is worth noting that the total effect of users' motivation on users' susceptibility is proven to be significant in the structural model. This variation in the construct's direct and total effect results revealed the possibility that other mediator variables significantly control this relationship.

Secondly, the result of the second study hypothesis (Ha2) was statistically significant but with an opposite sign to what has been expected. This unexpected result makes the present study recognise the importance of testing the mediators' effect which could reveal the right relationship with the predicted sign between the number of connections and susceptibility to SE victimisation.

8.11.1 Personality Traits Hypotheses

The personality traits regression tests in Section 8.10.2 revealed that there are no direct relationships between the five personality traits and susceptibility to SE victimisation. Yet, there are direct relationships between four of the personality traits (neuroticism, extraversion, agreeableness, and conscientiousness) and other constructs in the model which demonstrate the possibility to have indirect effects of personality traits on user's susceptibility if those constructs were treated as mediators of these relationships. Therefore, based on the result of the regression analysis and with support from the literature, the hypotheses have been developed for the indirect effects of the personality traits on the user's susceptibility to social engineering victimisation and will be explained as follows.

8.11.1.1 Neuroticism

Neurotic people are usually anxious and worry about every step they take (Taormina & Sun, 2015). High levels of stress and anxiety could lead to a decrease in risk-taking behaviour (Lauriola & Weller, 2018). Neurotic people has been observed as having high vulnerability level to email phishing (Halevi et al., 2013). Yet, neuroticism is also found to increase correct judgement over whether information should be trusted or not, and thereby, decreases phishing susceptibility (Cho, Cam, & Oltramari, 2016). Consequently, the present study hypothesised that this trait has a negative relation to trust, and therefore, is negatively related to susceptibility to social engineering attacks. However, this trait is also assumed to be negatively related to the user's competence, since dealing with stressful situations is a weakness of neurotic characters.

- **Hc1.1.** Neuroticism has a negative indirect effect on susceptibility to SE victimisation that is mediated by trust and competence.

8.11.1.2 Extraversion

People with this trait are usually seen as sociable and attention-seekers. A recent study revealed that people with high extraversion tend to have high motivation to engage in social networks (Chua & Chua, 2017), and more importantly, to maintain substantial friendship connections (Quercia, Lambiotte, Stillwell, Kosinski, & Crowcroft, 2012). Extraversion is also found to positively impact the user's willingness to comply with phishing requests (Alseadoon et al., 2015). Therefore, it has been predicted that this distinctive feature will have a positive effect on susceptibility to social engineering and this effect is mediated by the individual's motivation to engage in social networks.

- **Hc1.2.** Extraversion has a positive indirect effect on susceptibility to SE victimisation that is mediated by motivation.

8.11.1.3 Agreeableness

People with this trait usually have the disposition to trust others as they are generally kind and like to help. In the context of social networks, agreeable people have a high propensity to self-disclosure (Seidman, 2013) which is believed to be risky behaviour leading to possible security and privacy exploitation (Nosko, Wood, & Molema, 2010). Moreover, previous research (Parrish Jr. et al., 2009) argued that this aspect of personality is the most strongly related to phishing email victimisation. Therefore, this study predicts a positive relationship between this trait and experience with cybercrime and also an indirect effect between this trait and victimisation.

- **Hc1.3.** Agreeableness has a positive indirect effect on susceptibility to SE victimisation that is mediated by past experience with cybercrime.

8.11.1.4 Conscientiousness

High concentration and attention to detail characterise this trait. Such people are usually organised and known for their self-control. A previous study (Di Giunta et al., 2013) reveals a positive relationship between conscientiousness and self-efficacy. Users with high self-efficacy are likely to take control and protect their personal information online (Milne et al., 2009). Therefore, the current study hypothesised a positive relationship between this trait and user competence. People who exhibit conscientiousness can control their desire and manifest low motivation to engage in social networks (Chua & Chua, 2017). Thus, the indirect effect of this trait on susceptibility to social engineering-based attacks is mediated by the user's competence and motivation and is hypothesised to be negative.

- **Hc1.4.** Conscientiousness has a negative indirect effect on susceptibility to SE victimisation that is mediated by competence and motivation.

Figure 8.3 shows the extended structural model which includes all the constructs with the mediations relationships which will be tested in the next sub-section.

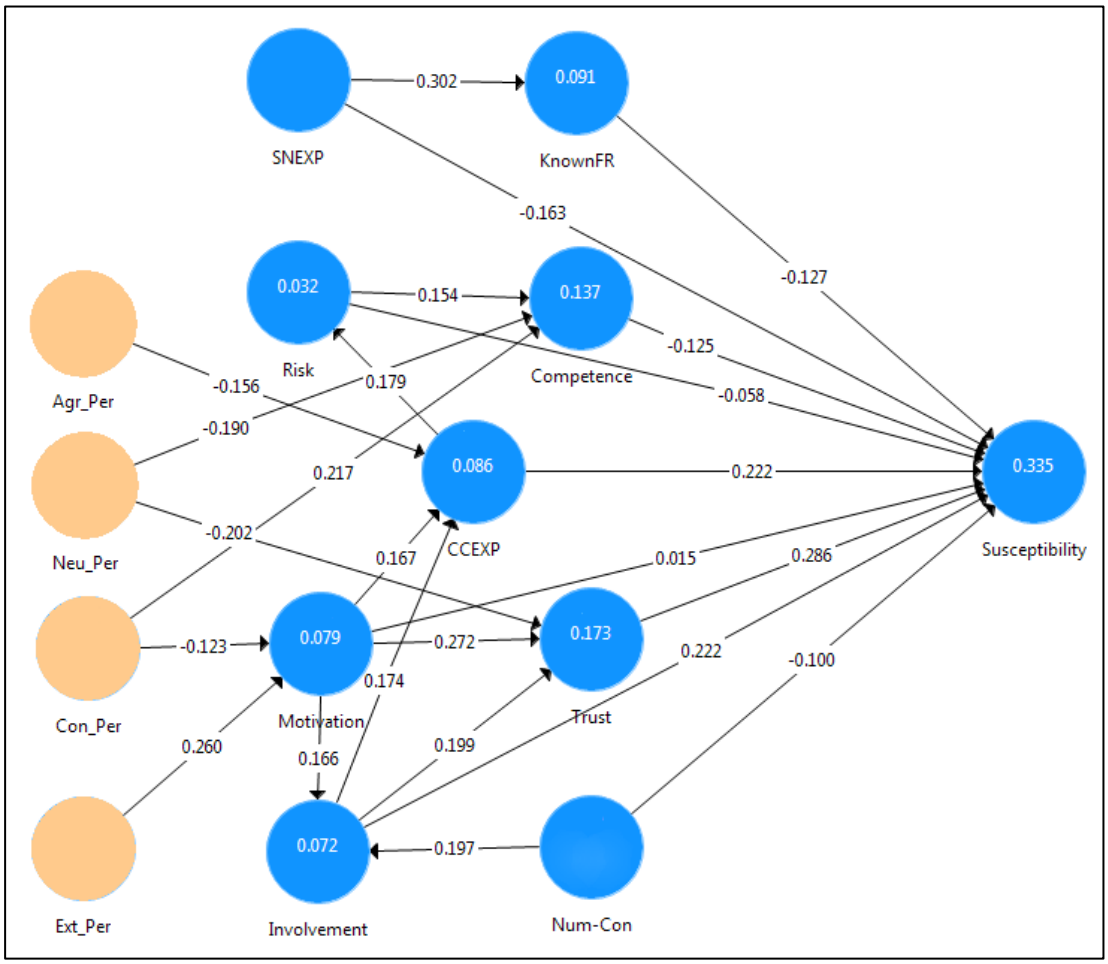


Figure 8.3 The Extended Structural Model with Path Coefficients

8.11.2 Personality Traits Indirect Effect

The extended structural model in Figure 8.3 reveals that the relationships between the personality traits and susceptibility to SE victimisation are mediated and controlled by multiple constructs. For instance, neuroticism's impact on user susceptibility has been hypothesised to be mediated by competence and trust. Also, the influence of conscientiousness on user susceptibility has been mediated by competence and motivation. Therefore, a simple mediation analysis is not suitable in this case as it might produce biased results (Hair et al., 2017). Thus, multiple mediation analysis will be used to test the indirect relationships in the extended structural model.

All the personality traits except openness-to-experience have been included in the extended structural model to test the mediation effects simultaneously in the model as a whole with all the mediation relationships involved. To examine the mediation effect, bootstrapping technique of the indirect effect has been used in SmartPLS v3. This approach generates a reliable biased corrected confidence interval that fit most study conditions and researchers

recommended utilizing this approach with multiple mediation tests in a regression context (Preacher & Hayes, 2008) as well as in PLS-SEM context (Hair et al., 2017).

The guidelines provided in Figure 8.4 was used when examining mediation effects, the direct effect (p_3) and the indirect effect ($p_1.p_2$) between independent and dependent variables should be considered. Based on the result of these two effects, the type of mediation could be identified. According to Zhao, Lynch, and Chen (2010), there are two classes of non-mediation and three classes of mediation types. This classification of the mediations types has been followed to analyse the present study result.

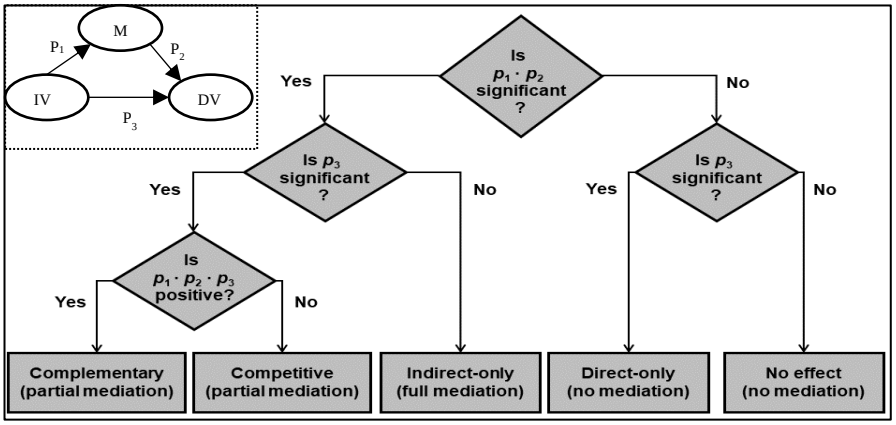


Figure 8.4 Mediation Analysis Classification (Zhao et al., 2010)

Table 8.27 shows the result of the multiple mediation analysis in order to test the mediation effect of each mediator on the relationship between personality traits and susceptibility to SE. The result indicates that neuroticism has a strong significant negative relationship with user's susceptibility mediated by user's trust ($t=-3.22$, $p<0.001$). While the bootstrapping confidence interval for this relation via competence as a mediator includes zero which might draw no mediation effect, the t-value and p-value have forced the conclusion that weak positive indirect only mediation effect is present in this relationship ($t=2.00$, $p<0.05$).

Moreover, the indirect effect between extraversion and user's susceptibility to SE is considered statistically not significant when only mediated by user's motivation ($p>0.05$), whereas, positively significant when jointly mediated (serial mediation) by motivation and trust ($t=2.857$, $p<0.01$). For agreeableness, an adverse influence has been found between this trait and user's susceptibility which is mediated by the user's past experience with cybercrimes ($t=-2.188$, $p<0.05$).

Additionally, the result revealed that user's competence ($t=-2.077$, $p<0.05$) mediates the relationship between conscientiousness and susceptibility to SE; whereas, motivation alone cannot be considered as a mediator between conscientiousness and susceptibility ($p>0.05$).

The model has other factors that also mediate the relationship between the user's motivation and the user's susceptibility, such as the user's trust. Motivation and trust act like joint mediators (serial mediation) of the relationship between conscientiousness and susceptibility to SE in which their indirect effect was significant (t=-2.00, p<0.05).

Table 8.27 Specific Mediators Test

Mediation Path	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Mediation Type
					2.5%	97.5%	
Neu → Sus via Comp	0.024	0.012	2.000	0.046	0.000	0.048	Indirect only
Neu → Sus via Trust	-0.058	0.018	3.222	0.001	-0.093	-0.023	Indirect only
Ext → Sus via Mot	0.004	0.012	0.333	0.739	-0.020	0.028	No effect (no mediation)
Ext → Sus via Mot+Trust	0.020	0.007	2.857	0.004	0.006	0.034	Indirect only Serial Mediation
Agr → Sus via CCExp	-0.035	0.016	2.188	0.029	-0.066	-0.004	Indirect only
Con → Sus via Comp	-0.027	0.013	2.077	0.038	-0.053	-0.001	Indirect only
Con → SUS via Mot	-0.002	0.006	0.333	0.739	-0.014	0.010	No effect (no mediation)
Con → Sus via Mot+Trust	-0.010	0.005	2.000	0.046	-0.020	0.000	Indirect only Serial Mediation

In conclusion, as the extended model has complex multiple mediators, the analysis will rely on the total indirect effect to conclude the personality traits impact on the user's susceptibility to SE victimisation. Table 8.28 shows the total indirect effect of the personality traits on the user's susceptibility to SE victimisation. It can be concluded from the results of the total indirect effect that conscientiousness (t=-2.912, p<0.01) and agreeableness (t=-2.245, p<0.05) have negative indirect influence on the user's susceptibility to SE victimisation; whereas, extraversion has a strong positive indirect impact on the user's susceptibility (t=2.959, p<0.01). Thus, hypotheses Hc1.2 and Hc1.4 are supported, while Hc1.3 is rejected since agreeableness was hypothesised to have a positive impact on user susceptibility and the result showed an adverse effect on users' susceptibility.

Despite the fact that neuroticism has a robust negative effect on the user's susceptibility mediated by the user's trust, the total indirect effect of neuroticism appears to be weak and not significant (t=-1.593, p>0.05). Thus, this study could conclude that Hc1.1 is partially supported.

Table 8.28 Total Indirect Effects of Personality Traits on User Susceptibility

Hypo	Relationship	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Decision
						2.5%	97.5%	
Hc1.1	**Neu_Per → Susceptibility**	-0.034	0.021	1.593	0.111	-0.079	0.005	Rejected
Hc1.2	**Ext_Per → Susceptibility**	0.047	0.016	2.959	0.003	0.021	0.084	Supported**
Hc1.3	**Agr_Per → Susceptibility**	-0.033	0.014	2.245	0.025	-0.070	-0.010	Rejected [a]
Hc1.4	**Con_Per → Susceptibility**	-0.049	0.017	2.912	0.004	-0.086	-0.021	Supported**

Statistically significant at **p<0.01, *p<0.05; [a] Statistically significant but in the opposite direction to that hypothesised

8.11.3 Mediators between Motivation and Susceptibility to SE Victimisation

Motivation has no direct effect on the user's susceptibility as revealed by the previous analysis. Yet, motivation has been found to positively relate to the user's experience with cybercrimes, user's involvement, as well as user's trust. Therefore, those three variables can mediate the relationship between the user's motivation and the user's vulnerability to SE victimisation. Table 8.29 shows that past experience with cybercrime, user's involvement, and trust are all positively mediated the relationship between motivation and user's susceptibility. Trust is considered the strongest mediator between users' motivation and their susceptibility to social engineering attacks ($t=3.391$, $p<0.001$) followed by user's involvement ($t=2.467$, $p<0.05$).

Table 8.29 Mediators Effect between Motivation and Susceptibility to SE

Mediation Path	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Mediation Type
					2.5%	97.5%	
Mot → Sus via Inv	0.037	0.015	2.467	0.014	0.008	0.066	Indirect only mediation
Mot → Sus via Trust	0.078	0.023	3.391	0.001	0.033	0.123	Indirect only mediation
Mot → Sus via CCExp	0.037	0.017	2.176	0.030	0.004	0.070	Indirect only mediation

8.11.4 Mediators between Number-of-Connections and Susceptibility to SE Victimisation

The result of the analysis of the structural model earlier revealed that the number of connections on the user's account is negatively related to the user's susceptibility which means that individuals with a high number of friends' connections are less vulnerable to cyber-attacks than those with a low number of connections. This result opposes the study hypothesis that this relationship is positive as when the user has many connections, the one will be more vulnerable to social engineering victimisation. Therefore, this study argues that the indirect relationship between the number of connections and user's susceptibility which mediated by user's involvement can provide the right relationship.

Table 8.30 indicated that user's involvement does mediate the positive effect of the number of connections on the user's susceptibility to SE victimisation ($t=2.444$, $p<0.05$). This mediation is considered competitive as both direct, and indirect effects are significant but have opposite signs (Zhao et al., 2010).

Table 8.30 Mediator Effect between Number-of-Connections and Susceptibility to SE

Mediation Path	Std. Beta	STDEV	T-Value	P-Value	95% Confidence interval		Mediation Type
					2.5%	97.5%	
Num_Con → Sus via Inv	0.044	0.018	2.444	0.015	0.009	0.079	Competitive mediation

8.12 Assessment of Social Engineering Attacks Types

In the present study, different types of social engineering attacks have been considered (four high-risk attacks, and two low-risk attacks). In this section, a comparison between users' response to the high-risk social engineering attacks and their response to the low-risk social engineering attacks was conducted. Then, a comparison between each type of the four high-risk attacks was performed to explore whether user characteristics could differently impact these four types of social engineering.

8.12.1 High-Risk Attacks vs. Low-Risk Attacks

In the study model, only high-risk scenarios have been considered to measure user susceptibility to social engineering-based attacks. However, including the low-risk scenarios in this study will help identify if users rely on their perceptions and experience to judge those scenarios. Thus, comparing individuals' response to the high-risk attacks and their response to the low-risk attacks aims to examine if users rely on their characteristics when judging the different scenarios and not on other influencing factors such as source credibility (Algarni et al., 2017) or visual message triggers (Wang, Herath, Chen, Vishwanath, & Rao, 2012).

A stepwise linear regression test has been conducted on each type of the considered social engineering attacks to explore if users' characteristics influence them differently. The regression analysis results in Table 8.31 indicated no significant difference with regard to the user characteristics that affect people's susceptibility or resistance to the high-risk scenarios and low-risk scenarios. For example, user past experience and trust are the two factors that found to be significant to increase users' response to the two low-risk requests which align with the finding that these two factors also increase users' response to the other four high-risk attacks. Moreover, competence is the factor that has been found to decrease user possibility to respond to both the low-risk requests and the high-risk requests.

Table 8.31 Regression Analysis Test of Each Type of Social Engineering Attack

Type of cyber-attack	Significant impact	Factors	Std. Beta	T-Value	P-Value
Phishing R^2=0.312	positive	Involvement	0.196	3.930	<0.001
		CCEXP	0.250	5.156	<0.001
		Trust	0.265	5.203	<0.001
	negative	SNEXP	-0.223	-4.663	<0.001
		Competence	-0.138	-2.832	0.005
Clickjacking R^2=0.182	positive	Involvement	0.114	2.113	0.035
		CCEXP	0.194	3.675	<0.001
		Trust	0.234	4.375	<0.001
	negative	SNEXP	-0.158	-3.024	0.003
Malware R^2=0.162	positive	Involvement	0.182	3.245	0.001
		CCEXP	0.148	2.771	0.006
		Trust	0.213	3.800	<0.001
	negative	Num-Con	-0.118	-2.210	0.028
		KnownFR	-0.133	-2.543	0.011
		Competence	-0.125	-2.309	0.022
Phishing scam R^2=0.137	positive	Involvement	0.188	3.366	0.001
		Trust	0.193	3.528	<0.001
	negative	Num-Con	-0.116	-2.142	0.033
		KnownFR	-0.186	-3.524	<0.001
Low-risk 1 R^2=0.025	positive	CCEXP	0.111	1.982	0.048
	negative	Competence	-0.118	-2.114	0.035
Low-risk 2 R^2=0.036	positive	Trust	0.139	2.418	0.016
	negative	Num-Con	-0.110	-1.977	0.049
		Competence	-0.119	-2.065	0.040

8.12.2 The Role of the Type of the Cyber-Attack in Users' Victimisation

As mentioned in the previous section, stepwise regression analysis has been conducted to examine the most influencing factors on every kind of the social engineering-based attack. This further analysis has been performed with the objective of exploring opportunities for designing new training and education approaches that are personalised to the end-user's needs.

The result of the regression analysis in Table 8.31 generally revealed no significant differences among the factors that influence people susceptibility to the four high-risk types of social engineering attacks. Users' involvement, cybercrime experience, and trust have been indicated as predictors of users' vulnerability to all the four types of SE. However, no significant impact has been found of cybercrime experience on phishing scam victimisation.

According to the factors that predict user resistance ability to the four types of cyber-attacks, some variability has been accounted. Years of experience in the network could highly help to indicate individuals who can detect phishing ($t=-4.663$, $p<0.001$) and clickjacking attacks ($t=-3.024$, $p<0.01$). User competence to deal with threats show strong prediction of users' ability to detect phishing ($t=-2.832$, $p<0.01$) and malware attacks ($t=-2.309$, $p<0.05$). Furthermore, low connections with strangers in the network significantly prevent users from being vulnerable to phishing scam ($t=-3.524$,$p<0.001$) and malware attacks ($t=-2.543$, $p<0.05$).

Users with a high number of connections have also shown some slight detection capabilities when facing malware and phishing scam. Yet, the result of the mediation analysis

in Section 8.11 revealed that this negative influence should be rejected as the correct path relation between the number of connections and user vulnerability indicated to be positive.

The R square results vary between being substantial (phishing) to medium (clickjacking, malware, and phishing scam) for all the four models when considering the dependent variable to be one single type of cyber-attack. Based on these findings, it is noted that people can be classified into segments based on their characteristics and their associated type of vulnerability. This conclusion could help to design a novel personalised semi-automated security advisory system which will be discussed further in the next chapter.

8.13 Chapter Summary

The present chapter demonstrates the results of the analysis of the scenario-based experiment, which provides an explanation of the feasibility of the proposed model in predicting people's vulnerability to social engineering victimisation. The results indicated an acceptable model fit and an appropriate predictive ability. The R^2 for user susceptibility is 0.335, which is satisfactory taken into consideration the complexity of the model. The positive results demonstrate evidence of achievement of the current research in identifying the four perspectives that predict people's behaviour online. The analysis did not stop at this stage but proceeded by examining the interaction among the factors in the four identified perspectives, as well as testing the mediation effects of some of the considered factors. All of this analysis helped to conclude that the study model shows good fit and capability to predict users' vulnerability to social engineering-based attacks in Facebook.

More importantly, the comparison of people's reaction to different types of social engineering attacks affords insight on the feasibility of segmenting users based on their behaviour and vulnerabilities. This segmentation could help to target each vulnerable group through more focused and relevant advice that meet users' needs. To this end, the present study has proposed an architecture for a novel semi-automated security advisory system which will be presented and discussed in the next chapter.

Finally, this chapter was dedicated to present the results of the scenario-based experiment and the analysis of the model fit and predictive ability, which answered the research sub-question (RQ2.1) which was stated as "To what extent does each of the conceptual model factors predict users' susceptibility to social engineering-based attacks on social networking sites?" More detailed discussion of the present quantitative phase findings will be provided in the discussion and conclusion chapter (chapter 10).

Chapter 9. A SEMI-AUTOMATED SECURITY ADVISORY SYSTEM

9.1 Overview

Results from the user study reported in the previous chapter, provide insight on the possibility of segmenting social network users based on their characteristics and vulnerabilities, as a basis for a semi-automated security advisory system that seeks to address user vulnerabilities. Most previous studies that have considered persuasion tactics in social engineering (SE) exploits have focused on phishing as the typical type of cyber-attack while limited research has investigated other forms, such as malware or clickjacking. Figure 9.1 shows that 37% of participants in the scenario-based study fell victim to a phishing scam attack that asked them to validate their Facebook account using a phishing link, while only 28% fell victim to a phishing attack that asked them to register their information to enter a prize draw.

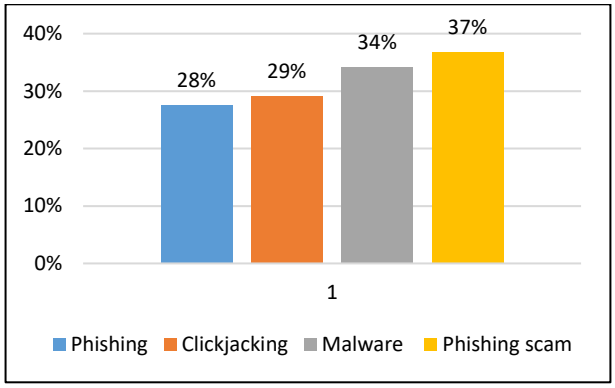


Figure 9.1 Percentage of SE Victims

These findings have indicated the need for further investigation of people's vulnerability to different types of cyber-attack and the need to explore which groups of users are more vulnerable to specific kinds of cyber-attack in a social network context. Identifying the characteristics of most susceptible individuals for a particular type of attack could feed into the design of an advisory system that pushes awareness messages to exposed individuals. Such a security advisory system, based upon observed user behaviour and characteristics, is expected to reduce people's susceptibility to different types of social engineering attacks on social networks.

Consequently, Martens et al. (2019) study compared end-users motivation to protect themselves against two different types of cybercrime (malware and scams) and found significant differences. Thus, the present study argues that people's vulnerabilities change depending upon the type of cyber-attack and this study investigation addresses the human

characteristics associated with victimisation for a range of social engineering attacks which, in turn, facilitates the design of a semi-automated security advisory system that relies on the idea of people segmentation and targeting.

The Segmentation, Targeting, and Positioning strategic approach is a well-known model that has been applied to modern marketing research (Yi, 2018). According to this model, there are three primary processes to segment people in order to deliver them effective messages that are focused to their needs. The present study has adopted this approach to outline a security advisory system based on social network users' characteristics and associated threat vulnerability. Therefore, the present chapter will examine whether the collected user data could help in designing a semi-automated advisory system that classifies participants into different vulnerability segments, in order to provide personalised awareness messages.

This chapter is organised as follows. Section 9.2 provides a discussion of the impact of users' characteristics on their susceptibility to different types of social engineering. An outline approach to a semi-automated advisory system is proposed in Section 9.3. Finally, Section 9.4 offers conclusions from the present chapter.

9.2 Susceptibility to Different Types of Social Engineering

The previous chapter has tested which group of people are vulnerable to each type of social engineering attack in the scenario-based experiment, based upon their rating response to the different statements. Table 9.1 describes the mean from the five-point Likert-scale and its corresponding vulnerability level.

Table 9.1 Description of the Scale Mean

Mean	Likert Scale	Vulnerability Level
1.00-1.79	Strongly Disagree	Low vulnerable
1.80-2.59	Disagree	
2.60-3.39	Neither Agree nor Disagree	Moderately vulnerable
3.40-4.19	Agree	Highly Vulnerable
4.20-5.00	Strongly Agree	

9.2.1 Demographics Differences

9.2.1.1 Gender

To examine whether user demographics have an impact on user susceptibility to social engineering victimisation, every demographic variable has been tested individually to identify which group of people is more vulnerable to a particular type of attack. Female participants are found to be more vulnerable than male participants to all considered cyber-attacks. Figure 9.2 shows that among the four selected types of attack, the phishing scam that impersonates a

Facebook technical support message is most successful among male and female participants with means of 1.92 and 2.32, respectively.

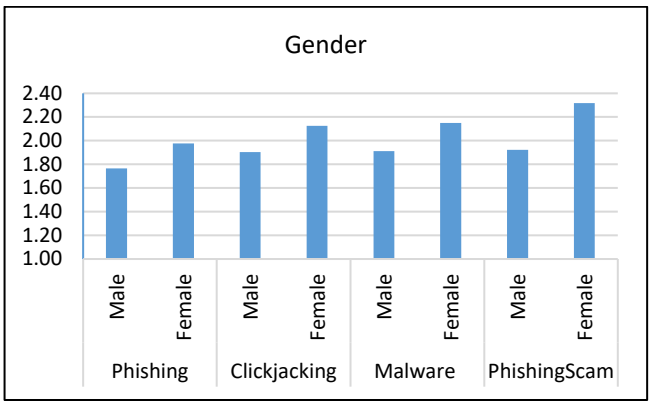


Figure 9.2 Gender Comparisons of Vulnerability to SE

9.2.1.2 Age

Generally, younger adults are less vulnerable to social engineering attacks than older adults (as appears in Figure 9.3). Surprisingly, in the phishing that offers a prize as well as in the malware attack, the oldest group (45-55) was most vulnerable (phishing=2.60, malware=2.80) while the mid-aged group (35-44) was least likely to respond to these kinds of attack (phishing=1.71, malware=1.64).

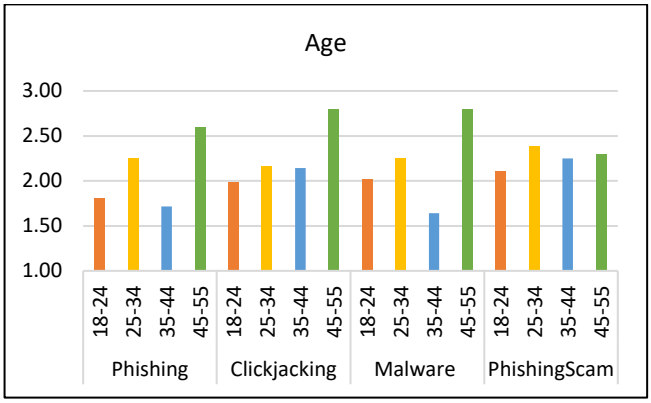


Figure 9.3 Age Comparisons of Vulnerability to SE

9.2.1.3 Education Level

Figure 9.4 shows the analysis of different groups with various education levels and their response to the four types of SE attacks which revealed that master's degree holders are more vulnerable to clickjacking than to other types of cyber-attack (M=2.14). While high school and bachelor's degree holders are more susceptible to the phishing scam that impersonates a legitimate social network provider (with a mean of 2.10, and 2.31 respectively).

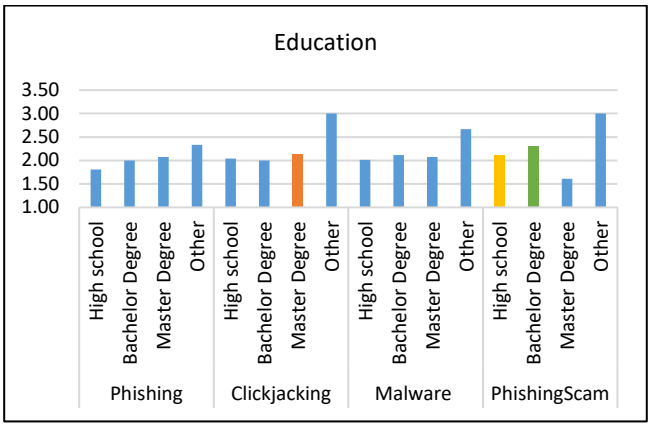


Figure 9.4 Education Levels Comparisons of Vulnerability to SE

9.2.1.4 Major

Users with a technical education background were shown in Figure 9.5 to be less vulnerable to the four types of social engineering attacks. In contrast, while Business School participants are more vulnerable to the phishing attack that offers a prize than other attacks, people specialised in Humanities and Arts are more susceptible to the malware attack. Users with Medical and Science education backgrounds are more vulnerable to the phishing scam that impersonates a Facebook technical support message.

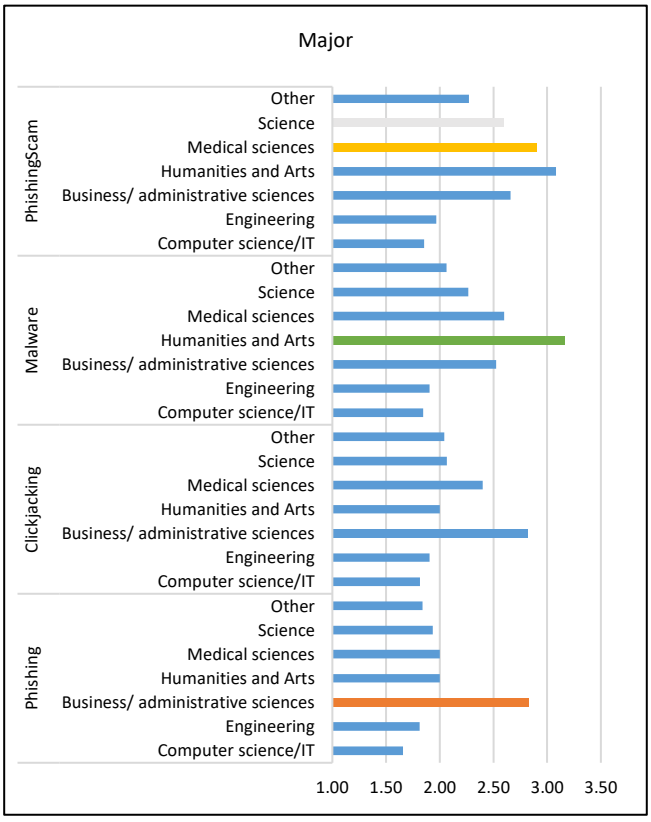


Figure 9.5 Major Comparisons of Vulnerability to SE

9.2.2 Prevention Factors

In order to investigate whether user characteristics can prevent user's vulnerability to specific types of attacks, three factors have been chosen (user's competence, social network experience, low connections with strangers) based on the result of the regression analysis in the previous chapter, to consider whether their prevention effect is similar across the four types of attacks. The objective of conducting the multiple regression analysis is to test the impact of these three variables on preventing users from falling victim to cyber-attacks. These factors are shown to decrease people's vulnerability to the four considered social engineering attacks when combined in the structural model earlier in this study. However, this section will present the result of their impact on each type of attack individually as shown in Figure 9.6.

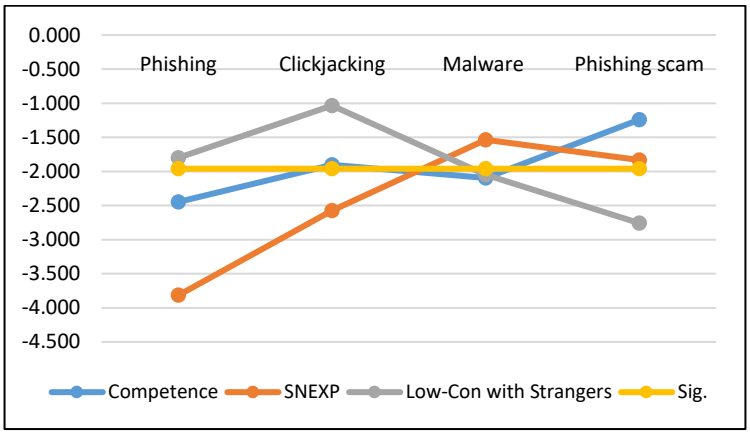


Figure 9.6 Regression Analysis Results

9.2.2.1 User's Competence

Analysing the effect of users' competence on decreasing users' susceptibility to different social engineering attacks shows that measuring users' competence could identify less vulnerable individuals who can correctly detect phishing attack that offers a prize ($t=-2.447$, $p<0.05$) and also detectors of malware attack ($t=-2.098$, $p<0.05$). While competence could not prevent participants from falling victim to clickjacking and phishing scam attacks, as these relationships appear in Figure 9.6 to be not significant ($t>-1.96$).

9.2.2.2 Social Network Experience

Regression analysis of the impact of social network experience on decreasing individuals' response to different kinds of cyber-attack indicated that among the four types of social engineering, phishing attack that offers a prize ($t=-3.816$, $p<0.05$) and clickjacking ($t=-2.573$, $p<0.05$) are attacks that experienced social network users seem to have the ability to deal with and detect. It is also worth noting that there is a negative impact of social network

experience on the other two cyber-attacks, yet, this effect is still considered weak and not significant.

9.2.2.3 Low Connections with Strangers in Social networks

People with limited connections to strangers are less vulnerable to malware attack ($t=-2.049$, $p<0.05$) as well as to the phishing scam that impersonates a legitimate organisation ($t=-2.759$, $p<0.05$). The result also shows that such low connections decrease users' vulnerability to phishing and clickjacking, although these relationships are not strong enough to be significant.

9.3 The Architecture of a Security Advisory System

Results from the previous section in determining user vulnerabilities, afford a basis for profiling users according to their weakness in respect of particular threats. In turn, this provides a means to design a personalised advisory system that sends awareness posts to target individual users' needs. For example, if the characteristics of the user are similar to those who are vulnerable to clickjacking, the advisory system might send awareness posts to the user and advise him/her on how to deal with this type of threat. The architecture of the proposed semi-automated advisory system is shown in Figure 9.7. A brief description of each component is provided as follows.

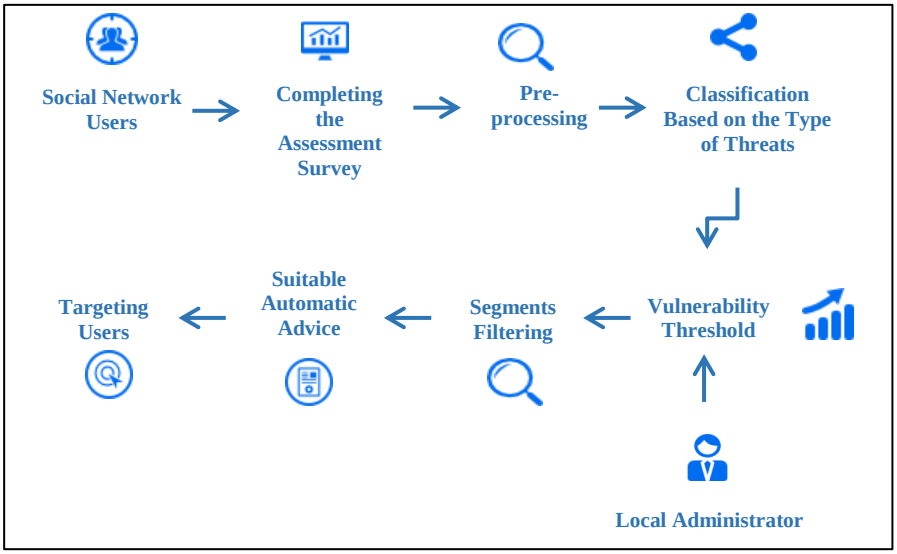


Figure 9.7 The Architecture of a Semi-Automated Advisory System

Social network users. A message must be sent to social network users who want to register and benefit from the advisory system.

Completing the assessment survey. Any new user should start by completing a start-up survey that helps to assess participants' behaviour and perception in online social networks. This assessment survey result will profile the user in the most suitable segment, to receive advice that suits the particular user's needs.

Pre-processing. The collected data will go through different screening and analysis tests such as construct reliability and validity tests.

User classification. The segmentation process can be based on two different machine learning approaches: supervised or unsupervised (Jordan & Mitchell, 2015). Using unsupervised techniques such as clustering might be not suitable in this system as it requires no prior knowledge and clusters users based on patterns of unlabelled data. The present system aims to group users based on their vulnerability to different cyber-attacks. Therefore, supervised techniques such as classification are more appropriate to this study goal, where the classes are predefined and the users grouped based on determined criteria.

Dividing users into segments can help in understanding their needs toward the design of better advice. Thus, users will be classified into different groups based on the result of the scenario-based experiment in the assessment survey. Every segment should include users who shared similar characteristics that were found to increase vulnerability to a particular type of threat. For example, based on users' response to the phishing attack in the scenario-based experiment, users may be grouped into at least three segments: high, moderate, and low vulnerability as can be seen in Table 9.2. However, as user characteristics have been considered in the classification process, it is likely to have multiple segments (each includes individuals with different characteristics) to be susceptible to the same type of attack. For example, age and gender are among the factors that are included in the classification process, so it is possible to have two high vulnerable segments to phishing attacks, e.g., one segment comprises young-adult males, and the other includes mid-aged females. This variation in the segmentation process can help in providing more individualised awareness messages.

Alternatively, users can be encouraged to report any instances of victimisation or different security incidents. Such details can be stored in a local database and used later as input to segment users based on their most reported type of attack. Then, other social network's users who share similar characteristics can be automatically classified into the predefined segments. For instance, if young-adult female users who are studying in a business school and

have high connections with strangers on the network are the most reported group for phishing attacks, then the system can include other social network users who share similar characteristics to the same vulnerable segment in order to receive appropriate advice. This method could help reduce the likelihood that social network users fall victim to phishing attacks.

Table 9.2 Vulnerability Segments

Type of Attack	Highly Vulnerable Segments (H)	Moderate Vulnerable Segments (M)	Low Vulnerable Segments (L)
(1) Phishing	SegH1.1, SegH1.2	SegM1.3	SegL1.4
(2) Clickjacking	SegH2.1	SegM2.2, SegM2.3	SegL2.4
(3) Malware	SegH3.1, SegH3.2	SegM3.3, SegM3.4	SegL3.5
(4) Phishing Scam	SegH4.1, SegH4.2, SegH4.3	SegM4.4	SegL4.5

Vulnerability Threshold. The local administrator can determine the threshold and the priority for each type of attack. For example, this study found that a phishing scam is the most effective attack. Therefore, the threshold for this type of attack may be set to 3 which means that high, moderate and low vulnerable segments will receive awareness advice on this type of threat. While the severity of malware attack is considered average in the current study, its threshold might be set to 2, meaning that malware-related advice will be sent to the high and moderate rated vulnerability segments. Both phishing and clickjacking thresholds may be set to 1, meaning that only high vulnerable segments will receive advice for these two types of attack. Evidently, a single user could be susceptible to different kinds of attack and assigned to more than one segment. Therefore, the priority of the received type of advice is also determined by the attack's vulnerability threshold as assigned by the local administrator, as shown in Table 9.3.

Table 9.3 Vulnerability Threshold and Priority

Vulnerability Threshold	Level of Vulnerability Included	Priority	Assigned Type of Attack
3	High-moderate-low	High priority	Phishing Scam
2	High-moderate	Moderate priority	Malware
1	High only	Low Priority	Phishing, Clickjacking

Segments filtering. In this step, segments are filtered based on threat thresholds. For each type of attack, only segments in the threshold vulnerability level will be addressed. For instance, only segments with high vulnerability to phishing and clickjacking attacks may be considered, while according to the threshold of a phishing scam, high, moderate, and low vulnerable segments should be considered.

Suitable automatic advice. Different user segments are vulnerable to various threats and require advice that is tuned to their needs. With this in mind, each of the identified risks has a set of recommendations that would help individuals to avoid falling victim to a particular threat.

Targeting users. Each segment of users will receive automatic advice that aims to sensitise them to threats to which they are more vulnerable, while every single user can receive more than one package of advice, based on attack priorities that he/she is susceptible to. For example, as can be seen from Table 9.4, Alice is classified into two segments (SegH4.1, SegH2.1) based on her assessment as she is considered highly vulnerable to phishing scam as well as to clickjacking. Based on the priority level of the two attacks, Alice will receive the phishing scam advice before receiving the clickjacking awareness advice. However, Carol is moderately vulnerable to malware attack and less susceptible to a phishing scam. However, as the local administrator gave high priority to a phishing scam, he will receive the advice posts of the phishing scam before the malware advice. Finally, Bob is only vulnerable to phishing attack in which he will receive the suitable advice.

Table 9.4 Example of User Targeting Process

User	Segments	Recommended Advice	Priority
Alice	SegH4.1	Phishing Scam	High
	SegH2.1	Clickjacking	Low
Bob	SegH1.2	phishing	Low
Carol	SegM3.4	Malware	Moderate
	SegL4.5	Phishing Scam	High

9.4 Chapter Summary

This study is investigating why people easily fall victim to social engineering in various online channels and whether vulnerabilities differ across cyber-attack categories in the context of social networks. The present study indicates that people respond differently to different types of social engineering. A phishing attack that pretended to be from an authorised and legitimate organisation (Facebook) is the most successful attack in this study with 37% of participants falling victim. Female participants were found to be more vulnerable to SE victimisation than male participants. Younger and mid-aged adults show high detection ability compared to other age groups. Education is found to influence people's capability, as users with technical majors were found to be competent to detect SE attacks. Furthermore, the study result demonstrates that users' competence level, their experience with social networks, and low connections with strangers on the network play an essential role in preventing people from falling victims to certain types of cyber-attacks.

The proposed semi-automated advisory system should help to address the problem of human vulnerabilities and weakness in detecting social engineering attacks. Assessing social network users and grouping them based on their behaviour and vulnerabilities is essential in order to focus relevant advice that meets users' needs. This technique is considered cost and time effective as users are only presented with insight on relevant threats.

Chapter 10. DISCUSSION AND CONCLUSION

10.1 Overview

The current thesis is composed of three main study phases. While the first study phase result was presented in Chapter 5 and the second was demonstrated in Chapter 6, the third study phase result was presented in Chapter 8. The present chapter is devoted to discussing the results of these three chapters and drawing a conclusion from the whole thesis. Firstly, this chapter starts by discussing the findings with an emphasis on the research questions (Section 10.2). Then, the impact of each perspective of human-related characteristics on vulnerability to social engineering (SE) attacks is discussed and compared with previous research findings in Section 10.3. After that, Section 10.4 illustrates the limitations of the first study phase, while Section 10.5 outlines the third study phase's limitations. Theoretical and practical implications of the thesis are presented in Section 10.6 and Section 10.7. A summary of the main contributions of the thesis is provided in Section 10.8. Recommendations for future research are offered in Section 10.9, followed by a conclusion to the present chapter (Section 10.10).

10.2 Summary of Findings with Emphasis on Research Questions

The work reported in this thesis was undertaken to answer the main research question: "What user characteristics influence user's susceptibility to SE victimisation on social networking sites?" In order to answer this research question, two research questions needed to be addressed.

The first question was related to the investigation of user-related factors that affect users' judgement of social engineering-based attacks, and was formed as "RQ1: What framework can be used as a basis for the user characteristics that influence user susceptibility to SE victimisation on social networking sites?" To answer this question, the literature has been reviewed to select relevant theories and frameworks for the purpose of identifying appropriate factors. Therefore, this research question has been answered as well as the following two additional sub-questions:

RQ1.1: What are the dimensions and attributes of the user characteristics framework that would influence user susceptibility to SE on social networking sites?

RQ1.2: What is the evaluation method that could be used to validate the proposed user-centric framework?

This thesis has reviewed the literature to select the most relevant studies that investigate factors influencing human vulnerabilities in similar or different contexts. Consideration of these factors went through different processing steps, as presented in chapter 4, to construct a holistic user-centric framework (UCF) based on previous literature and relevant theories. These processing steps started by listing all relevant attributes and factors, then combined them in groups based on their nature. After that, the selected attributes were classified and combined to form unique dimensions and perspectives that constitute the proposed UCF. Thus, RQ1.1 has been answered.

This proposed UCF was then validated using two rounds of mixed methods expert reviews, as explained in chapter 5. This expert evaluation has approved the feasibility of the framework factors and dimensions, while providing some minor amendments which have contributed to framework validity. Figure 10.1 presents the validated UCF, which consists of four perspectives and nine factors; thereby, research sub-question RQ1.2 was answered.

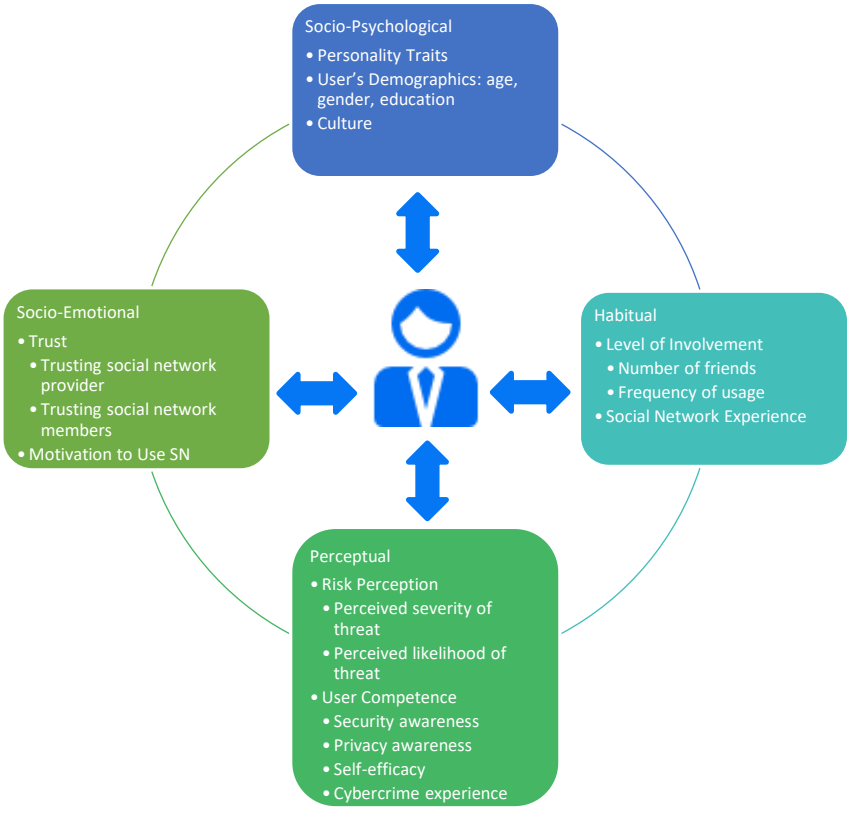


Figure 10.1 The validated User-Centric Framework

The second research question aimed to investigate whether the integration of different perspectives of user-characteristics could predict users' susceptibility to social engineering victimisation. This research question was stated as "RQ2: How can the selected factors in the

user-centric framework be tested in order to indicate whether these factors and dimensions can predict the user's poor judgement of SE attacks on social networking sites?" This question has been answered by addressing a critical objective of the current research which includes developing a conceptual model that could predict users' vulnerability based on their characteristics. However, to address the second research question, its sub-question "RQ2.1: To what extent does each of the conceptual model factors predict users' susceptibility to social engineering-based attacks on social networking sites?" should be answered too. Thus, to empirically test the importance of each perspective and associated factors in predicting users' susceptibility to SE attacks in the context of the social network, a conceptual model was proposed, and 18 hypotheses were postulated, as summarised in Table 10.1.

Table 10.1 Summary of Hypotheses Testing Results

H	Sub-H		Supported
Ha1		Users with a higher level of involvement will be more susceptible to SE attacks.	Yes
	Hb1	The user's level of involvement positively influences the user's experience with cybercrime.	Yes
	Hb2	The user's level of involvement positively influences the user's trust.	Yes
Ha2		Users with a higher number of connections will be more susceptible to SE attacks.	Direct effect (No-significant negative) Total effect (No)
	Hb3	The user's number of connections positively influences the user's level of involvement.	Yes
Ha3		Users with higher connections with known friends will be less susceptible to SE attacks.	Yes
Ha4		Users with a higher level of experience with social network will be less susceptible to SE attacks.	Yes
	Hb4	The user's social network experience positively influences the user's connections with known friends.	Yes
Ha5		Users with a higher level of risk perception will be less susceptible to SE attacks.	Direct effect (No) Total effect (No)
	Hb5	The user's perceived risk positively influences the user's competence.	Yes
Ha6		Users with a higher level of competence will be less susceptible to SE attacks.	Yes
Ha7		Users with a previous experience with cybercrime will be more susceptible to SE attacks.	Yes
	Hb6	The user's experience with cybercrime positively influences the user's perceived risk.	Yes
Ha8		Users with a higher level of trust will be more susceptible to SE attacks.	Yes
Ha9		Users with a higher level of motivation will be more susceptible to SE attacks.	Direct effect (No) Total effect (Yes)
	Hb7	The user's motivation positively influences the user's trust.	Yes
	Hb8	The user's motivation positively influences the user's level of involvement.	Yes
	Hb9	The user's motivation positively influences the user's experience with cybercrime.	Yes

Thus, the second research question (RQ2) and research sub-question (RQ2.1) have been answered in the third research phase after proposing and empirically testing the conceptual model and hypotheses. The analysis of the scenario-based experiment revealed that the proposed model showed satisfactory prediction capability of users' susceptibility to social

engineering victimisation on social networks. Figure 10.2 presents the result of the conceptual model that includes the impact (path coefficient) of each factor on users' susceptibility to SE victimisation.

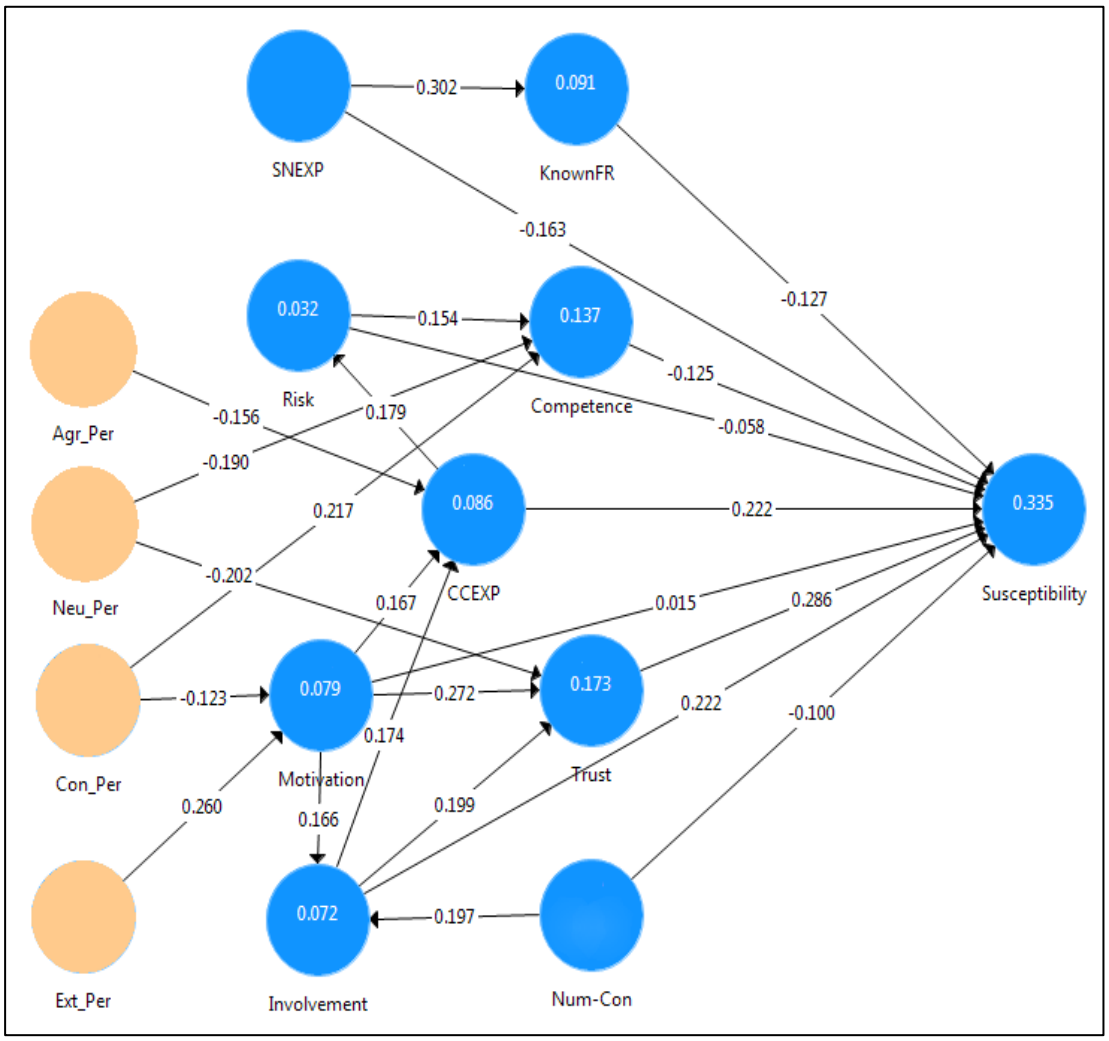


Figure 10.2 The Research Extended Conceptual Model

Additionally, an architecture for a semi-automated security advisory system was designed based upon the observed user behaviour in the empirical study, which represents an important objective of this research. The findings of the third research phase have indicated the need for further exploration of people's vulnerability to different types of SE and the need to examine which groups of users are more vulnerable to specific kinds of SE in a social network context. Assessing social network users and segmenting them based on their behaviour and vulnerabilities is essential in order to design relevant advice that meets users' needs. Figure 10.3 illustrates the architecture of the proposed semi-automated security advisory system. Finally, the findings of both study phases have been consolidated in the design of theory and practical recommendations which will be outlined later in this chapter.

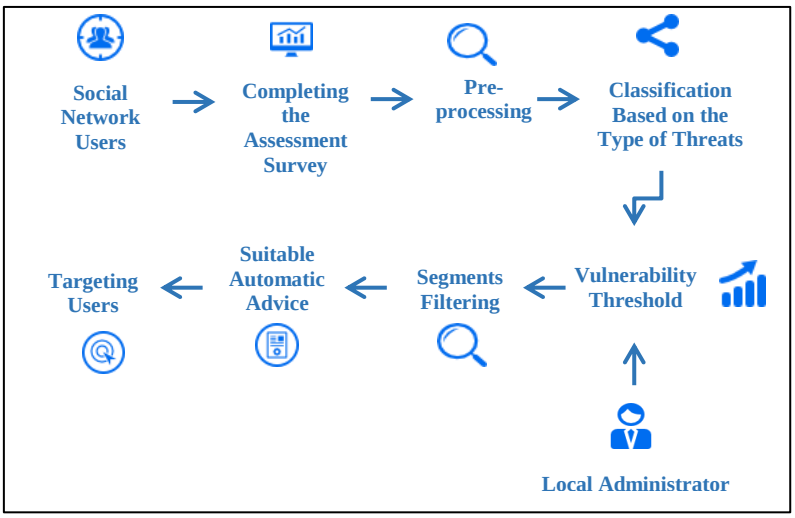


Figure 10.3 The Architecture of a Semi-Automated Advisory System

10.3 Discussion of the Model's Prediction Ability

10.3.1 Based on Individuals' Socio-Psychology

10.3.1.1 Gender and Age

Gender has been found to be a significant predictor of people's vulnerability in the information security (IS) field. In the present study, female Facebook users are found to be more vulnerable than male users. The present research finding is in line with the findings of multiple researchers on cyber-attack vulnerabilities (e.g., Algarni et al., 2017; Halevi et al., 2013; Iuga et al., 2016; Sheng et al., 2010), where "Female" has been repeatedly indicated as the weakest gender when it comes to detecting online threats. Sheng et al. (2010) have explained this female weakness as due to a lack of technical knowledge compared with that of males. However, in the current study, around 45% of female participants specialised in technical majors but were still found to be more vulnerable than men.

Conversely, female users have also shown high detection accuracy compared to males in a recent study (Wang et al., 2017). This observation is consistent with other email phishing studies that have found women to be less susceptible than men (Flores et al., 2014; Mohebzada et al., 2012), while contradicts the findings of recent studies (Diaz et al., 2018; Griffin, 2018) that found no correlation between gender and phishing susceptibility. These contrasting results suggest the existence of other substantial influencing factors apart from gender, such as motivation and level of involvement, which affect females' decisions.

Investigating the reasons why both genders continue to use social networking sites could reveal different opinions and views. Women use the social networks for social reasons, being motivated to maintain their relationships as well as to find social information, while men

are found to use social networks to enhance their capabilities and to seek general information (Krasnova, Veltri, Eling, & Buxmann, 2017). This could also explain why female users are more vulnerable to victimisation than male users. Perhaps women are more socially motivated. Social motivation has been confirmed by the present study to be positively related to SE victimisation.

Additionally, compared to male Facebook users, female users show more addiction symptoms related to Facebook involvement (Andreassen, Pallesen, & Griffiths, 2017; Chabrol, Laconi, Delfour, & Moreau, 2017). Such excessive engagement in the network is also identified as a significant predictor of social engineering victimisation in the current study. This can help in understanding the reasons behind the findings that female users are more vulnerable to social engineering.

In terms of the impact of age, younger adults have been seen as a reckless group when dealing with risk in email settings (Alseadoon, 2014; Griffin, 2018; Jagatic et al., 2007; Sheng et al., 2010) or social network settings (Algarni et al., 2017). Yet, this study found no significant difference between age groups regarding their vulnerability to social engineering. However, when the four types of attack have been compared, a different result is indicated, as younger adults have shown their competency in detecting phishing and clickjacking attacks in social networks compared to older adults. This result concurs with another study conducted by Benson et al. (2015), which examined students' vulnerabilities to severe cybercrimes on social networks and found that a student is less likely to be victimised. A previous phishing study (Marriott, 2018) also found that older adults are more vulnerable to email phishing. However, Iuga et al. (2016) measured people's phishing detection scores after evaluating responses to a number of malicious Facebook login webpages and found that age had no impact on phishing detection. One explanation for this variance between the effect of age on email and social network settings might be that younger adults' awareness and experience with social networks surpasses their knowledge of email environments and associated risks.

10.3.1.2 Education and Expertise

The present study found that educational level has no significant impact on users' vulnerability to victimisation. While educational level could affect the time people spend in evaluating a phishing webpage, this still does not influence their phishing detection scores (Iuga et al., 2016). Benson et al. (2015) claim that students are less likely to fall for cybercrimes on social networks when compared with non-students. However, their study did not distinguish between students' educational levels (e.g., undergraduate and postgraduate).

A recent study (Griffin, 2018) found that the more educated is the user the less susceptible he/she is to phishing victimisation. Therefore, the present study has tested which educational level is more vulnerable to each type of cyber-attack. Master's degree holders are found to be more susceptible to clickjacking attacks. This might be due to the fact that educated people usually seek new information even if there is risk associated with it. However, high school and bachelor's degree holders show a moderate vulnerability level in instances where phishing impersonates a legitimate social network provider, compared to other types of cyber-attacks that were considered. This could be partly because students generally show high commitment behaviour (Vishwanath, 2015). Individuals with a high commitment level have been revealed as more likely to succumb to social engineering attacks (Workman, 2008a).

Although it has been claimed that general technical expertise is unrelated to improving phishing detection ability (Alsharnouby et al., 2015), the present study found that Facebook users with technical study backgrounds, for example in IT, computing, and engineering, are the group least vulnerable to social engineering-based attacks. However, participants with business and management backgrounds are the most vulnerable group in the present study. This finding is not the first to indicate the weakness of business school students and graduates, as they demonstrate greater likelihood of opening phishing emails when compared to IT or humanities students (Goel et al., 2017; Griffin, 2018). One reason for this weakness is that students and employees in the business sector are accustomed to a competitive environment and try to show their commitment through quick response to emails (Goel et al., 2017). With a focus on business students as a study population, Wright and Marett (2010) revealed that experiential factors such as online experience, together with security and computer knowledge, are critical factors in decreasing the success of deception attacks that target students. Thus, providing security awareness and training courses in the first semester of students' enrolment at university is recommended to reduce their vulnerability (Kim, 2013).

10.3.1.3 Personality Traits

People with neuroticism in their personalities generally have difficulty in dealing with stressful situations, which makes them less able to protect themselves from online threats, as found in the present study. The Halevi et al. (2013) study supports this finding with the view that neurotic women are more vulnerable to phishing. Yet, highly neurotic people also tend to be overly concerned about everything, which makes them less trusting. The present study found the relationship between neuroticism and trust (t=-4.077) to be stronger than the relationship between neuroticism and competence (t=-3.294), which supports the final result that, even if people with neuroticism in their personalities might not be competent enough,

their lack of trust in other people makes them less vulnerable to social network threats. This finding concurs with the Cho, Cam, and Oltramari (2016) study, which also found that lack of trust in a neurotic personality helps to decrease the individual's likelihood of being phished.

The tendency to extraversion is the personality characteristic that makes users most vulnerable to cyber-attack victimisation on social networking sites such as Facebook. The result of the present study revealed that this personality trait is the only one that is positively associated with cyber-attack victimisation. This positive and robust effect is mediated by the impact of this trait on people's motivation and trust when engaging in social networks, which is also supported by the findings of recent studies (Chua & Chua, 2017; Cusack & Adedokun, 2018). One possible reason for this positive impact might be that people with this trait are usually more active in using Facebook and more inclined to connect with strangers in order to maintain more substantial friendship connections (Tsai, Chang, Chang, & Chang, 2017). Furthermore, the present study finding agrees with that of Alseadoon et al. (2015) that a high level of extraversion increases people's tendency to obey and respond to email phishing requests. Yet, this result contradicts another empirical study conducted by Pattinson et al. (2012) which indicated that people with extroverted personalities are highly effective in dealing with phishing emails. However, it is important to note that the Pattinson et al. (2012) study has a sample limitation, namely, N=59.

Alseadoon et al. (2015) revealed that people with high openness-to-experience in their personalities are more likely to respond to email phishing. But another study detects the opposite relationship, in which the more open the user, the better performance he/she will show in dealing with phishing emails (Pattinson et al., 2012). However, the present study result showed that openness has no direct or indirect effect on a user's susceptibility: a finding that agrees with Halevi et al. (2013), who found no relation between openness and email phishing victimisation.

People with a high level of agreeableness are inclined to help others in need and are known to be kind and cooperative. Therefore, based on previous study results (Alseadoon et al., 2015), this study hypothesised that individuals possessing agreeableness as a personality trait are more likely to fall for cyber-attacks. Yet, the result of the present research rejected this hypothesis, indicating that agreeableness significantly decreases the user's susceptibility to cyber-attack. This result can be seen as contrary to common sense, but interesting, as agreeable people had low past victimisation experience ($t=-2.912$), and thereby, a negative relationship ($t=-2.245$, $p<0.05$) with cyber-attack vulnerability. This result also accords with the claim that high level of agreeableness might reduce risk behaviours (Lauriola & Weller,

2018). People with agreeableness are more likely to adopt security software than other users (Shropshire, Warkentin, & Sharma, 2015). Agreeable users usually follow organisational rules and show high commitment and integrity in their workplace (Guay et al., 2016). Furthermore, agreeable individuals showed high information security awareness (McCormac et al., 2017) as well as great efficiency in detecting phishing attacks, in a previous study (Cho et al., 2016). These findings might explain the result of the present study, since agreeable users could be following security and privacy rules in social networks and therefore could be less vulnerable to cyber-attack victimisation.

Conscientiousness in a personality is always associated with self-control as well as high concentration, which make users with this personality trait keen to protect themselves from potential online threats. The present study found this trait to be strongly and negatively related to social network threat victimisation. Yet, this relationship has been found to be mediated by the individual's competence and motivation to engage with social networks. This result accords with previous findings of Pattinson et al. (2012), that low-impulsive people are better and more effective at dealing with phishing emails. Conscientiousness in a personality is also associated with low motivation to engage in social networks (Chua & Chua, 2017), high information security awareness (McCormac et al., 2017), rules commitment (Guay et al., 2016), risk avoidance (Lauriola & Weller, 2018), and willingness to use security software (Shropshire et al., 2015). All of these findings support the present study's claim that people with this personality trait are generally competent, less motivated to use social networks and, thus, less susceptible to cybercrime.

Personality traits are considered important predictors of human behaviour in IS research. Yet, previous studies that treat these traits as having direct effects on the dependent variables often conclude with conflicting and inconsistent results. The present study found personality traits (except openness to experience) to be significant predictors of human vulnerability to cyber-attacks. But these relations are indirect and mediated by other relevant factors. The study results demonstrate that users' trust, competence, motivation, and past experience with cybercrimes play an important role in explaining the influence of the five personality traits on users' susceptibility to social engineering attacks on social networks. Conscientiousness, agreeableness, and neuroticism are found to significantly decrease the user's susceptibility to SE victimisation in social network settings. However, extraversion is found to strongly increase the user's likelihood of falling victim to social engineering attacks.

10.3.2 Based on Individuals' Habits

When discussing the result of the dimensions for the habitual perspective, it is hard to compare and relate it to the results of the literature on email phishing studies, because in this section, the focus will be mainly on discussing user behaviour in a social network context that makes them more vulnerable to SE.

Facebook users' involvement level is revealed in the present study to have a strong significant effect on their susceptibility to SE victimisation. This finding confirms the results of previous research (Saridakis et al., 2016; Vishwanath, 2015). Since most social network users are highly involved in online networks, it is hard to generalise that all involved people are vulnerable. However, high involvement affects other critical factors in the present model, i.e., experience with cybercrime and trust, which in turn have powerful impacts on users' susceptibility to victimisation.

People who spend more time on the network and interact more frequently with its other members are more likely to have previous experience with cybercrime threats. Such past experience with cybercrime has proved by the results of this study ($t=3.736$, $p<0.001$) to have a significant impact on users' susceptibility. Additionally, high involvement has been found to strongly increase people's trust in the network provider to protect them, along with their belief that other network members are harmless and trustworthy ($t=3.914$, $p<0.001$). The extent of people's trust in the network can identify the success of any social network service, as people can only engage with networks that they trust, a pattern sometimes referred to as "engagement trust" (Sherchan et al., 2013). Even though this type of trust is favourable to the network provider, it could expose the network users to being easily deceived by cyber-attacks.

The number of friends has been found to have a direct negative impact on people's vulnerability, which is against what the present study hypothesised, as this relationship had been assumed to be positive. Yet, level of involvement plays a critical part in this relationship as it mediates the significant positive relationship between numbers of friends and people's susceptibility to victimisation ($t=2.444$, $p<0.05$). This finding concurs with previous claims that large network size makes individuals more vulnerable to social networks risks (Buglass et al., 2016; Vishwanath, 2015). Facebook users seem to accept friend requests from strangers to expand their friendship network. Around 48% of the participants in this study stated that they know less than 10% of their Facebook network personally.

The current study found that low connections with strangers can protect people from being deceived in social networks. Connecting with strangers on the network has previously

been seen as the first step in falling prey to social engineering attacks (Vishwanath, 2015), while also being regarded as a measure of risky behaviour on social networks (Alqarni et al., 2016). A high percentage of strangers with whom the user is connected can be seen as a determinant of the user's low level of suspicion. This is because connecting with strangers is considered risky behaviour which could ultimately expose the user to threats such as Internet scams, loss of privacy, and information leakage (Rashtian, Boshmaf, Jaferian, & Beznosov, 2014).

However, even when people are mostly connected with known friends, they should remain aware and alert. Previous research claims that connecting with close friends on the network decreases people's perception of the likelihood of threat occurrence, and this is considered a risk (Alqarni et al., 2016). Users should be aware that they might face cyber-attack posts coming from hacked accounts of known friends (Egele, Stringhini, Kruegel, & Vigna, 2017).

Furthermore, social network experience has been found to significantly predict people's susceptibility to social engineering in the present study. People's ability to detect social network deception has been said to depend on information communication technology literacy (Tsikerdekis & Zeadally, 2014). Thus, experienced users are more familiar with cyber-attacks such as phishing and clickjacking, and easily detect them. This is further supported by Algarni et al. (2017), who pointed out that the less time that has elapsed since the user joined Facebook, the more susceptible he or she is to social engineering. Yet, their research treated user experience with social networks as a demographic variable and did not examine whether this factor might affect other aspects of user behaviour. For instance, results from the present study reveal that users who are considered more experienced in social networks have fewer connections with strangers ($t=6.091$, $p<0.001$), which further explains why they are less susceptible than novice users.

Unlike the present study, previous research that considered computer knowledge as a cybercrime resistance factor has found this relationship to be insignificant (Saridakis et al., 2016; Vishwanath et al., 2011). One explanation for this inconsistent finding might be that computer experience is usually measured with the use of a self-reported scale on which users normally overestimate their technical ability. In contrast, the present study has measured social network knowledge according to the number of years of usage to reveal a reasonable gauge of social network experience.

10.3.3 Based on Individuals' Perceptions

Perceived risk has been found to have no direct effect on user susceptibility in the current study. This is because perceived risk has been treated as a formative construct with two sub-dimensions, perceived severity and perceived likelihood of threat. It has been found that perceived severity of threat decreases people's vulnerability to SE while perceived likelihood has a positive, yet not significant, impact on their vulnerability. This might be because people's perceived likelihood of being victimised failed to affect their protection behaviour toward social cybercrimes (Martens et al., 2019).

Similarly, Alqubaiti (2016) has adopted the protection motivation theory to investigate users' precautionary behaviour on social networks. The result of the study indicated no correlation between the protection motivation theory factors (perceived severity of threats, perceived vulnerability, response efficacy, and self-efficacy) and people's safe behaviour on Facebook. One major limitation of Alqubaiti's study is the lack of diversity, as all the approached participants were students in the information technology department and thus had sufficient computer knowledge. Additionally, among many studies that have considered perception of the risk associated with engaging in online activities to have a direct influence on people's vulnerability to online threats (e.g., Saridakis et al., 2016; Vishwanath et al., 2016; Wright & Marett, 2010), only the Vishwanath et al. (2016) study found this relation to be significant. The results of the other studies accord with the finding of the present study.

Perception of risk has no direct influence on people's vulnerability, but the present study found perceived risk to significantly increase people's level of competence to deal with social engineering attacks. This also accords with the Schaik et al. (2018) study, which found that Facebook users with high risk perception adopt precautionary behaviours such as restrictive privacy and security-related settings. Most importantly, perceived cybercrime risk has also been indicated as influencing people to take precautions and avoid using online social networks (Riek et al., 2016).

Little research has identified or focused upon the concept of user competence or its dimensions in the IS field, even though research repeatedly reports users as the weakest link in security. Measuring user competence levels would contribute to our understanding of the reasons behind user weakness in detecting online security or privacy threats. In the present study, the measure of an individual's competence level in dealing with cybercrime was based upon three dimensions: security awareness, privacy awareness, and self-efficacy. The empirical results show that this competence measure can significantly predict the individual's ability to detect social engineering attacks on Facebook. Individuals' perception of their self-

ability to control the content shared on social network websites has been previously considered a predictor of their ability to detect social network threats (Saridakis et al., 2016), as individuals who have this confidence in their self-ability as well as in their security knowledge seem to be competent in dealing with cyber threats (Flores et al., 2015; Wright & Marett, 2010).

The result of the present study found that people with past experience of cybercrime are more vulnerable to social engineering victimisation in the context of social networks. This finding is in line with the results of prior research which found that previous email phishing victimisation failed to increase phishing detection accuracy (Wang et al., 2017). This might be because people with prior knowledge of social cybercrimes tend to underestimate the likelihood of their potential vulnerability (Martens et al., 2019). However, in the email context, Workman (2008b) assumed this relation to be negative as the previous victimisation could decrease people's vulnerability to social engineering. Yet, the result of their study found this relationship to be not significant. This difference in the assumption of the impact of prior knowledge of cybercrime might have arisen because Workman (2008b) has considered only people's past experience with email phishing, whereas in the present study four different types of social engineering attacks were used to measure people's experience with cybercrime.

Furthermore, the present study found that previous cybercrime experience positively impacts upon users' perception of the risk associated with using social networks. The study results accord with the finding of Riek et al. (2016) that previous cybercrime experience has a positive and substantial impact on users' perceived risk. Yet, this high-risk perception did not decrease users' vulnerability in the present study. This could be because experience and knowledge of the existence of threats do not need to be reflected in people's behaviour. For example, individuals who had previously undertaken security awareness training still underestimated the importance of some security practices, such as frequent change of passwords (Kim, 2013).

10.3.4 Based on Individuals' Socio-Emotions

The impact of factors from this perspective on people's vulnerability to SE-based attacks in the context of social networks is considered novel and interesting. In previous literature, limited research has considered investigating them. Yet, the impact of socio-emotional factors has been examined in different research contexts, for instance, by investigating people's disclosure of private information in social networks. Thus, the present study will compare its findings with the results of related research in these different contexts.

The present research found that people's trust in the social network's provider and members were the strongest determinants of their vulnerability to social engineering attacks ($t=5.202$, $p<0.001$). Previous email phishing research (e.g., Alseadoon et al., 2015; Workman, 2008a) has also stressed that people's disposition to trust has a significant impact on their weakness in detecting phishing emails. Yet, little was known about the impact of trust in providers and other members of social networks on people's vulnerability to cyber-attacks. These two types of trust have been found to decrease users' perception of the risks associated with disclosing private information on social networks (Cheung et al., 2015). Similarly, trusting social network providers to protect members' private information has caused Facebook users (especially females) to be more willing to share their photos in the network (Beldad & Hegner, 2017). These findings draw attention to the huge responsibility that social network providers have to protect their users. In parallel, users should be encouraged to be cautious about their privacy and security.

People's motivation to use social networks has no direct influence on their vulnerability to SE victimisation, as evidenced by the results of this study. Yet, this motivation significantly affects different essential aspects of user behaviour and perception such as user involvement, trust, and previous experience with cybercrime. These three factors substantially mediate the positive relationship between users' motivation and their susceptibility to victimisation. Thus, the claim that motivated users are more vulnerable to SE victimisation is supported by the results of the present study ($t=3.854$, $p<0.001$). Similarly, people's perceived benefits of network engagement have a positive impact on their willingness to disclose private information, such as photos online (Beldad & Hegner, 2017). For instance, using Facebook for social motivation has been found to increase people's disclosure of basic, sensitive, and highly sensitive information (Chang & Heo, 2014). This concurs with the present study's result that social motivation has been found to strongly increase people's vulnerability to victimisation ($t=5.680$, $p<0.001$).

10.4 Limitations of the First Study Phase (Mixed-Methods)

The present study has several limitations that must be acknowledged. The experts' review approach that has been used in this study may not be considered the best way to predict user vulnerability. At some stage, this requires experimental studies, which can provide more empirical and accurate results. Also, the sample size is relatively small. This is often the case in expert review studies as it is difficult to find a large number of experts willing to participate in such a study. Yet, the purpose of the first study phase is not to generalise the proposed

framework to the study area, as is the case with empirical studies, but to shed light on critical factors and dimensions that have not been previously addressed, especially in the context of social networks. The objective of conducting qualitative-based research is to understand an event rather than to generalise a finding (Creswell & Creswell, 2018). From this perspective, the chosen approach and the sample size used in the expert review are adequate for the study purposes.

Another limitation is that the knowledge backgrounds of the participants are not diverse, as all of them specialise in the IS field. It would be worth knowing what experts from different disciplines think about the proposed framework. This limitation was addressed later when validating the study scales and dimensions, as participants from various fields were recruited in the second study phase.

Finally, while several steps have been taken to ensure the inclusion of all influential factors in the framework, it is not feasible to guarantee that all possibly influencing attributes are included in this framework. This limitation has been minimised by the qualitative part of the study that includes open-ended questions. This step prevented experts from being limited to the framework's factors and allowed them to suggest other factors that they believed to be important. Therefore, using a mixed methods approach in the expert review has addressed the limitations of both the quantitative and the qualitative parts of the study.

10.5 Limitations of the Third Study Phase (Quantitative)

Using a scenario-based experiment instead of conducting a real attack study is one of the main limitations of the present study, but was considered unavoidable due to ethical considerations. However, the selected attack scenarios were designed to match recent and real social engineering-based attacks on Facebook.

Another limitation of this study is that the use of a self-reported questionnaire may not accurately convey people's real characteristics. For instance, using a self-reported personality test may not precisely reflect the individual's real personality, as people sometimes behave differently based on other stimuli. Predicting user behaviour is a complex task, and understanding and examining online behaviour certainly needs further research, e.g., to focus on why users respond to different attacks differently and why particular types of cyber-attacks show a high success rate compared with others.

Additionally, the present study was undertaken in full consciousness of the fact that when measuring people's previous experience with cybercrime, some participants might be

unaware of their previous victimisation and so might respond inaccurately. In order to mitigate this limitation, different types of SE attacks have been considered in the scale that measures previous experience with cybercrime, such as phishing, identity theft, harassment, and fraud.

This research selected Saudi Arabia as the study population due to its unique culture that differs from western cultures; the latter have been thoroughly studied, as mentioned in the systematic review by Cao et al. (2015). However, drawing comparisons between the impacts of the proposed conceptual model factors on people's susceptibility in different contexts could yield new insights in future studies. But due to time constraints on the production of the present thesis, the research could not examine and compare the effects of culture on the study model. Furthermore, this research has focused only on academic communities as all the participants in the third phase of this study were students, academic, and administrative staff of two universities. This could be seen as a limitation as the result may not reflect the behaviour of the general public in Saudi Arabia. The university context is important however, and cyber-criminals have targeted universities recently due to their importance in providing online resources to their students and community (Öğütçü et al., 2016).

Another limitation that has been acknowledged by scholars in social networks research is the focus on one brand of social network, such as Facebook in this study case (Rains & Brunner, 2015). Facebook has been selected as it is the world's most popular social network, in Saudi Arabia as well as elsewhere. Regardless of being repeatedly considered in security and privacy research, the most famous and severe social engineering attacks have taken place on the Facebook platform. Future studies could investigate users' vulnerability to social engineering victimisation on other social network platforms such as Twitter and compare the results with the current research.

10.6 Theoretical Implications

The present study aims to make several contributions to both information security and social network research. The results of this study provide evidence for the importance of different user-related perspectives that have been identified before in the literature, such as the socio-psychological, the perceptual, and the habitual, while adapting and incorporating them together with a new perspective, the socio-emotional, to develop a UCF that aims to examine people's judgement of and response to social engineering-based attacks in the social network context. The social network context is different from an email context, a fact which presents the need to adapt previously examined factors and incorporate new elements to suit the new setting.

Social networks research that relies upon a strong theoretical background is limited, as revealed by a previous systematic review (Cao et al., 2015). Proposing the UCF that incorporates four different perspectives is a novel contribution to social network theories as well. This UCF could be beneficial in marketing and advertising research that investigates strategies for predicting the behaviour of a particular group of people on social networks. This primary result also paves the way for further work that considers the four proposed perspectives in explaining human behaviour in other research contexts. Furthermore, studies that investigate technology adoption and satisfaction, such as adoption of e-government services, could incorporate the four perspectives into their theoretical models in order to examine the impact of these perspectives on people's behaviour toward new services and technology.

The steps taken to develop the proposed framework, which built on previous theories and literature by replacing some of the identified elements with SN-oriented elements, contribute to a theory building process, especially in the IS field. This may provide a practical example of how theories and frameworks could be generated in new contexts. Researchers could use the same steps to build more focused frameworks based on elements extracted from similar studies in other research contexts.

The proposed conceptual model was developed by integrating different theories such as protection motivation theory, the five personality traits, and competence conceptualisation, to build a holistic model. The developed conceptual model shows an acceptable prediction ability of people's vulnerability to social engineering in social networks as revealed by the results of this study. The proposed model could be used by information security researchers (or researchers from different fields) to predict responses to different security-oriented risks. For instance, decision-making research could benefit from the proposed framework and model as they indicate new perspectives on user-related characteristics that could affect decision-making abilities in times of risk.

Gender differences in dealing with cybersecurity risks are among the most controversial topics in IS research. The findings of the present investigation revealed that women are more vulnerable to social engineering attacks in social networks, which supports the theoretical view of previous research that explains the role of gender variation in responding to online threats (e.g., Algarni et al., 2017; Halevi et al., 2013; Iuga et al., 2016; Sheng et al., 2010). Yet, this study encourages further investigation of why this variation exists in IS research and why women apparently show less ability to deal with risky situations online.

10.7 Practical Implications

Multiple solutions (reviewed in chapter 2) have been proposed in the literature to mitigate social engineering threats. Most of the proposed countermeasures are focused on technical solutions. Despite the importance and effectiveness of these proposed technical solutions, social engineers try to exploit human vulnerabilities; hence we require solutions that understand and guard against human weaknesses. Given the limited number of studies that investigate the impact of human characteristics on predicting vulnerability to social network security threats, the present study can be considered useful, having critical practical implications that should be acknowledged in this section.

Many social media channels compete to attract more users, but recently users are becoming increasingly familiar with news of potential threats and misuse of these channels. In order for social network providers to guarantee sustained usage of their services and channels, users must first be assured of their safety. Based on the current study results, different recommendations will be given to social network providers and to training program stakeholders which could help reduce social networks users' vulnerability. A service scenario is also provided to give a practical example of how the proposed framework can be adopted.

10.7.1 Recommendations for Social Network Providers and Users

Gaining a greater understanding of those users' characteristics that influence the judgement of cyber-attacks, social network providers will be able to protect their members by designing and implementing more reliable protection features and providing better security and privacy settings. For instance, given that users' trust in social network providers and members positively affects their vulnerability to social engineering, social network providers should take this trust seriously and be very cautious about security issues in their network. Users rely on social network providers to keep their personal information confidential and protected. Protecting users' personal information is an essential element in promoting sustainable use of social networks (Kayes & Iamnitchi, 2017). Social network providers should provide better privacy rules and policies and develop more effective security and privacy settings. A live chat threat report must be essential in social network channels in order to reduce the number of potential victims of specific threatening posts or accounts. Providing security and privacy-related tools could also help increase users' satisfaction with social networks.

Past experience with cybercrime has been repeatedly shown to be an indication of increasing awareness of such threats. But assuming that people who have previous experience

of victimisation will no longer be vulnerable is a wrong hypothesis. The result of this study revealed that past experience of cybercrime is a strong indication of weak and vulnerable individuals. Social network providers should encourage people to report their victimisation, as this information could help providers to focus on users who require greater protection. Organisations could also distribute a questionnaire on past experience with security threats in order to identify vulnerable individuals.

Reviewing previous anti-phishing recommendation approaches revealed that most of them fail to match the specific needs of victims (Tambe Ebot, 2018). The present study provides a practical solution to this problem. The designed semi-automated advisory system could be used as an approach with which to classify social network users according to their vulnerability type and level. Then the network provider could send awareness posts that target the particular group's needs. Since social engineering techniques are rapidly changing and improving, the attack scenarios that are used in the assessment step could be updated from time to time. The registered users in the semi-automated advisory system also need to be reassessed regularly in order to observe any changes in their vulnerability.

Social network providers could start recording users' behaviour attributes in order to facilitate future classification. For example, if the user checked or adjusted the privacy settings, they might be given points in the network. These points may help social network providers to measure privacy awareness, and thereby identify users' competence level in dealing with online threats. The competence dimensions and measure that has been proposed in the present study could provide a foundation for automatically identifying less competent users and thus allow social network providers to take extra steps to protect this group of users.

The finding of gender differences in vulnerability level is vital to purveyors of social network services. Revealing that women users of social networks are more vulnerable to SE could assist developers in designing more effective defensive tools: for example, by providing security management tools enabling women to easily and effectively control their social network profiles. Demographic differences and their relation to a particular type of social engineering finding are also useful for focused social media channels such as social groups, social communities, company profiles, and university accounts. Obtaining user-related characteristics is achievable in such channels as they usually have a small network size. This could aid in designing more focused warning and awareness posts that these small communities' channels could publish in their social media to target their audience's (followers') need.

The specific company or community followers' vulnerability type and level could be identified based on their characteristics. For example, in a make-up brand profile on social networks, customers always communicate to share their knowledge of products, brand satisfaction, and prices. This interaction could lead to potential security risks such as spreading scam and fake links to product discounts which could cause the brand to lose its customers and reputation. The brand firm could protect its customers from such threats by giving more attention to the problem and recognising that most of their followers are, for instance, women and their ages are between 18 and 24 years old. According to the present study results, this group are more vulnerable to phishing scams that impersonate legitimate organisations and to malware attacks. If the brand's social network profile could post awareness information on how to avoid these two types of attack, it might protect customers and be more effective than posting general information about wider security risks.

Business, marketing, and social commerce agencies have started to engage with social networks in order to follow the large scale of customers. The findings of this study could contribute to increasing their customers' satisfaction if more attention were given to protecting customers' personal information. Considering individual characteristics of their customers, for instance by obtaining their usage frequency and habits to identify their vulnerability level, would provide essential insights to help in the design of appropriate risk warning messages.

10.7.2 Recommendations for Training and Awareness Programs

Despite the importance of online awareness campaigns as well as the rich training programs that organisations adopt, problems persist because humans are still the weakest link (Aldawood & Skinner, 2018). Changing beliefs and behaviour is a complex procedure that needs more research. However, the present study offers clear insight into specific individual characteristics that make people more vulnerable to cybercrimes. Using these characteristics to design training programs is a sensible approach to the tuning of security awareness messages. Similarly, the results of this research will be helpful in conducting more successful training programs that incorporate the identified essential attributes from the four proposed perspectives, as educational elements to increase people's awareness. While these identified factors might reflect a user's weak points, the factors could also be targeted by enforcing behavioural security strategies in order to mitigate social engineering threats.

The proposed user competence measure can also be useful if targeted by training programs. For example, designing a training program that focuses exclusively on increasing people's security awareness, privacy awareness, and self-efficacy can contribute to increasing individual competence to deal with threats, as revealed by this study's results. Initiating such

customised programs might protect organisations from potential financial and reputational damage. The present study's results signify the importance of perceived severity of threats in preventing people from being vulnerable to them. This can be beneficial when designing training programs. If the severity of losing sensitive information in social networks is emphasised in an awareness campaign, for instance, this will potentially increase compliance with protective behaviour and safe practice, as confirmed by this study's empirical results.

Determining user competence level has many practical benefits for individuals and, more importantly, for organisations. For example, organisations often conduct information security training programs without differentiating between employees in terms of their knowledge or skills. Such differentiation could make training programs more specialised and meaningful if designed to meet the needs of particular groups of employees. Otherwise, the result is likely to be generic programs having less effect (Spears & Barki, 2010). Identifying the dimensions that reflect user competence would simplify the task of classifying users based on their competence and could facilitate the design of tailored training sessions. The present research investigated the user competence dimensions in relation to detecting online threats in the context of social networks. One of the main contributions of this study is to propose measurement scales that can be used to model the user competence construct. This has been combined with an approach to validating those measurements, with a view to its use in future studies.

Organisations can use the proposed UCF to evaluate and understand employee perspectives when using social networks in order to initiate more effective interventions. Several types of intervention can be generated based on the present research findings. Education-based interventions can be proposed to enhance people's awareness and skills in detecting social networks threats. Also, special-features interventions could be designed to address the weak points of a specific group of people. For example, if a particular company noticed a lack of privacy awareness in their employees, a tool could be designed to offer more efficient privacy control in keeping with the company's policy and needs.

The developed conceptual model could be used in the assessment process for an organisation's employees, especially those working in sensitive positions. Also, the model and associated scales could be of help in employment evaluation tests, particularly in security-critical institutions, since the proposed model may predict those weak aspects of an individual that could increase his/her vulnerability to social engineering.

10.7.3 A Service Scenario for Using the Proposed Framework

This section introduces a potential service scenario that can make it possible to extract a user's vulnerabilities based on the proposed UCF. Figure 10.4 presents the six steps that can identify and protect against users' vulnerabilities. Firstly, using the four proposed perspectives, the considered population's ability to deal with cyber-attacks can be tested. In this step, users' behaviour and perceptions can be collected either by monitoring or by designing a questionnaire. After that, an analysis of the received data is essential to estimate the weakest points of the considered population and to determine which perspective is considered at risk. The vulnerable perspective can be regarded as the driver for training in the subsequent step.

A purpose-focused training session will be designed specifically for vulnerable users, thereby reducing the cost of training sessions for everyone in the considered population. Furthermore, designing interventions that could serve as a back-up for the identified weak points of vulnerable users would be useful. Finally, this process can be beneficial if conducted on a regular basis (e.g. annually). For example, if the monitoring process should reveal that the population's security and privacy awareness are limited, this would indicate vulnerability to exploitation in the perceptual perspective of those users. Therefore, designing a training program that focuses on increasing users' perception of the risks arising from their work environment would be appropriate. The training may present real case examples of how users can maintain their knowledge and ability to secure their private data. Additionally, algorithms can be developed based on the proposed characteristics, in order to automatically identify vulnerable individuals in the population and provide security interventions that protect them.

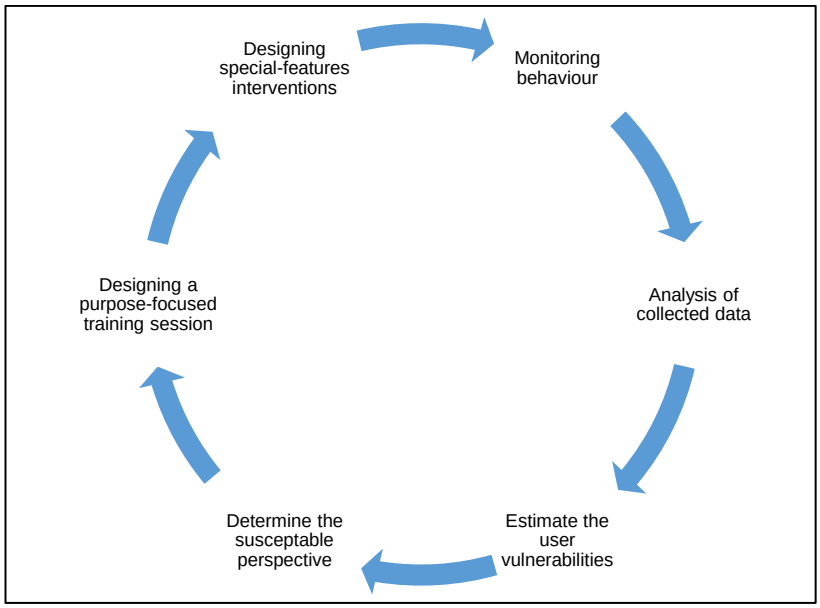


Figure 10.4 A Service Scenario for Using UCF

10.8 Summary of Main Contributions

Table 10.2 presents all the main contributions of the current research along with their key theoretical and practical benefits.

Table 10.2 Key Benefits of Main Contributions of the Current Research

Research Main Contribution	Key Benefits	
	Theoretical	**Practical**
User-Centric Framework	• Proposing the user-centric framework that incorporates four different perspectives is a novel contribution to social network theories and more importantly to research investigating human behaviour. • Incorporating experts' evaluation of the framework provides evidence for the importance of the four user-related perspectives: socio-psychological, habitual, perceptual, and socio-emotional, in examining people's judgement and response to SE-based attacks in the SN context.	• Proposing a service scenario that can enable extracting user's vulnerabilities based on the proposed user-centric framework. • Helpful for conducting more successful training programs that incorporate the identified essential attributes from the four proposed perspectives, as educational elements to increase people's awareness. • Organisations can use the proposed user-centric framework to evaluate and understand employee perspectives when using social networks in order to initiate more effective interventions.
The Conceptual Model	• Integrating different theories such as protection motivation theory, the five personality traits, and competence conceptualisation to build a new holistic model provides a better understanding of people's behaviour toward social engineering attacks in the social network context. • The model shows an acceptable prediction ability of people's vulnerability to social engineering in social networks. • Useful for information security researchers and researchers from different fields to predict people's responses to different security-oriented risks.	• The model is useful for helping SN providers to develop more effective security and privacy settings. o A live chat threat report must be essential in SN channels in order to reduce the number of potential victims of specific threatening posts or accounts. • Revealing that women users of SNs are more vulnerable to SE could help developers to design more effective defensive tools. o Providing security management tools for women to control their SN profiles easily and effectively. • Determining user competence level has many practical benefits for individuals and more importantly for organisations. o The competence dimensions and measure that have been proposed in the present study could provide a foundation for automatically identifying less competent users and could allow social network providers to take extra steps to protect this group of users. • Useful in the assessment process for an organisation's employees, especially those working in sensitive positions. • Useful for training programs. o Differentiating between employees in terms of their knowledge or skills could make training programs more specialised and meaningful if designed to meet the needs of particular groups of employees. o Designing a training program that focuses exclusively on increasing people's security awareness, privacy awareness, and self-efficacy can contribute to increasing individual competence to deal with threats.
An Architecture of a Semi-Automated Security Advisory System	• This research proposed a novel architecture of a semi-automated security advisory system.	• An approach to classifying social network users according to their vulnerability type and level. • Useful for enabling focused social media channels such as social groups, social communities, and company profiles to target their audience by designing advertisements focused on needs, as well as awareness posts. • Useful for SN providers to focus on people who require greater protection. • Provides insight that could help SN providers to enhance their security strategies by facilitating future classification through: o Encouraging people to report their victimisation. o Recording users' behaviour attributes.

10.9 Recommendations for Future Research

As an extension of the present research, the framework could be enhanced to suit different security issues related to cloud computing or Internet-of-Things, in order to understand the key factors affecting the individual's threat detection ability in these contexts. Since the proposed UCF could help in determining the competence level of social network users for detecting social engineering-based attacks, this could provide new technical solutions that rely on monitoring human activities: for example, enriching security alerts by integrating network intelligence and insights into human behaviour. Future research can go further by automatically classifying social network users based on the framework's attributes, which can be retrieved from the network in order to add an extra layer of security for those characterised as more vulnerable.

The conceptual study model could be used to test user vulnerability to different types of privacy or security hazards associated with the use of social networks: for instance, by measuring users' response to the risk related to loose privacy restrictions, or to sharing private information on the network. Furthermore, investigating whether social network users have different levels of vulnerability to privacy and security associated risks is another area of potential future research. The proposed model's prediction efficiency could be compared to different types of security and privacy threats. This comparison would offer a reasonable future direction for researchers to consider.

Future research could focus more on improving the proposed model by giving perceived trust greater attention, as this factor was the highest behaviour predictor in the present model. The novel conceptualisation of users' competence in the conceptual model has proved to have a profound influence on their behaviour toward social engineering victimisation, a finding which can offer additional new insight for future investigations.

Another element that is considered worthy of further scientific study is user motivation. While the result of the present research indicated the importance of this element, this factor needs further investigation. Many insights can be gained from research that focuses only on this element and investigates all its dimensions in relation to people's vulnerability. In the current study, as this element was being examined for the first time, it was risky to give it so much attention inasmuch as a result could be disappointing. However, as the motivation impact on user vulnerability was positive, this could be taken as an incentive for future researchers to investigate motivation as a stand-alone factor. Undertaking a qualitative study would be an appropriate way to explore this phenomenon.

Another potential gap in the literature can be noticed in the area of automatically predicting vulnerable individuals based on features extracted directly from the network. Considering this area for future research is likely to prove valuable. Further efforts are needed in this sphere, as predicting human behaviour is a complex task. The present study offers a basis for investigating the impact of different dimensions of user characteristics that affect human vulnerability to social engineering-based attacks.

10.10 Chapter Summary

Information security uses various efficient technical and non-technical protection methods. Social engineering-based attacks pose one of the most concerning online risks, and one that is hard to detect by those methods, as these attacks tend to target and exploit points of human weakness. The findings of this research clearly highlight the fact that social engineering attacks in the social network context are still successful. Limited research has investigated why people are easily deceived by social engineering attacks in the social network context, in order to help individuals, organisations, and researchers to tackle this problem and design more effective countermeasures. Thus, assessing users' characteristics and behaviour that impact on users' vulnerability is essential in combatting social engineering risks. Knowing where the weakness resides can help focus awareness-raising and target training sessions for those individuals, with the aim of reducing their likely victimisation. Theories that guide user behaviour, such as protection motivation theory, the five personality traits, and competence conceptualisation have not been integrated previously as antecedents of users' online risky behaviour. The present thesis provides exploratory research which investigates and evaluates the associations between these theories and other user-related factors as predictors of user vulnerability to social engineering-based attacks.

This thesis has presented a novel framework and model to show how user behaviour can be predicted, based on the integration of socio-psychological, habitual, perceptual, and socio-emotional perspectives. The results of this study fill a vital gap in the literature, since socio-emotional and perceptual factors, which have been given less attention in earlier literature, have proved to be critical aspects in predicting users' online behaviour. The research indicated 18 factors that impact on a user's vulnerability either positively or negatively. Among these, the user's trust and involvement in the network are the strongest predictors of the person's likelihood of victimisation. In general, the developed model showed an acceptable prediction ability regarding users' vulnerability and provided guidance to the decision-making process within organisations, since it is feasible to use this model as an assessment method for

online users or employees working with sensitive and critical data. This research articulates ways in which training stakeholders may improve their programs by incorporating the identified attributes as educational elements and designing focused programs that aim to enhance the three sources of people's competency to deal with threat: namely, self-efficacy, security awareness, and privacy awareness.

This research has made the first attempt to determine what combination of characteristics make a user the most vulnerable to a particular type of social engineering attack in social networks. Based on the findings of this research, it might be useful for social network providers to record users' behaviour attributes, design easy-to-use security management tools for female users, provide a live chat through which to report security incidents, and run a regular and up-to-date awareness campaign. Additionally, these findings have allowed this research to develop an innovative solution that can mitigate social engineering attacks, by designing a semi-automated advisory system.

Social network users have different personalities, experiences, and backgrounds. Limited research in this field seeks to consider these differences and offer personalised advice that suits different users' needs. Clearly, providing inappropriate and random training programs and recommendations can have expensive and ineffective results. Linking social network users' characteristics with their type and level of vulnerabilities is another novel achievement of this research, affording a significant theoretical and practical foundation for developing user profiling mechanisms as well as efficient countermeasures.

Based on the idea of user profiling, this research has established a practical solution which can semi-automatically predict users' vulnerability to various types of social engineering attacks. The present thesis has provided an architecture for a personalised advisory system that aims to identify which group of social network users are more susceptible to these types of attacks. Significant outcomes were noted with practical implications for how social network users could be assessed and segmented based on their characteristics, behaviour, and vulnerabilities, in turn facilitating their protection from such threats by targeting them with relevant advice and education that meets users' needs. This system is considered cost and time effective, as integrating individuals' needs with the administrator's knowledge of existing threats could avoid the overhead and inconvenience of sending blanket advice to all users.

It is important to further expand studies that investigate people's vulnerabilities, as the up-to-date information produced from such research is substantial, enabling training and awareness programs, social network providers, and the individual user to be kept fully informed about users' weaknesses and limits and how to diminish their vulnerabilities. Future

studies could focus on examining and comparing users' vulnerability to other security and privacy risks. Focusing on improving the proposed model and trying to automatically predict a user's vulnerability based on information extracted directly from the social network is another potentially useful area for future research.

REFERENCES

Abdul Molok, N. N., Ali, A. M., Talib, S., & Mahmud, M. (2014). Information security awareness through the use of social media. In *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICT4M.2014.7020668

Abulaish, M., & Bhat, S. Y. (2015). Classifier Ensembles Using Structural Features For Spammer Detection In Online Social Networks. *Foundations of Computing and Decision Sciences*, *40*(2), 89–105. https://doi.org/10.1515/fcds-2015-0006

Acquisti, A., Adjerid, I., Balebako, R. H., Brandimarte, L., Cranor, L. F., Komanduri, S., … Wilson, S. (2016). Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. *SSRN Electronic Journal*, *50*(3). https://doi.org/10.2139/ssrn.2859227

Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., & Razak, S. A. (2017). Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications*, *79*(November 2016), 41–67. https://doi.org/10.1016/j.jnca.2016.11.030

Aguti, B., Wills, G. B., & Walters, R. J. (2014). An evaluation of the factors that impact on the effectiveness of blended e-learning within universities. In *International Conference on Information Society* (pp. 117–121). IEEE. https://doi.org/10.1109/i-Society.2014.7009023

Al-Hamar, M., Dawson, R., & Guan, L. (2010). A Culture of Trust Threatens Security and Privacy in Qatar. In *2010 10th IEEE International Conference on Computer and Information Technology* (pp. 991–995). IEEE. https://doi.org/10.1109/CIT.2010.182

Al-Qurishi, M., Alrubaian, M., Rahman, S. M. M., Alamri, A., & Hassan, M. M. (2018). A prediction system of Sybil attack in social network using deep-regression model. *Future Generation Computer Systems*, *87*, 743–753. https://doi.org/10.1016/j.future.2017.08.030

Al Omoush, K. S., Yaseen, S. G., & Atwah Alma'aitah, M. (2012). The impact of Arab cultural values on online social networking: The case of Facebook. *Computers in Human Behavior*, *28*(6), 2387–2399. https://doi.org/10.1016/j.chb.2012.07.010

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering* (pp. 62–68). IEEE. https://doi.org/10.1109/TALE.2018.8615162

Alexander, C. S., & Becker, H. J. (1978). The Use of Vignettes in Survey Research. *Public Opinion Quarterly*, *42*(1), 93. https://doi.org/10.1086/268432

Algarni, A., & Xu, Y. (2013). Social Engineering in Social Networking Sites: Phase-Based and Source-

Based Models. *International Journal of E-Education, e-Business, e-Management and e-Learning*, *3*(6), 456–463. https://doi.org/10.7763/IJEEEE.2013.V3.278

Algarni, A., Xu, Y., & Chan, T. (2015). Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook. In *36th International Conference on Information Systems* (pp. 1–23).

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Algarni, A., Xu, Y., Taizan Chan, & Yu-Chu Tian. (2013). Social engineering in social networking sites: Affect-based model. In *2013 IEEE Third International Conference on Information Science and Technology (ICIST)* (pp. 508–515). IEEE. https://doi.org/10.1109/ICIST.2013.6747602

Alqarni, Z., Algarni, A., & Xu, Y. (2016). Toward Predicting Susceptibility to Phishing Victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC)* (pp. 419–426). IEEE. https://doi.org/10.1109/SCC.2016.61

Alqubaiti, Z. Y. (2016). *The Paradox of Social Media Security: A Study of IT Students ' Perceptions versus Behavior on Using Facebook*. *Masters dissertation*. Kennesaw State University. Retrieved from https://digitalcommons.kennesaw.edu/msit_etd/3

Alseadoon, I. (2014). *The impact of users' characteristics on their ability to detect phishing emails*. *Doctoral Thesis*. Queensland University of Technology.

Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails? In H. A. Sulaiman, M. A. Othman, M. F. I. Othman, Y. A. Rahim, & N. C. Pee (Eds.), *Advanced Computer and Communication Engineering Technology* (Vol. 315, pp. 949–962). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07674-4_89

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Amichai-Hamburger, Y., & Vinitzky, G. (2010). Social network use and personality. *Computers in Human Behavior*, *26*(6), 1289–1295. https://doi.org/10.1016/j.chb.2010.03.018

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology*, *76*(5), 732–740. https://doi.org/10.1037/0021-9010.76.5.732

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., … Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Andreassen, C. S., Pallesen, S., & Griffiths, M. D. (2017). The relationship between addictive use of social media, narcissism, and self-esteem: Findings from a large national survey. *Addictive Behaviors*, *64*, 287–293. https://doi.org/10.1016/j.addbeh.2016.03.006

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and Individual Differences*, *124*, 150–159. https://doi.org/10.1016/j.paid.2017.12.018

Baabdullah, A. M. (2018). Consumer adoption of Mobile Social Network Games (M-SNGs) in Saudi Arabia: The role of social influence, hedonic motivation and trust. *Technology in Society*, *53*, 91–102. https://doi.org/10.1016/j.techsoc.2018.01.004

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and Reliability Reporting Practices in the Field of Health Education and Behavior A Review of Seven Journals. *Health Education & Behavior*, *41*(1), 12–18. https://doi.org/10.1177/1090198113483139

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Barwise, P., & Watkins, L. (2018). The evolution of digital dominance: how and why we got to GAFA. In *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (pp. 21–49). Oxford University Press.

Basak, E., & Calisir, F. (2015). An empirical study on factors affecting continuance intention of using Facebook. *Computers in Human Behavior*, *48*, 181–189. https://doi.org/10.1016/j.chb.2015.01.055

Beldad, A. D., & Hegner, S. M. (2017). More Photos From Me to Thee: Factors Influencing the Intention to Continue Sharing Personal Photos on an Online Social Networking (OSN) Site among Young Adults in the Netherlands. *International Journal of Human–Computer Interaction*, *33*(5), 410–422. https://doi.org/10.1080/10447318.2016.1254890

Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. (2010). Detecting spammers on twitter. In *Seventh annual Collaboration, Electronic messaging, Anti- Abuse and Spam Conference (CEAS)*. Redmond,Washington.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Purpose of social networking use and victimisation: Are there any differences between university students and those not in HE? *Computers in Human Behavior*, *51*, 867–872. https://doi.org/10.1016/j.chb.2014.11.034

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606. https://doi.org/10.1037//0033-

2909.88.3.588

Bertino, E., & Ferrari, E. (2018). Big Data Security and Privacy. In S. Flesca, S. Greco, E. Masciari, & D. Saccà (Eds.), *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years* (Vol. 31, pp. 425–439). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-61893-7_25

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web* (pp. 551–560). New York, USA: ACM Press. https://doi.org/10.1145/1526709.1526784

Binks, A. (2019). The art of phishing: past, present and future. *Computer Fraud & Security*, *2019*(4), 9–11. https://doi.org/10.1016/S1361-3723(19)30040-5

Bohme, R., & Moore, T. (2012). How do consumers react to cybercrime? In *2012 eCrime Researchers Summit* (pp. 1–12). IEEE. https://doi.org/10.1109/eCrime.2012.6489519

Bossetta, M. (2018). The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy. *Journal of International Affairs*, *71*(1.5), 97–106. Retrieved from https://www.jstor.org/stable/26508123

Bracken, B. A., & Barona, A. (1991). State of the Art Procedures for Translating, Validating and Using Psychoeducational Tests in Cross-Cultural Assessment. *School Psychology International*, *12*, 119–132. https://doi.org/10.1177/0143034391121010

Brandtzæg, P. B., & Heim, J. (2009). Why People Use Social Networking Sites. In A. A. Ozok & P. Zaphiris (Eds.), *Online Communities and Social Computing* (Vol. 5621, pp. 143–152). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-02774-1_16

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology* (pp. 57–71). Washington: American Psychological Association. https://doi.org/10.1037/13620-004

Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology*, *1*(3), 185–216.

Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival*, *55*(2), 81–96. https://doi.org/10.1080/00396338.2013.784468

Buettner, R. (2017). Predicting user behavior in electronic markets based on personality-mining in large online social networks. *Electronic Markets*, *27*(3), 247–265. https://doi.org/10.1007/s12525-016-0228-z

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. M. (2016). When 'friends' collide: Social heterogeneity and user vulnerability on social network sites. *Computers in Human Behavior*, *54*, 62–72. https://doi.org/10.1016/j.chb.2015.07.039

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security*, *25*(5), 593–613. https://doi.org/10.1108/ICS-03-2017-0009

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal Deception Theory. *Communication Theory*, *6*(3), 203–242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Cao, B., & Lin, W.-Y. (2015). How do victims react to cyberbullying on social networking sites? The influence of previous cyberbullying victimization experiences. *Computers in Human Behavior*, *52*, 458–465. https://doi.org/10.1016/j.chb.2015.06.009

Cao, J., Basoglu, K. A., Sheng, H., & Lowry, P. B. (2015). A systematic review of social networks research in information systems: Building a foundation for exciting future research. *Communications of the Association for Information Systems*, *36*(1), 727–758. Retrieved from https://ssrn.com/abstract=2525108

Carminati, B., Ferrari, E., & Perego, A. (2009). Enforcing access control in Web-based social networks. *ACM Transactions on Information and System Security*, *13*(1), 1–38. https://doi.org/10.1145/1609956.1609962

Carstensen, L. L., Isaacowitz, D. M., & Charles, S. T. (1999). Taking time seriously: A theory of socioemotional selectivity. *American Psychologist*, *54*(3), 165–181. https://doi.org/10.1037/0003-066X.54.3.165

Chabrol, H., Laconi, S., Delfour, M., & Moreau, A. (2017). Contributions of Psychopathological and Interpersonal Variables to Problematic Facebook Use in Adolescents and Young Adults. *International Journal of High Risk Behaviors and Addiction*, *6*(1). https://doi.org/10.5812/ijhrba.32773

Chaiken, S., Liberman, A., & Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. In J. S. Uleman & J. A. Bargh (Eds.), *Unintended thought* (pp. 212–252). New York: Guilford Press.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, *30*, 79–86. https://doi.org/10.1016/j.chb.2013.07.059

Chang, P. F., Choi, Y. H., Bazarova, N. N., & Löckenhoff, C. E. (2015). Age Differences in Online Social Networking: Extending Socioemotional Selectivity Theory to Social Network Sites. *Journal of Broadcasting & Electronic Media*, *59*(2), 221–239.

https://doi.org/10.1080/08838151.2015.1029126

Chen, H. (2012). Relationship between Motivation and Behavior of SNS User. *Journal of Software*, *7*(6), 1265–1272. https://doi.org/10.4304/jsw.7.6.1265-1272

Cheung-Blunden, V., & Ju, J. (2016). Anxiety as a Barrier to Information Processing in the Event of a Cyberattack. *Political Psychology*, *37*(3), 387–400. https://doi.org/10.1111/pops.12264

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279–299. https://doi.org/10.1108/IntR-09-2013-0192

Chin, W. W. (2010). How to Write Up and Report PLS Analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of Partial Least Squares* (pp. 655–690). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_29

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. G. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems*, *42*(3), 1872–1888. https://doi.org/10.1016/j.dss.2006.04.001

Chiu, C.-M., Wang, E. T. G., Fang, Y.-H., & Huang, H.-Y. (2014). Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information Systems Journal*, *24*(1), 85–114. https://doi.org/10.1111/j.1365-2575.2012.00407.x

Cho, J.-H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. In *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. IEEE. https://doi.org/10.1109/COGSIMA.2016.7497779

Chua, Y. P., & Chua, Y. P. (2017). Do computer-mediated communication skill, knowledge and motivation mediate the relationships between personality traits and attitude toward Facebook? *Computers in Human Behavior*, *70*, 51–59. https://doi.org/10.1016/j.chb.2016.12.034

Cialdini, R. B. (2001). *Influence : science and practice*. Boston: Allyn & Bacon.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.).

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608.

Costa, P. T., & McCrae, R. R. (1992). Four ways five factors are basic. *Personality and Individual Differences*, *13*(6), 653–665. https://doi.org/10.1016/0191-8869(92)90236-I

Costa, P. T., Terracciano, A., & McCrae, R. R. (2001). Gender differences in personality traits across cultures: Robust and surprising findings. *Journal of Personality and Social Psychology*, *81*(2), 322–331. https://doi.org/10.1037/0022-3514.81.2.322

Costello, A. B., & Osborne, J. W. (2005). Best Practices in Exploratory Factor Analysis : Four Recommendations for Getting the Most From Your Analysis. *Practical Assessment, Research & Evaluation*, *10*(7).

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative and Mixed Method Aproaches*. *SAGE Publications* (Fifth edit).

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user ' s susceptibility to social engineering attacks. In *proceedings ofthe 16th Australian Information Security Management Conference* (pp. 83–89). https://doi.org/10.25958/5c528ffa66693

Darwish, A., Zarka, A. El, & Aloul, F. (2012). Towards understanding phishing victims' profile. In *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCSII.2012.6454454

Di Giunta, L., Alessandri, G., Gerbino, M., Luengo Kanacri, P., Zuffiano, A., & Caprara, G. V. (2013). The determinants of scholastic achievement: The contribution of personality traits, self-esteem, and academic self-efficacy. *Learning and Individual Differences*, *27*, 102–108. https://doi.org/10.1016/j.lindif.2013.07.006

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index Construction with Formative Indicators: An Alternative to Scale Development. *Journal of Marketing Research*, *38*(2), 269–277. https://doi.org/10.1509/jmkr.38.2.269.18845

Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *ArXiv Preprint*. Retrieved from http://arxiv.org/abs/1811.06078

Dijkstra, T. K., & Henseler, J. (2015). Consistent and asymptotically normal PLS estimators for linear structural equations. *Computational Statistics & Data Analysis*, *81*, 10–23. https://doi.org/10.1016/j.csda.2014.07.008

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. In *Proceedings of Americas Conference on Information Systems (AMCIS)* (p. 339).

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, *69*, 18–34. https://doi.org/10.1016/j.cose.2016.12.013

Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. (2017). Towards Detecting Compromised Accounts on Social Networks. *IEEE Transactions on Dependable and Secure Computing*, *14*(4), 447–460. https://doi.org/10.1109/TDSC.2015.2479616

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*, *9*(1), 1–11. https://doi.org/10.5815/ijcnis.2017.01.01

Farrahi, K., & Zia, K. (2017). Trust reality-mining: evidencing the role of friendship for trust diffusion. *Human-Centric Computing and Information Sciences*, *7*(1), 4. https://doi.org/10.1186/s13673-016-0085-y

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Ferguson, E., & Cox, T. (1993). Exploratory Factor Analysis: A Users' Guide. *International Journal of Selection Assessment*, *1*(2), 84–94.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96–104. https://doi.org/10.1145/2818717

Finn, A., & Wang, L. (2014). Formative vs. reflective measures: Facets of variation. *Journal of Business Research*, *67*(1), 2821–2826. https://doi.org/10.1016/j.jbusres.2012.08.001

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019–2036. https://doi.org/10.1109/COMST.2014.2321628

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security*, *23*(2), 178–199. https://doi.org/10.1108/ICS-05-2014-0029

Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, *22*(4), 393–406. https://doi.org/10.1108/IMCS-11-2013-0083

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Fokes, E., & Li, L. (2014). A survey of security vulnerabilities in social networking media. In *Proceedings of the 3rd annual conference on Research in information technology - RIIT '14* (pp. 57–62). New York, USA: ACM Press. https://doi.org/10.1145/2656434.2656444

Foozy, C., Ahmad, R., Abdollah, M., Yusof, R., & Mas'ud, M. Z. (2011). Generic Taxonomy of Social Engineering Attack. In *Malaysian Technical Universities International Conference on Engineering Technology MUiCET (2011)*.

Fu, Q., Feng, B., Guo, D., & Li, Q. (2018). Combating the evolving spammers in online social networks.

Computers & Security, *72*, 60–73. https://doi.org/10.1016/j.cose.2017.08.014

Gan, D., & Jenkins, L. (2015). Social Networking Privacy—Who's Stalking You? *Future Internet*, *7*(4), 67–93. https://doi.org/10.3390/fi7010067

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security Issues in Online Social Networks. *IEEE Internet Computing*, *15*(4), 56–63. https://doi.org/10.1109/MIC.2011.50

General Authority for Statistics. (2016). *Demography Survey 2016*. Retrieved from http://www.stats.gov.sa/sites/default/files/ar-demographic-research-2016_0.pdf

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. Retrieved from https://aisel.aisnet.org/jais/vol18/iss1/2

Götz, O., Liehr-Gobbers, K., & Krafft, M. (2010). Evaluation of Structural Equation Models Using the Partial Least Squares (PLS) Approach. In V. Esposito Vinzi, W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of Partial Least Squares* (pp. 691–711). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_30

Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. *Group Decision and Negotiation*, *13*(2), 149–172. https://doi.org/10.1023/B:GRUP.0000021839.04093.5d

Gregory, R. J. (2007). *Psychological testing: History, principles, and applications*. (P. International, Ed.) (Fifth Edit). Allyn and Bacon.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In *2014 IEEE Security and Privacy Workshops* (pp. 236–250). IEEE. https://doi.org/10.1109/SPW.2014.39

Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010). @spam: The Underground on 140 Characters or Less. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 27–37). New York, USA: ACM Press. https://doi.org/10.1145/1866307.1866311

Griffin, R. (2018). *A Demographic Analysis to Determine User Vulneraability among Several Categories of Phishing*. *Masters dissertation*. Dublin Institute of Technology.

Griffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the Heuristic-Systematic Model and Depth of Processing. *Communication Research*, *29*(6), 705–732. https://doi.org/10.1177/009365002237833

Guay, R. P., Choi, D., Oh, I.-S., Mitchell, M. S., Mount, M. K., & Shin, K.-H. (2016). Why people harm the organization and its members: Relationships among personality, organizational commitment, and workplace deviance. *Human Performance*, *29*(1), 1–15. https://doi.org/10.1080/08959285.2015.1120305

Gundecha, P., Barbier, G., & Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 511–519). New York, USA: ACM Press. https://doi.org/10.1145/2020408.2020489

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Gupta, N., Aggarwal, A., & Kumaraguru, P. (2014). bit.ly/malicious: Deep dive into short URL based e-crime detection. In *2014 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 14–24). IEEE. https://doi.org/10.1109/ECRIME.2014.6963161

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: a global perspective* (7th Editio). New Jersey, USA: Pearson Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd Ed.). SAGE Publications.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, Personality Traits and Facebook. *ArXiv Preprint*. Retrieved from http://arxiv.org/abs/1301.7643

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, *48*(3), 1–39. https://doi.org/10.1145/2835375

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., … Calantone, R. J. (2014). Common Beliefs and Reality About PLS. *Organizational Research Methods*, *17*(2), 182–209. https://doi.org/10.1177/1094428114526928

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, *20*(1), 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337–347. https://doi.org/10.1016/j.im.2014.12.006

Hoehle, H., & Venkatesh, V. (2015). Mobile Application Usability: Conceptualization and Instrument

Development. *MIS Quarterly*, *39*(2), 435–472. https://doi.org/10.25300/MISQ/2015/39.2.08

Holz, H. J., Applin, A., Haberman, B., Joyce, D., Purchase, H., & Reed, C. (2006). Research methods in computing: what are they, and how should we teach them? *ACM SIGCSE Bulletin*, *38*(4), 96–114. https://doi.org/10.1145/1189136.1189180

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74. https://doi.org/10.1145/2063176.2063197

Hornsby, J. S., Kuratko, D. F., Holt, D. T., & Wales, W. J. (2013). Assessing a Measurement of Organizational Preparedness for Corporate Entrepreneurship. *Journal of Product Innovation Management*, *30*(5), 937–955. https://doi.org/10.1111/jpim.12038

Howard, M. C., & Melloy, R. C. (2016). Evaluating Item-Sort Task Methods: The Presentation of a New Statistical Significance Formula and Methodological Best Practices. *Journal of Business and Psychology*, *31*(1), 173–186. https://doi.org/10.1007/s10869-015-9404-y

Hu, H., Ahn, G.-J., & Jorgensen, J. (2013). Multiparty Access Control for Online Social Networks: Model and Mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, *25*(7), 1614–1627. https://doi.org/10.1109/TKDE.2012.97

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods*, *3*(4), 424–453. https://doi.org/10.1037/1082-989X.3.4.424

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards Automating Social Engineering Using Social Networking Sites. In *2009 International Conference on Computational Science and Engineering* (pp. 117–124). IEEE. https://doi.org/10.1109/CSE.2009.205

Hyman, P. (2013). Cybercrime: It's Serious, But Exactly How Serious? *Communications of the ACM*, *56*(3), 18. https://doi.org/10.1145/2428556.2428563

Inouye, J. (2014). *Risk Perception: Theories, Strategies, And Next Steps*. *Campbell Institute National Safety Council*.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse Social Engineering Attacks in Online Social Networks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 55–74). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22424-9_4

Islam, M. B., Watson, J., Iannella, R., & Geva, S. (2017). A greater understanding of social networks privacy requirements: The user perspective. *Journal of Information Security and Applications*, *33*, 30–44. https://doi.org/10.1016/j.jisa.2017.01.004

Islam, R., & Abawajy, J. (2013). A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications*, *36*(1), 324–335. https://doi.org/10.1016/j.jnca.2012.05.009

ISO/IEC 27000. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved February 19, 2018, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, *6*(1), 8. https://doi.org/10.1186/s13673-016-0065-2

Jagatic, T. N., Johnson, N. a., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jakobowicz, E., & Derquenne, C. (2007). A modified PLS path modeling algorithm handling reflective categorical variables and a new model building strategy. *Computational Statistics & Data Analysis*, *51*(8), 3666–3678. https://doi.org/10.1016/j.csda.2006.12.004

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Mudassar Alam, S., & Ashraf, R. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 5040–5048). IEEE. https://doi.org/10.1109/BigData.2018.8622505

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

Johnson, P. (2001). Detecting deception: adversarial problem solving in a low base-rate world. *Cognitive Science*, *25*(3), 355–392. https://doi.org/10.1016/S0364-0213(01)00040-4

Joinson, A. N. (2008). Looking at, looking up or keeping up with people? Motives and Uses of Facebook. In *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems* (pp. 1027–1036). New York, USA: ACM Press. https://doi.org/10.1145/1357054.1357213

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255–260. https://doi.org/10.1126/science.aaa8415

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. https://doi.org/10.1016/j.chb.2016.09.012

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, *3–4*, 1–21. https://doi.org/10.1016/j.osnem.2017.09.001

Khan, B., Alghathbar, K., Nabi, S., & Khan, M. (2011). Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, *5*(26), 10862–10868. https://doi.org/10.5897/AJBM11.067

Khlobystova, A., Abramov, M., & Tulupyev, A. (2019). An Approach to Estimating of Criticality of

Social Engineering Attacks Traces. In O. Dolinina, A. Brovko, V. Pechenkin, A. Lvov, V. Zhmud, & V. Kreinovich (Eds.), *Recent Research in Control Engineering and Decision Making* (Vol. 199, pp. 446–456). Springer International Publishing. https://doi.org/10.1007/978-3-030-12072-6_36

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective*, *22*(4), 171–179. https://doi.org/10.1080/19393555.2013.828803

Kim, Y. H., Kim, D. J., & Wachter, K. (2013). A study of mobile user engagement (MoEN): Engagement motivations, perceived value, satisfaction, and continued engagement intention. *Decision Support Systems*, *56*(1), 361–370. https://doi.org/10.1016/j.dss.2013.07.002

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, *65*(23), 2276–2284. https://doi.org/10.2146/ajhp070364

Kiss, G., & Szasz, A. (2016). Level of the information security awareness of the mechanical engineering students. In *15th International Conference on Information Technology Based Higher Education and Training (ITHET)* (pp. 1–6). IEEE. https://doi.org/10.1109/ITHET.2016.7760758

Knijnenburg, B. P. (2017). Privacy? I Can't Even! Making a Case for User-Tailored Privacy. *IEEE Security & Privacy*, *15*(4), 62–67. https://doi.org/10.1109/MSP.2017.3151331

Koo, C., Chung, N., & Kim, H.-W. (2015). Examining explorative and exploitative uses of smartphones: a user competence perspective. *Information Technology & People*, *28*(1), 133–162. https://doi.org/10.1108/ITP-04-2013-0063

Kottner, J., Audige, L., Brorson, S., Donner, A., Gajewski, B. J., Hróbjartsson, A., … Streiner, D. L. (2011). Guidelines for Reporting Reliability and Agreement Studies (GRRAS) were proposed. *International Journal of Nursing Studies*, *48*(6), 661–671. https://doi.org/10.1016/j.ijnurstu.2011.01.016

Kraiger, K., Ford, J. K., & Salas, E. (1993). Application of cognitive, skill-based, and affective theories of learning outcomes to new methods of training evaluation. *Journal of Applied Psychology*, *78*(2), 311–328. https://doi.org/10.1037/0021-9010.78.2.311

Krasnova, H., Veltri, N. F., Eling, N., & Buxmann, P. (2017). Why men and women continue to use social networking sites: The role of gender differences. *The Journal of Strategic Information Systems*, *26*(4), 261–284. https://doi.org/10.1016/j.jsis.2017.01.004

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS*

'09. New York, USA: ACM Press. https://doi.org/10.1145/1572532.1572536

Lakshmi, V. S., & Vijaya, M. S. (2012). Efficient prediction of phishing websites using supervised learning algorithms. *Procedia Engineering*, *30*(2011), 798–805. https://doi.org/10.1016/j.proeng.2012.01.930

Lauriola, M., & Weller, J. (2018). Personality and Risk: Beyond Daredevils— Risk Taking from a Temperament Perspective. In M. Raue, E. Lermer, & B. Streicher (Eds.), *Psychological Perspectives on Risk and Risk Analysis* (pp. 3–36). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-92478-6_1

Leedy, P. D., & Ormrod, J. E. (2015). *Practical Research: Planning and Design* (11th Editi). Pearson education.

Leftheriotis, I., & Giannakos, M. N. (2014). Using social media for work: Losing your time or improving your work? *Computers in Human Behavior*, *31*(1), 134–142. https://doi.org/10.1016/j.chb.2013.10.016

Leong, L.-Y., Jaafar, N. I., & Sulaiman, A. (2017). Understanding impulse purchase in Facebook commerce: does Big Five matter? *Internet Research*, *27*(4), 786–818. https://doi.org/10.1108/IntR-04-2016-0107

Liu, D., & Campbell, W. K. (2017). The Big Five personality traits, Big Two metatraits and social media: A meta-analysis. *Journal of Research in Personality*, *70*, 229–240. https://doi.org/10.1016/j.jrp.2017.08.004

Liu, D., Mei, B., Chen, J., Lu, Z., & Du, X. (2015). Community Based Spammer Detection in Social Networks. In J. Wang, H. Xiong, Y. Ishikawa, J. Xu, & J. Zhou (Eds.), *Web-Age Information Management* (pp. 554–558). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-319-21042-1_61

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 61–70). New York, USA: ACM Press. https://doi.org/10.1145/2068816.2068823

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems*, *26*(6), 546–563. https://doi.org/10.1057/s41303-017-0066-x

Luo, X. (Robert), Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28–38. https://doi.org/10.1016/j.cose.2012.12.003

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334. Retrieved from

http://dl.acm.org/citation.cfm?id=2017510%5Cnpapers3://publication/uuid/E4D3717C-7F3F-4791-8835-141D4309976B

Madden, M. (2012). *Privacy management on social media sites*. *Pew Research center*. Retrieved from http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). *Teens, social media, and privacy*. *Pew Research center*. Retrieved from http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

Madejski, M., & Bellovin, S. M. (2011). *The Failure of Online Social Network Privacy Settings*. *Technical Report CUCS-010-11, Columbia University*.

Mahuteau, S., & Zhu, R. (2016). Crime Victimisation and Subjective Well-Being: Panel Evidence From Australia. *Health Economics*, *25*(11), 1448–1463. https://doi.org/10.1002/hec.3230

Mansour, R. F. (2016). Understanding how big data leads to social networking vulnerability. *Computers in Human Behavior*, *57*, 348–351. https://doi.org/10.1016/j.chb.2015.12.055

Marcolin, B. L., Compeau, D. R., Munro, M. C., & Huff, S. L. (2000). Assessing User Competence: Conceptualization and Measurement. *Information Systems Research*, *11*(1), 37–60. https://doi.org/10.1287/isre.11.1.37.11782

Marriott, C. (2018). *Through the Net: Investigating How User Characteristics Influence Susceptibility to Phishing*. *Masters dissertation*. Dublin Institute of Technology.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*(May 2018), 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological Methods*, *17*(3), 437–455. https://doi.org/10.1037/a0028085

Messias, J., Schmidt, L., Oliveira, R., & Benevenuto, F. (2013). You followed my bot! Transforming robots into influential users in Twitter. *First Monday*, *18*(7). https://doi.org/10.5210/fm.v18i7.4217

Mester, Y., Kökciyan, N., & Yolum, P. (2015). Negotiating Privacy Constraints in Online Social Networks. In F. Koch, C. Guttmann, & D. Busquets (Eds.), *Advances in Social Computing and*

Multiagent Systems (Vol. 541, pp. 112–129). Springer, Cham. https://doi.org/10.1007/978-3-319-24804-2_8

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Mircioiu, C., & Atkinson, J. (2017). A Comparison of Parametric and Non-Parametric Methods Applied to a Likert Scale. *Pharmacy*, *5*(4), 26. https://doi.org/10.3390/pharmacy5020026

Mitchell, B., & Alfuraih, A. (2018). The Kingdom of Saudi Arabia: Achieving the Aspirations of the National Transformation Program 2020 and Saudi Vision 2030 Through Education. *Journal of Education and Development*, *2*(3), 36. https://doi.org/10.20849/jed.v2i3.526

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element in Security*. John Wiley & Sons.

Modic, D., & Anderson, R. (2014). Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior*, *41*, 71–79. https://doi.org/10.1016/j.chb.2014.09.014

Mohebzada, J. G., Zarka, A. El, Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. In *2012 International Conference on Innovations in Information Technology (IIT)* (pp. 249–254). IEEE. https://doi.org/10.1109/INNOVATIONS.2012.6207742

Moore, K., & McElroy, J. C. (2012). The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior*, *28*(1), 267–274. https://doi.org/10.1016/j.chb.2011.09.009

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka (Eds.), *ICT and Society* (pp. 266–279). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44208-1_22

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Muhlbacher, T., & Piringer, H. (2013). A Partition-Based Framework for Building and Validating Regression Models. *IEEE Transactions on Visualization and Computer Graphics*, *19*(12), 1962–1971. https://doi.org/10.1109/TVCG.2013.125

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, *140*(4), 70–92. https://doi.org/10.1162/DAED_a_00116

Munro, M. C., Huff, S. L., Marcolin, B. L., & Compeau, D. R. (1997). Understanding and measuring user competence. *Information & Management*, *33*(1), 45–57. https://doi.org/10.1016/S0378-

7206(97)00035-9

Nikiforakis, N., Maggi, F., Stringhini, G., Rafique, M. Z., Joosen, W., Kruegel, C., … Zanero, S. (2014). Stranger danger. In *Proceedings of the 23rd international conference on World wide web - WWW '14* (pp. 51–62). New York, USA: ACM Press. https://doi.org/10.1145/2566486.2567983

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, *26*(3), 406–418. https://doi.org/10.1016/j.chb.2009.11.012

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust* (pp. 60–68). IEEE. https://doi.org/10.1109/STAST.2011.6059257

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Orchard, L. J., Fullwood, C., Galbraith, N., & Morris, N. (2014). Individual Differences as Predictors of Social Networking. *Journal of Computer-Mediated Communication*, *19*(3), 388–402. https://doi.org/10.1111/jcc4.12068

Parrish Jr., J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. In *Southwest Decision Sciences Institute (SWDSI) annual meeting* (pp. 285–296).

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28. https://doi.org/10.1108/09685221211219173

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. *Information Systems Security*, *15*(5), 13–21. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3

Petter, S., Straub, D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly*, *31*(4), 623–656. https://doi.org/10.2307/25148814

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Advances in experimental social psychology* (Vol. 19, pp. 123–205). https://doi.org/10.1016/S0065-2601(08)60214-2

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010). Using social networks to harvest email addresses. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society* (pp. 11–20). New York, USA: ACM Press. https://doi.org/10.1145/1866919.1866922

Ponemon Insititute LLC. (2017). *2017 Cost of Data Breach Study: Global Overview*. Retrieved from http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, *40*(3), 879–891. https://doi.org/10.3758/BRM.40.3.879

Proofpoint. (2018). *The Human Factor 2018 Report*. Retrieved from https://www.proofpoint.com/sites/default/files/pfpt-us-wp-human-factor-report-2018-180425.pdf

PwC. (2016). *Global Economic Crime Survey*. Retrieved from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Quercia, D., Lambiotte, R., Stillwell, D., Kosinski, M., & Crowcroft, J. (2012). The personality of popular facebook users. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work - CSCW '12* (pp. 955–964). New York, USA: ACM Press. https://doi.org/10.1145/2145204.2145346

Rae, J. R., & Lonborg, S. D. (2015). Do motivations for using Facebook moderate the association between Facebook use and psychological well-being? *Frontiers in Psychology*, *6*, 771. https://doi.org/10.3389/fpsyg.2015.00771

Rahman, M. S., Huang, T.-K., Madhyastha, H. V, & Faloutsos, M. (2012). Efficient and Scalable Socware Detection in Online Social Networks. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security 12)* (pp. 663–678).

Rains, S. A., & Brunner, S. R. (2015). What can we learn about social network sites by studying Facebook? A call and recommendations for research on social network sites. *New Media & Society*, *17*(1), 114–131. https://doi.org/10.1177/1461444814546481

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of Research in Personality*, *41*(1), 203–212. https://doi.org/10.1016/j.jrp.2006.02.001

Rashtian, H., Boshmaf, Y., Jaferian, P., & Beznosov, K. (2014). To Befriend Or Not? A Model of Friend Request Acceptance on Facebook. In *Proceedings of the Tenth Symposium On Usable Privacy and Security* (pp. 285–300).

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social network security: Issues,

challenges, threats, and solutions. *Information Sciences*, *421*, 43–69. https://doi.org/10.1016/j.ins.2017.08.063

Rathore, S., Sharma, P. K., & Park, J. H. (2017). XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs. *Journal of Information Processing Systems*, *13*(4), 1014–1028. https://doi.org/10.3745/JIPS.03.0079

Razali, N. M., & Wah, Y. B. (2011). Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests. *Journal of Statistical Modeling and Analytics*, *2*(1), 21–33.

Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018). An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (pp. 1–13). New York, USA: ACM Press. https://doi.org/10.1145/3173574.3174086

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly*, *36*(1). Retrieved from https://ssrn.com/abstract=2176426

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 93–114.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, *25*(2), 578–586. https://doi.org/10.1016/j.chb.2008.12.024

Rungtusanatham, M., Wallin, C., & Eckerd, S. (2011). The Vignette in a Scenario-Based Role-Playing Experiment. *Journal of Supply Chain Management*, *47*(3), 9–16. https://doi.org/10.1111/j.1745-493X.2011.03232.x

Sahoo, S. R., & Gupta, B. B. (2019). Classification of various attacks and their defence mechanism in online social networks: a survey. *Enterprise Information Systems*, *13*(6), 832–864. https://doi.org/10.1080/17517575.2019.1605542

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Saunders, M., Lewis, P., & Thornhill., A. (2016). *Research Methods for Business Students* (7th ed.).

Pearson education.

Schriesheim, C. a., & Hinkin, T. R. (1990). Influence tactics used by subordinates: A theoretical and empirical analysis and refinement of the Kipnis, Schmidt, and Wilkinson subscales. *Journal of Applied Psychology*, *75*(3), 246–257. https://doi.org/10.1037/0021-9010.75.3.246

Schriesheim, C. A., Powers, K. J., Scandura, T. A., Gardiner, C. C., & Lankau, M. J. (1993). Improving Construct Measurement In Management Research: Comments and a Quantitative Approach for Assessing the Theoretical Content Adequacy of Paper-and-Pencil Survey-Type Instruments. *Journal of Management*, *19*(2), 385–417. https://doi.org/10.1177/014920639301900208

Seidman, G. (2013). Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and Individual Differences*, *54*(3), 402–407. https://doi.org/10.1016/j.paid.2012.10.009

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill building approach*. John Wiley & Sons.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10* (pp. 373–382). New York, USA: ACM Press. https://doi.org/10.1145/1753326.1753383

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys*, *45*(4), 1–33. https://doi.org/10.1145/2501654.2501661

Shindarev, N., Bagretsov, G., Abramov, M., Tulupyeva, T., & Suvorova, A. (2018). Approach to Identifying of Employees Profiles in Websites of Social Networks Aimed to Analyze Social Engineering Vulnerabilities. In A. Abraham, S. Kovalev, V. Tarassov, V. Snasel, M. Vasileva, & A. Sukhanov (Eds.), *Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17)* (pp. 441–447). Springer International Publishing. https://doi.org/10.1007/978-3-319-68321-8_45

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, *65*, 14–28. https://doi.org/10.1016/j.cose.2016.09.009

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Soper, D. (2012). A-priori sample size calculator. Retrieved from https://www.danielsoper.com/statcalc/calculator.aspx?id=1

Sophos. (2011). *Security Threat Report*. Retrieved from http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-2011-wpna.pdf

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503–522. Retrieved from http://www.jstor.org/stable/25750689

Statista. (2018). Leading global social networks 2018 | Statistic. Retrieved May 10, 2018, from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Statista. (2019). Number of Facebook users in Saudi Arabia from 2015 to 2023 (in millions). Retrieved May 10, 2018, from https://www.statista.com/statistics/558237/number-of-facebook-users-in-saudi-arabia/

Stern, A. (2014). Social Networkers Beware: Facebook is a Major Phishing Portal – Kaspersky Lab official blog. Retrieved March 8, 2018, from https://www.kaspersky.com/blog/1-in-5-phishing-attacks-targets-facebook/5180/

Stevens, J. P. (2009). *Applied Multivariate Statistics for the Social Sciences* (Fifth Edit). New York: Routledge.

Such, J. M., & Rovatsos, M. (2016). Privacy Policy Negotiation in Social Media. *ACM Transactions on Autonomous and Adaptive Systems*, *11*(1), 1–29. https://doi.org/10.1145/2821512

Tabachnick, B. G., & Fidel, L. S. (2013). *Using Multivariate Statistics* (6th editio). Boston: Pearson.

Tambe Ebot, A. (2018). Using stage theorizing to make anti-phishing recommendations more effective. *Information and Computer Security*, *26*(4), 401–419. https://doi.org/10.1108/ICS-06-2017-0040

Taormina, R. J., & Sun, R. (2015). Antecedents and Outcomes of Psychological Insecurity and Interpersonal Trust Among Chinese People. *Psychological Thought, 8 (2)*(2015), 173–188. https://doi.org/10.5964/psyct.v8i2.143

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014–1023. https://doi.org/10.1080/0144929X.2013.763860

Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. (2013). How bad is it?–a branching activity model to estimate the impact of information security breaches. In *12th Workshop on the Economics of Information Security* (pp. 1–47).

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European Data Protection Law* (Vol. 20, pp. 333–365). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14

Tsai, T.-H., Chang, H.-T., Chang, Y.-C., & Chang, Y.-S. (2017). Personality disclosure on social network sites: An empirical examination of differences in Facebook usage behavior, profile contents and privacy settings. *Computers in Human Behavior*, *76*, 469–482. https://doi.org/10.1016/j.chb.2017.08.003

Tsikerdekis, M., & Zeadally, S. (2014). Online deception in social media. *Communications of the ACM*, *57*(9), 72–80. https://doi.org/10.1145/2629612

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24–30). IEEE. https://doi.org/10.1109/STAST.2014.12

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Vision 2030. (2016). *KSA Vision 2030: Strategic Objectives and Vision Realization Programs*. Retrieved from https://vision2030.gov.sa/sites/default/files/vision/Vision Realization Programs Overview.pdf

Viswanath, B., Post, A., Gummadi, K. P., & Mislove, A. (2010). An analysis of social network-based Sybil defenses. In *Proceedings of the ACM SIGCOMM 2010 conference* (p. 363). New York, USA: ACM Press. https://doi.org/10.1145/1851182.1851226

Wang, J.-L., Jackson, L. A., Wang, H.-Z., & Gaskin, J. (2015). Predicting Social Networking Site (SNS) use: Personality, attitudes, motivation and Internet self-efficacy. *Personality and Individual Differences*, *80*, 119–124. https://doi.org/10.1016/j.paid.2015.02.016

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE*

Transactions on Professional Communication, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

Wang, J., Li, Y., & Rao, H. R. (2017). Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. *Information Systems Research*, *28*(2), 378–396. https://doi.org/10.1287/isre.2016.0680

Weiss, N. E., & Miller, R. S. (2015). The Target and Other Financial Data Breaches: Frequently Asked Questions. *Congressional Research Service*, *4*, 1–38.

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. *MIS Quarterly*, *33*(1), 177–195. Retrieved from https://www.jstor.org/stable/20650284

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Winter, J. C. F. De, & Dodou, D. (2010). Five-Point Likert Items : t test versus Mann-Whitney-Wilcoxon. *Practical Assessment, Research & Evaluation*, *15*(11), 1–12.

Wishart, R., Corapi, D., Marinovic, S., & Sloman, M. (2010). Collaborative Privacy Policy Authoring in a Social Networking Context. In *2010 IEEE International Symposium on Policies for Distributed Systems and Networks* (pp. 1–8). IEEE. https://doi.org/10.1109/POLICY.2010.13

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, *98*, 95–108. https://doi.org/10.1016/j.ijhcs.2016.09.006

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(6), 315–331. https://doi.org/10.1080/10658980701788165

Workman, M. (2008a). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463–483. https://doi.org/10.1108/09685220810920549

Workman, M. (2008b). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27*(1),

273–303. https://doi.org/10.2753/MIS0742-1222270111

Yahya, F., Walters, R. J., & Wills, G. B. (2016). Goal-based security components for cloud storage security framework: a preliminary study. In *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)* (pp. 1–5). IEEE. https://doi.org/10.1109/CyberSecPODS.2016.7502338

Yang, C., Harkreader, R., Zhang, J., Shin, S., & Gu, G. (2012). Analyzing spammers' social networks for fun and profit. In *Proceedings of the 21st international conference on World Wide Web - WWW '12* (pp. 71–80). New York, USA: ACM Press. https://doi.org/10.1145/2187836.2187847

Yang, H.-L., & Lin, C.-L. (2014). Why do people stick to Facebook web site? A value theory-based view. *Information Technology & People*, *27*(1), 21–37. https://doi.org/10.1108/ITP-11-2012-0130

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017). Use of Phishing Training to Improve Security Warning Compliance. In *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp on - HoTSoS* (pp. 52–61). New York, USA: ACM Press. https://doi.org/10.1145/3055305.3055310

Yao, G., Wu, C., & Yang, C. (2007). Examining the content validity of the WHOQOL-BREF from respondents' perspective by quantitative methods. *Social Indicators Research*, *85*(3), 483–498. https://doi.org/10.1007/s11205-007-9112-8

Yi, Z. (2018). Market Segmentation, Targeting, and Positioning. In *Marketing Services and Resources in Information Organizations* (pp. 39–48). Elsevier. https://doi.org/10.1016/B978-0-08-100798-3.00004-0

Yu, D., Chen, N., Jiang, F., Fu, B., & Qin, A. (2017). Constrained NMF-based semi-supervised learning for social media spammer detection. *Knowledge-Based Systems*, *125*, 64–73. https://doi.org/10.1016/j.knosys.2017.03.025

Zhang, K. Z. K., Zhao, S. J., Cheung, C. M. K., & Lee, M. K. O. (2014). Examining the influence of online reviews on consumers' decision-making: A heuristic–systematic model. *Decision Support Systems*, *67*, 78–89. https://doi.org/10.1016/j.dss.2014.08.005

Zhang, Z. (2016). Missing data imputation: focusing on single imputation. *Annals of Translational Medicine*, *4*(1), 9. https://doi.org/10.3978/j.issn.2305-5839.2015.12.38

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *Journal of Consumer Research*, *37*(2), 197–206. https://doi.org/10.1086/651257

Zheng, X., Zeng, Z., Chen, Z., Yu, Y., & Rong, C. (2015). Detecting spammers on social networks. *Neurocomputing*, *159*(1), 27–34. https://doi.org/10.1016/j.neucom.2015.02.047

Zolait, A. H. S., Anizi, R. R. Al, Ababneh, S., BuAsalli, F., & Butaiba, N. (2014). User awareness of social media security: the public sector framework. *International Journal of Business Information Systems*, *17*(3), 261–282. https://doi.org/10.1504/IJBIS.2014.064973

APPENDICES

Appendix A. Experts' Review Evaluation Survey

User-Centric Framework Evaluation Survey

Thank you for participating in this survey. As an information security expert, you have been invited to participate in validating the proposed User-Centric Framework due to your knowledge and experience in information security field. I appreciate your time and valuable feedback. Your participation in this study is voluntary and you are free to withdraw your participation from this study if required. It should only take 10-15 minutes to complete the survey.

This research aims to investigate the user characteristics that influence users' vulnerability to social engineering-based attacks in social networks. This survey has been approved by Departmental Ethics Committee of Strathclyde University. There are no risks associated with participating in this study. The survey collects no identifying information of any respondent. All responses in the survey will be recorded anonymously.

By completing and submitting this survey, you are indicating your consent to participate in the study. If you have any further concerns regarding your participation in this study or any other questions, please don't hesitate to contact the researcher by email.

Your participation is highly appreciated,

Researcher Contact Details:
Samar Albladi
Computer and information sciences department
University of Strathclyde
Email: samar.albladi@strath.ac.uk

Supervisor Contact Details:
Dr. George Weir
Computer and information sciences department
University of Strathclyde
Email: george.weir@strath.ac.uk

Demographics

Q1: What is your age?

□ <18	□ 18 – 24	□ 25-34	□ 35-44	□ 45-55	□ >55

Q2: What is your gender?

□ Male	□ Female

Q3: What is your nationality?

□ Saudi	□ UK	□ Other (please specify) ……

Q4: What is your last education degree?

□ High school	□ Bachelor's degree	□ Master's degree	□ PhD degree	□ Other (please specify) ……...

Q5: How long have you been specialising in information security field?

□ 1-5 years	□ 6-10 years	□ 11-15 years	□ Over 15 years

Framework Evaluation

The proposed User-Centric Framework in Figure 1 includes 4 perspectives: socio-psychological, perceptual, habitual, and socio-emotional. Each perspective includes number of factors that might have an impact on users' vulnerability to social engineering attacks in social networks. Based on the given framework, Answer the following questions:

User characteristics			
Socio-Psychological	**Perceptual**	**Habitual**	**Socio-Emotional**
a. Personality traits b. User's demographics: age, gender, education, computer knowledge c. Culture	a. Perceived risk of social network activities b. Past experience with social engineering c. Perceived severity of threat d. Perceived likelihood of threat e. Privacy awareness f. Security awareness g. Self-efficacy	a.Level of involvement: users can be classified as high or less active users based on many variables, for instance, number of friends and frequency of use	a. Trusting social network provider b. Trusting social network members c. Motivation to use social networks
Vulnerability Level: High or Low			

Figure 1 User-Centric Framework (UCF)

Q6: Can you please read carefully the factors definitions given in the table below, then rate the importance of each factor of the Framework in terms of its effect on users' poor judgements of social engineering attacks in social networks? *From (1) Not Important to (5) Very Important.*

The Factors	Not Important (1)	Slightly Important (2)	Moderately Important (3)	Important (4)	Very Important (5)
Socio-psychological Perspective					
1. The individual's personality trait: User behaviour can be patterned and categorised into five different traits which are: neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness. Those traits can determine the individual's personality.					
2. The individual's age					
3. The individual's gender					
4. The individual's education level					
5. The individual's height					
6. The individual's computer knowledge: The level of the individual's expertise in using computers.					
7. The individual's culture: The individual's nationality and language.					
Habitual Perspective					
8. Number of friends: The number of friends that the individual user is connected with on their social network account.					
9. Frequency of using social network: The number of days per week and the number of hours per day that the individual usually spends visiting their own social network account.					
Perceptual Perspective					
10. Perceived risk of social networks: The extent to which the user is uncertain whether an online action is worthwhile or not.					
11. Past experience with social engineering: Has the individual previously faced or fallen victim for any kind of social engineering attacks such as identity theft, phishing...etc.					
12. Perceived severity of threats: The individual's perception of the severity of threats that might be occurred in social networks and the negative consequences of those threats.					
13. Perceived likelihood of threats: The individual's perception of the likelihood of threats occurrence and the possibility of falling victim to social engineering attacks in social networks.					
14. Privacy awareness: The individuals' awareness of actions and behaviour required to protect their personal information online.					
15. Security awareness: The individuals' awareness of actions and behaviour to protect themselves from online security threats.					
16. Self-efficacy: The individuals' confidence in their ability to protect themselves from any online undesirable incidence.					
Socio-emotional Perspective					
17. Trusting social network provider: The extent to which the individual trusts and relies on the social network's service provider to protect their personal information.					
18. Trusting social network members: The extent to which the individual believes that other social network members are trustworthy and not harmful.					
19. Motivation to use social networks: The motivation that causes the individual to engage more in social networks.					

Qualitative Part (Open-ended Questions)

Q7: From your experience, are there any factors in the framework that should be combined?

Q8: From your experience, is there any factor in the framework that should be split?

Q9: From your experience, do you think there are any other factors that should be included in the framework?

The End,

Appendix B. Experts' Evaluation Ethical Approval

CIS Ethics Approval System

You are Samar Albladi (Research Student - 201561781)

Title of research:
Vulnerability to Social engineering in social network: User-centric based framework

Summary of research (short overview of the background and aims of this study):

The present research aims to design a user-centric framework that illustrates the factors that influence user vulnerability to social engineering-based attacks in social networks.

How will participants be recruited?
Participants will be contacted directly via email or personal contact.

What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee. PDF File: None.

a. Participants will be asked to give their permission to include their data in the study.
b. Participants will receive a participation request by email that include an online questionnaire-based survey.
c. Participants will be informed that their participation is voluntary.

How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. It is particularly important that you make the rights of the participants to freely withdraw from the study at any point (if they begin to feel stressed for example), nor feel under any pressure or obligation to complete the study, answer any particular question, or undertake any particular task. Their rights regarding associated data collected should also be made explicit.
PDF File: None.
The first page of the survey will include the consent details which will make it clear for participants that:

a. Their participation will be completely anonymous and confidential.
b. Their participation is voluntary, and if they begin the study, they can quit whenever they wish.
c. The survey questions should not cause any pain or discomfort.

What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out. Please also confirm (where appropriate) that your supervisor has seen and approved both your planned study and this associated ethics application. PDF File: None. PDF File: None.

a. Participants will be told that by completing and submitting this survey, they are indicating their consent to participate in the study.
b. Participants will be asked to answer some demographic questions and some other questions related to users' online behavior and perception.
c. Completing the survey will take about 10 to 15 minutes.

What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.

a. The researcher will abide by the provisions of the Data Protection Regulation (GDPR).
b. Data and results of this survey will only be used in the present study.
c. The data will be processed and analysed fairly, with limited purposes, and not kept longer than necessary.

How will the data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to describing how personal or sensitive data will be handled and how GDPR regulations will be met.

a. The data will be analysed and processed based on the research focus.
b. The data will be compared with other sources such as related articles, and other empirical studies results. This comparison will support the reliability of the present study.

How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed.
PDF File: None.

a. The collected data will be seen only by the researcher and the research supervisor and will not include any information that could identify any individual participant.
b. Data will be stored for a maximum of one year after the conclusion of the researcher's present study degree.
c. All data will be stored in a secure PGR database that can be accessed only by the authenticated researcher.

Appendix C. Experts' Review (Nonparametric Test Results)

Table C.1 Descriptive Statistics

Group No.		Per_T	Age	Gender	Education	Comp_K	Culture	Num_Con	Frq_use	Risk	Severity	Likelihood	Sec_aware	Priv_aware	Self_efficacy	CCEXP	TrustP	TrustM	Motiv
1	N	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
Mean		4.143	4.143	3.143	4.571	4.500	4.143	3.642	3.642	4.000	3.429	3.642	4.429	4.071	3.643	4.071	3.929	4.071	3.571
Mode		5.00	5.00	3.00	5.00	5.00	4.00	3.00[a]	3.00[a]	5.00	4.00	3.00[a]	5.00	5.00	4.00	5.00	5.00	4.00	4.00
2	N	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
Mean		3.750	3.500	3.083	3.833	4.333	3.250	3.417	3.917	4.000	3.750	3.500	4.583	4.333	3.917	4.000	4.167	4.333	3.333
Mode		4.00	4.00	3.00[a]	4.00	5.00	4.00	3.00	5.00	4.00	5.00	2.00[a]	5.00	5.00	4.00	5.00	5.00	5.00	3.00

a. Multiple modes exist. The smallest value is shown

Table C.2 Mann-Whitney Independent Samples Test (Gender)

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Per_T is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	1.000[1]	Retain the null hypothesis.
2	The distribution of Age is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.634[1]	Retain the null hypothesis.
3	The distribution of Gender is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.711[1]	Retain the null hypothesis.
4	The distribution of Education is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.525[1]	Retain the null hypothesis.
5	The distribution of Comp_K is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.339[1]	Retain the null hypothesis.
6	The distribution of Culture is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.792[1]	Retain the null hypothesis.
7	The distribution of Num_Con is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.039[1]	Reject the null hypothesis.
8	The distribution of Frq_use is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.002[1]	Reject the null hypothesis.
9	The distribution of Risk is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.200[1]	Retain the null hypothesis.
10	The distribution of Severity is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.133[1]	Retain the null hypothesis.
11	The distribution of Likelihood is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.560[1]	Retain the null hypothesis.
12	The distribution of Sec_aware is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.874[1]	Retain the null hypothesis.
13	The distribution of Priv_aware is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.634[1]	Retain the null hypothesis.
14	The distribution of Self_efficacy is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.200[1]	Retain the null hypothesis.
15	The distribution of CCEXP is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.525[1]	Retain the null hypothesis.
16	The distribution of TrustP is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.107[1]	Retain the null hypothesis.
17	The distribution of TrustM is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.107[1]	Retain the null hypothesis.
18	The distribution of Motivation is the same across categories of Part_gender.	Independent-Samples Mann-Whitney U Test	.120[1]	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

[1] Exact significance is displayed for this test.

Table C.3 Mann-Whitney Independent Samples Test (Culture)

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Per_T is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.145[1]	Retain the null hypothesis.
2	The distribution of Age is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.193[1]	Retain the null hypothesis.
3	The distribution of Gender is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.980[1]	Retain the null hypothesis.
4	The distribution of Education is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.046[1]	Reject the null hypothesis.
5	The distribution of Comp_K is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.899[1]	Retain the null hypothesis.
6	The distribution of Culture is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.095[1]	Retain the null hypothesis.
7	The distribution of Num_Con is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.781[1]	Retain the null hypothesis.
8	The distribution of Frq_use is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.374[1]	Retain the null hypothesis.
9	The distribution of Risk is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	1.000[1]	Retain the null hypothesis.
10	The distribution of Severity is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.462[1]	Retain the null hypothesis.
11	The distribution of Likelihood is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.705[1]	Retain the null hypothesis.
12	The distribution of Sec_aware is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.667[1]	Retain the null hypothesis.
13	The distribution of Priv_aware is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.667[1]	Retain the null hypothesis.
14	The distribution of Self_efficacy is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.527[1]	Retain the null hypothesis.
15	The distribution of CCEXP is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.940[1]	Retain the null hypothesis.
16	The distribution of TrustP is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.631[1]	Retain the null hypothesis.
17	The distribution of TrustM is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.432[1]	Retain the null hypothesis.
18	The distribution of Motivation is the same across categories of Group_No.	Independent-Samples Mann-Whitney U Test	.494[1]	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

[1] Exact significance is displayed for this test.

Appendix D. Content Validity Survey

This survey is part of an ongoing research at Strathclyde University that investigates the users' characteristics that affect their perception and judgement of social networks security threats. This assessment aims to evaluate the measurement scales items that will be used to measure our study factors in order to assess the feasibility of the selected items. You will be asked to read the factors definitions carefully first and then; you can start reading each item in the provided measurement scales and based on your judgement assign each item to the factor that the item best indicates or measures. This assessment survey should only take 15 minutes to complete.

All responses will be confidential and anonymous. Only the researchers can access the survey result which includes no information that could identify you. The data will be only used for this study. After completing the study, the data will not be stored more than necessary and will be disposed of immediately after the conclusion of the researcher's present study degree. Participating in this study is voluntary but will highly contribute to this research field. There are no harm or risk associated with participating in this study. However, you have the right to withdraw from this study at any time if you feel uncomfortable. Please consider that after submitting the response, it could be hard to identify the participant response, as no identifiable information will be collected. The survey questions should not cause any discomfort. Yet, you have the right not to answer any question that you may feel uncomfortable with. The collected hard copy records will be stored in a locked cabinet, within a locked office, accessed only by the researcher. Electronic data will be stored on Strathclyde university secure network space with password protected files.

This survey has been approved by the ethics committee of the Department of Computer and Information Sciences at Strathclyde University. By completing and submitting this survey, you are indicating your consent to participate in the study. Please note: after completing this survey, please submit it to the researcher either by hand or send it back to the researcher email. If you have any concerns regarding your participation in this study or any other queries, please don't hesitate to contact the researchers or The Departmental Ethics Committee by email.

Your participation is highly appreciated,
Contact Details:

Samar Albladi (Researcher)
Livingstone tower, office: LT1206
Computer and information sciences department
University of Strathclyde
Email: samar.albladi@strath.ac.uk

Dr. George Weir (Research Supervisor)
Computer and information sciences department
University of Strathclyde
Email: george.weir@strath.ac.uk

The Departmental Ethics Committee
Email: enquiries@cis.strath.ac.uk

Instrument Content Validity Assessment

Q1. What is your age?	☐	18 – 24	☐	25-34	☐	35-44	☐	45-55	☐	>55
Q2. What is your gender?	☐	Male			☐	Female				
Q3. What is your nationality?	☐	UK	☐	Saudi	☐	Other (please specify) ……..……				
Q4. What is your last education degree?	☐	Bachelor's degree	☐	Master's degree	☐	PhD degree	☐	Other (please specify) ……. ….		
Q5. Which field of study are you interested in?	……									

Q6. Please read carefully the constructs definitions given in table 1. Then, can you please read each item (rows) in table 2 and based on your judgement assign each item to the construct (columns) that the item best indicates or measures. Follow the following instructions:

1. **If you feel the statement describes ONLY ONE construct, place a tick (√) in the appropriate column.**
2. **If you feel the statement describes MORE THAN ONE construct, place a (1) in the column that you feel BEST describes it, a (2) in the column that NEXT BEST describes it, and so on, as you wish.**

Table 1. Constructs Definitions

Construct	Definition
Self-efficacy	The individuals' confidence in their ability to protect themselves from any undesirable online incidence.
Privacy Awareness	The individuals' awareness of actions and behaviour required to protect their personal information online.
Security Awareness	The individuals' awareness of actions and behaviour to protect themselves from online security threats.
Perceived Severity of Threat	The individual's perception of the severity of threats that might be occurred in social networks (SN) and the negative consequences of those threats.
Perceived Likelihood of Threat	The individual's perception of the likelihood of threats occurrence and the possibility of falling victim to social engineering attacks in social networks.
Experience with Cybercrime	Has the individual previously faced or fallen victim for any kind of social engineering attacks such as identity theft, phishing...etc.

Table 2. Content Validation Matrix (Perceptual)

Items	Self-efficacy	Privacy Awareness	Security Awareness	Perceived Severity of Threat	Perceived Likelihood of Threat	Experience with Cybercrime
1. Has the individual ever experienced somebody stealing their personal data and impersonating them, e.g. shopping under their name, open SN account in their name.						
2. The individual believes that losing financial information while using Facebook would be harmful for them.						
3. Has the individual ever experienced online fraud where goods purchased were not delivered, counterfeit or not as advertised.						
4. The individual does not use third party apps (apps that offer new features that are not available in the official version) to access their social networks accounts.						
5. The individual believes that having strangers eavesdropping on their Facebook account would be a severe problem for them.						
6. The individual is confident that they can avoid any hazards while using Facebook.						
7. The individual believes that having their messages and chats seen or listened to in Facebook would be a severe problem for them.						
8. Has the individual ever received emails fraudulently asking for money or personal details (including banking or payment information).						
9. The individual usually reports any malicious accounts to SN provider.						
10. The individual believes that having their identity stolen in Facebook would be a severe problem for them.						
11. The individual's opinion about how likely it is for one's financial information to be stolen in Facebook.						
12. The individual believes that losing their data privacy while using Facebook would be a severe problem for them.						
13. The individual's opinion about how likely it is that one's identity can be stolen in Facebook.						
14. The individual is skilled at avoiding dangers while using Facebook.						
15. The individual has the knowledge and the ability to secure their Facebook account by adjusting the account settings.						
16. The individual has the ability to protect themselves from any online threats while using Facebook.						

Items	Self-efficacy	Privacy Awareness	Security Awareness	Perceived Severity of Threat	Perceived Likelihood of Threat	Experience with Cybercrime
17. The individual reviewed the SN privacy policy and they know how to configure it.						
18. The individual restricts access to their account by adjusting the privacy setting.						
19. The individual's opinion about how likely it is for one's privacy to be invaded without their knowledge while using Facebook.						
20. The individual's opinion about how likely it is for one's personal information to be secure while using Facebook.						
21. The individual uses password for their SN account different from the passwords they use to access other sites.						
22. On Facebook, the individual does not feel safe regarding their personal data, who can contact them, and the exchange of thoughts and feelings.						
23. The individual uses a specific new email for their SN account different from their personal or work email.						
24. The individual updates their password on a regular basis.						
25. Has the individual ever received harassing messages, inappropriate comments, or other persistent behaviour that endanger their safety?						
26. The individual does not share personal information in SN such as birthdate, phone number, workplace, or address.						
27. The individual does not share their current or future location in SN, for example, images for their current vacation, or plans for future vacation.						
28. The individual does not use similar usernames for different social media accounts.						
29. The individual always reads and pays attention to the security warning messages on Facebook.						

Q7. Can you please list the numbers of the above statements that you found unclear? Write down any concept or term that you read in the above statements that you think need more clarification?

Q8. Please read carefully the constructs definitions given in table 3. Then, can you please read each item (rows) in table 4 and based on your judgement assign each item to the construct (columns) that the item best indicates or measures. Follow the following instructions:

1. **If you feel the statement describes ONLY ONE construct, place a tick (√) in the appropriate column.**
2. **If you feel the statement describes MORE THAN ONE construct, place a (1) in the column that you feel BEST describes it, a (2) in the column that NEXT BEST describes it, and so on, as you wish.**

Table 3. Constructs Definitions

Construct	Definition
Level of Involvement	The extent to which a user engages in social network activities.
Social Motivation	The extent to which social network mediums are perceived to improve the relationship and the impression of friends and family.
Information Motivation	The extent to which social network mediums are perceived to satisfy the desire of expression and information seeking and sharing.
Hedonic Motivation	The extent to which participating in social network mediums is considered enjoyable and pleasurable.
Trust in Provider	The extent to which the individual trusts and relies on the social network's service provider to protect their personal information.
Trust in Members	The extent to which the individual believes that other social network members are trustworthy and not harmful.

Table 4. Content Validation Matrix (Habitual and Socio-emotional)

Items	Level of Involvement	Social Motivation	Information Motivation	Hedonic Motivation	Trust in Provider	Trust in Members
1. The individual believes that Facebook members will always keep the promises they make to one another.						
2. How often does the individual comment on other people's status update or pictures?						
3. The individual uses Facebook to express and share their opinion freely.						
4. The individual enjoys using the wide range of applications in Facebook such as games.						
5. Approximately how many ''friends" does the individual have on their account?						
6. The individual believes that Facebook can be relied on to keep its promises and commitment to its members.						
7. The individual believes that using social networks makes a good impression on other people.						

Items	Level of Involvement	Social Motivation	Information Motivation	Hedonic Motivation	Trust in Provider	Trust in Members
8. The individual believes that Facebook members will not misuse the information they found about them in their account.						
9. The individual can count on Facebook to protect their personal information from unauthorised use.						
10. On a typical day, how many minutes does the individual spend on Facebook?						
11. The individual believes that Facebook is a trustworthy social network.						
12. The individual uses Facebook to share information, photos, or videos with others.						
13. The individual uses Facebook to maintain their popularity and prestige among peers.						
14. The individual uses Facebook to keep in touch with friends and family.						
15. The individual believes that using social networks is enjoyable and entertaining.						
16. The individual believes that Facebook members will not take advantage of others even when the opportunity arises.						
17. The individual can count on Facebook to protect their privacy.						
18. The individual believes that Facebook members are truthful in dealing with one another.						
19. The individual uses Facebook to pass the time.						
20. The individual uses Facebook out of curiosity, they want to know what their friends and other people are doing in Facebook.						
21. The individual uses Facebook to stay up to date with news and current events.						
22. The individual uses Facebook to connect with and meet new people with similar interests.						
23. The individual could obtain useful information from Facebook.						

Q9. Can you please list the numbers of the statements that you found unclear? Write down any concept or term that you read in the above statements that you think need more clarification?

The End

Appendix E. Content Validity Assessment Ethical Approval

CIS Ethics Approval System
You are Samar Albladi (Research Student - 201561781)

Title of research:

Vulnerability to Social Engineering in Social Networks- Content Validity Test

Summary of research (short overview of the background and aims of this study):

This survey is part of an ongoing research that investigates the users' characteristics that affect their susceptibility to social engineering-based attacks in social networks. This content validity test aims to evaluate the measurement scales items that will be used to measure our study factors in order to assess the feasibility of the selected items. Participants will be asked to complete a short survey, which consists of three parts. The first part is asking about some demographic factors such as age, gender, and field of study. The second part includes two validation matrixes which include measurements scales items of various constructs. Participants will be asked to judge and align each item in the matrixes with its relevant constructs. In the third part, participants will be asked to list the numbers of any statements that they found unclear and to write down any concept or term that they read in the statements that they think needs more clarification. The survey will be distributed to participants online via email or face to face as a printed version. The survey should only take 15 minutes to complete.

How will participants be recruited?

Limited number of participants (around 10 to 20 participants) is needed to conduct this content validity assessment. Thus, participants will be invited to participate in the study by two ways: First via email: Participants will be sent an invitation email first and will be asked if they would like to participate in this study. If participants reply with acceptance to participate, the survey will be emailed to them to complete and send back to the researcher. Second face to face: the researcher will approach participants as a group in a research meeting to invite them to participate in this study. Participants who indicate their willingness to take part will be given a hard copy of the survey. Participants' emails will be collected from the university website as the population is restricted to PhD students in computer and information science department. Participants would be invited to participate in this study if:

a. Their age is 18 or over.

b. They are PhD students in computer and information sciences department at Strathclyde University or Glasgow University.

What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee. PDF File: None.

a. Participants will be told that by completing and submitting this survey, they are indicating their consent to participate in the study.

b. Participants will be informed that their participation is voluntary and that there are no harm or risks associated with participation in this survey.

c. No information will be reported to anyone other than the researchers.

d. All responses will be confidential and anonymous.

e. Participants have the right to withdraw at any time before submitting their responses. Yet, after submitting the response, it would be hard to identify the participant response, as no identifiable information will be collected to identify a particular participant.

f. Participants have the right not to answer any question that they may feel uncomfortable with.

g. If participants have any concerns regarding their participation in this study or any other queries, they could contact the researchers or The Departmental Ethics Committee via email.

How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. PDF File: View document

The first page of the survey will include the consent details, which will make it clear for participants that:

a. Their participation will be completely anonymous and confidential.

b. Their participation is voluntary.

c. Participants have the right to withdraw at any time before submitting their responses. Yet, after submitting the response, it would be hard to identify the participant response, as no identifiable information will be collected.

d. The survey questions should not cause any discomfort. Yet, participants have the right not to answer any question that they may feel uncomfortable with.

e. Hard copy records will be stored in a locked cabinet, within locked office, accessed only by the researcher.

f. Electronic data will be stored on Strathclyde university secure network space with password protected files.

g. If participants have any concerns regarding their participation in this study or any other queries, they could contact the researchers or The Departmental Ethics Committee via email.

What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out. Please also confirm (where appropriate) that your supervisor has seen and approved both your planned study and this associated ethics application. PDF File: None.

Participates who will be approached face to face will be given a hard copy version of the survey and they should complete and return the survey to the researcher.

Participants who will be invited via email can complete the survey attached in the email and send it back to the researcher.

What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.

a. No sensitive personal or identifiable information will be collected.

b. The researcher will abide by the provisions of the General Data Protection Regulation (GDPR).

c. The data will be processed and analysed fairly, with limited purposes, and not kept longer than necessary.

d. Hard copy records will be stored in a locked cabinet, within locked office, accessed only by the researcher.

e. Electronic data will be stored on Strathclyde university secure network space with password protected files.

How will the data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to describing how personal or sensitive data will be handled.

a. The collected data will be used only for this investigation.

b. The data will be analysed and processed based on the research objectives, using statistical tools such as SPSS.

c. Access to data will be suitably secure and restricted to the researcher and the research supervisor.

d. Hard copy records will be stored in a locked cabinet, within locked office, accessed only by the researcher.

e. Electronic data will be stored on Strathclyde university secure network space with password protected files.

f. The data will be compared with other sources such as related articles and results from other studies. This comparison will support the reliability of the present study.

g. A report of the findings of this study might be published as a journal article or conference proceedings. The collected data will not include any information that could identify any individual participant.

How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed. PDF File: None.

a. Data will not be stored more than necessary and will be disposed of immediately after the conclusion of the researcher's present study degree.

b. When data no longer requires to be kept, it will be disposed of appropriately this will include:

- Confidential shredding of the collected hard copy surveys.
- Permanent deletion of electronic survey data.

Appendix F. Scenario-Based Experiment

Vulnerability to Social Engineering in Social Networks

Start of Block: Cover page

This research aims to investigate participants' behaviour and perception in online social networks. You will be asked to answer some questions about your habits and perceptions of different aspects of online social networks. The survey should approximately take 15 minutes to complete.

All responses will be confidential and anonymous. Only the researchers can access the questionnaire result which includes no information that could identify you. After completing the study, the data will be kept for a maximum of three years. Participating in this study is voluntary but will highly contribute to this research field. There are no harm or risk associated with participating in this study. However, you have the right to withdraw from this study at any time if you feel uncomfortable.

This survey has been approved by departmental ethics committee of Strathclyde University. By completing and submitting this survey, you are indicating your consent to participate in the study. Please note: if you have any concerns regarding your participation in this study or any other queries, please don't hesitate to contact the researcher by email.

Your participation is highly appreciated,

Researcher Contact Details:
Samar Albladi
Computer and information sciences department
University of Strathclyde
Email: samar.albladi@strath.ac.uk

Supervisor Contact Details:
Dr. George Weir
Computer and information sciences department
University of Strathclyde
Email: george.weir@strath.ac.uk

End of Block: Cover page

Start of Block: Demographic information

Q1. What is your age?

- 18-24
- 25-34
- 35-44
- 45-55
- More than 55

Q2. What is your gender?

- Male
- Female

Q3. What is your nationality?

- ${loc://CountryName}
- Other, please specify _____

Q4. What is your last education degree?

- High school
- Bachelor's degree
- Master's degree
- PhD
- Other, please specify _____

Q5. Your current status is:

- Student
- Employed
- Unemployed
- Retired

Q6. What is your major?

- Computer science/IT
- Engineering
- Business/ Administrative sciences
- Medical sciences
- Science
- Humanities and Arts
- Other, please specify _____

Q7. How well do the following statements describe your personality?

I see myself as someone who …

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
1. … is reserved (Per1_ExtR)	○	○	○	○	○
2.… is generally trusting (Per2_Agr)	○	○	○	○	○
3.… tends to be lazy (Per3_ConR)	○	○	○	○	○
4.… is relaxed, handles stress well (Per4_NeuR)	○	○	○	○	○
5.… has few artistic interests (Per5_OpeR)	○	○	○	○	○
6.… is outgoing, sociable (Per6_Ext)	○	○	○	○	○
7.… tends to find fault with others (Per7_AgrR)	○	○	○	○	○
8.… does a thorough job (Per8_Con)	○	○	○	○	○
9.… gets nervous easily (Per9_Neu)	○	○	○	○	○
10.… has an active imagination (Per10_Ope)	○	○	○	○	○

End of Block: Demographic information

Start of Block: Social Networks Habit

Q8. For how many years have you had your Facebook account?

- ○ Less than 1 year
- ○ 1-2 years
- ○ 3-4 years
- ○ 5-6 years
- ○ More than 6 years

Q9. How often do you comment on other people status update or pictures?

- ○ Always
- ○ Very Often
- ○ Sometimes
- ○ Rarely
- ○ Never

Q10. On a typical day, how many minutes do you spend on Facebook?

- ○ Less than 30 minutes
- ○ 30 minutes to 1 hour
- ○ 1-2 hours
- ○ 3-5 hours
- ○ 6 hours or more

Q11. Approximately how many ‘‘friends” do you have on your account?

_____

Q12. Estimate the percentage of your Facebook friends that you know personally?

- ○ 10% or less
- ○ 11%-30%
- ○ 31%-60%
- ○ 61%-90%
- ○ More than 90%

Q13. What are your main reasons of using social networks?

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
To keep in touch with friends and family (SM1)	○	○	○	○	○
To meet and connect with new people with similar interests (SM2)	○	○	○	○	○
To maintain my popularity and prestige among peers (SM3)	○	○	○	○	○
To pass the time (HM1)	○	○	○	○	○
Using social networks are enjoyable and entertaining (HM2)	○	○	○	○	○
They have a wide range of applications such as games, and I enjoy using them (HM3)	○	○	○	○	○
I could obtain useful information from them (IM1)	○	○	○	○	○
To stay up to date with current events and news (IM2)	○	○	○	○	○
I use them out of curiosity I want to know what my friends and other people are doing (IM3)	○	○	○	○	○

Q14. Please choose the best answer that indicates how much you agree with the following statements:

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
Facebook is a trustworthy social network (TP1)	○	○	○	○	○
I can count on Facebook to protect my privacy (TP2)	○	○	○	○	○
I can count on Facebook to protect my personal information from unauthorised use (TP3)	○	○	○	○	○
Facebook can be relied on to keep its promises and commitment to its members (TP4)	○	○	○	○	○
Facebook Members will not take advantage of others even when the opportunity arises (TM1)	○	○	○	○	○
Facebook Members will not misuse the information they found about me in my account (TM2)	○	○	○	○	○
Facebook Members are truthful in dealing with one another (TM3)	○	○	○	○	○
Facebook Members will always keep the promises they make to one another (TM4)	○	○	○	○	○

End of Block: Social Networks Habit

Start of Block: Social Networks Perception

Q15. Please choose the best answer in each statement that indicates the extent to which a statement is true for you:

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I am confident that I can avoid any hazards while using Facebook (SEF1)	○	○	○	○	○
I am skilled at avoiding dangers while using Facebook (SEF2)	○	○	○	○	○
I have the knowledge and the ability to secure my Facebook account by adjusting the account settings (SEF3)	○	○	○	○	○
I have the ability to protect myself from any online threats while using Facebook (SEF4)	○	○	○	○	○
I always read and pay attention to the security warning messages on Facebook (SA1)	○	○	○	○	○
I use password for my Facebook account different from the passwords I use to access other sites (SA2)	○	○	○	○	○
I update my account password on a regular basis (SA3)	○	○	○	○	○
I use a specific new email for my Facebook account different from my personal or work email (SA4)	○	○	○	○	○
I reviewed Facebook privacy policy and I know how to manage it (PA1)	○	○	○	○	○
I restrict access to my account by adjusting the privacy setting (PA2)	○	○	○	○	○
I don't share personal information on Facebook such as birthdate, phone number, workplace, or address (PA3)	○	○	○	○	○
I don't share my current or future location on Facebook for example, images for my current vacation, or plans for future vacation (PA4)	○	○	○	○	○
I believe that having my identity stolen in Facebook would be a severe problem for me (ST1)	○	○	○	○	○
I believe that losing my data privacy while using Facebook would be a severe problem for me (ST2)	○	○	○	○	○
I believe that having my messages and chats being seen or listened to in Facebook would be a severe problem for me (ST3)	○	○	○	○	○
I believe that losing my financial information while using Facebook would be harmful for me (ST4)	○	○	○	○	○

Q16. Answer the following questions according to your beliefs, attitudes, and experiences:

	Extremely Likely	Moderately Likely	Neither likely nor unlikely	Moderately Unlikely	Extremely Unlikely
How likely is it for your financial information to be stolen in Facebook? (LT1)	○	○	○	○	○
How likely is it that your identity can be stolen in Facebook? (LT2)	○	○	○	○	○
How likely is it for your privacy to be invaded without your knowledge while using Facebook? (LT3)	○	○	○	○	○
How likely is it for your personal information to be insecure while using Facebook? (LT4)	○	○	○	○	○

Q17. How often have you experienced or been a victim of the following incidents?

	Always	Very Often	Sometimes	Rarely	Never
Identity theft (somebody stealing your personal data and impersonating you, e.g. open SN account with your name, or shopping under your name) (PE1_It)	○	○	○	○	○
Phishing (received emails fraudulently asking for money or personal details, including banking or payment information) (PE2_Ph)	○	○	○	○	○
Online fraud where goods purchased were not delivered, counterfeit or not as advertised (PE3_OF)	○	○	○	○	○
Harassment, cyber-bullying (received harassing messages, inappropriate comments, or other persistent behaviour that endangers your safety) (PE4_Har)	○	○	○	○	○

End of Block: Social Networks Perception

Start of Block: Role-play Experiment

Q18. Pretend that you have seen the following six posts in your Facebook account. How much do you agree with the following statements?

1.

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this link (Attack_1a)	○	○	○	○	○
I would register my name and email to win (Attack_1b)	○	○	○	○	○

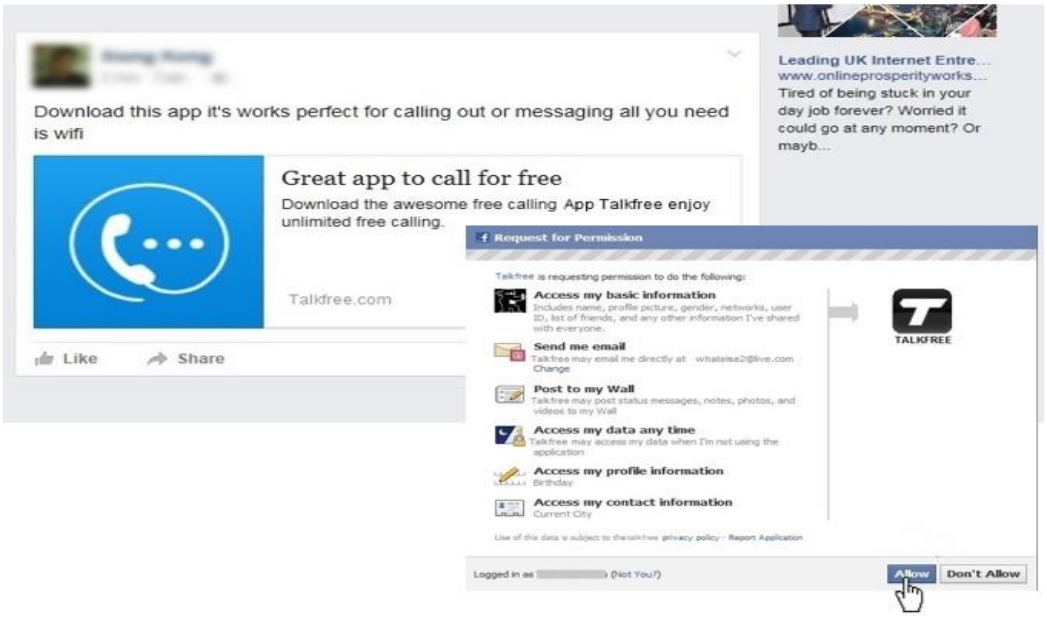
2.

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this button to read the file (Attack_2)	○	○	○	○	○

3.

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this video (Low_1)	○	○	○	○	○

4.

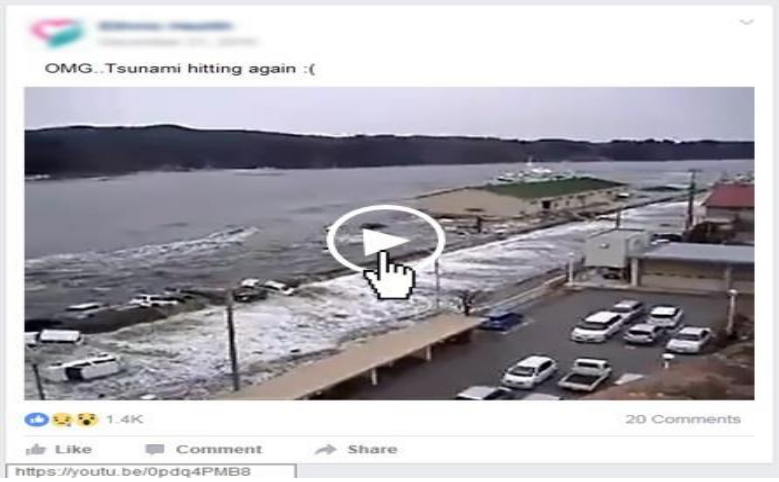


	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this button (Attack_3)	○	○	○	○	○

5.

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this link (Attack_4a)	○	○	○	○	○
I would confirm my account using this link (Attack_4b)	○	○	○	○	○

6.



	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree
I would click on this video (Low_2)	○	○	○	○	○

End of Block: Role-play Experiment

Appendix G. Scenario-Based Experiment Ethical Approval

CIS Ethics Approval System

You are Samar Albladi (Research Student - 201561781)

Title of research:

User's Vulnerability to Social Engineering in Social Networks- (Role-Play) Survey

Summary of research (short overview of the background and aims of this study):

Identifying the human factors that influence the human's ability to detect online security threats is a challenging problem in the information security field. This research aims to investigate the human weak points that influence their judgement of social engineering attacks in social networks. Therefore, the objective of this role-play quantitative survey is to measure the impact of various users' characteristics on social engineering victimisation in Facebook.

Participants will be asked to complete the survey by giving answers to some measurement scales related to online behaviour and perception. Additionally, participants will be presented with images of sample Facebook posts that include some famous social engineering attacks such as phishing, clickjacking, and malware. Participants will be asked how they would respond to these posts or requests if they saw them in their own profiles. The participants' responses to these role-play posts will help us to measure the participants' susceptibility to social engineering victimisation in Facebook. Completing this survey should only take 15 minutes of the participants' time. Participation in the present study has the benefit of shaping an important contribution in the research field.

How will participants be recruited?

Participants will be contacted and invited to participate in the study by the researcher or the person in authority via email or personal contact. Participants would be invited to participate in this survey if:

a. Their age is 18 or over.

b. They have an account in Facebook.

What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee. PDF File: None.

a. Participants will receive a participation request by email that include an online link to access the survey.

b. Participants will be informed that their participation is voluntary and that there are no risks associated with participation in this survey.

c. No information will be reported to anyone other than the researchers.

d. No personally identifying details will be recorded on the questionnaire.

How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. It is particularly important that you make the rights of the participants to freely withdraw from the study at any point (if they begin to feel stressed for example), nor feel under any pressure or obligation to complete the study, answer any particular question, or undertake any particular task. Their rights regarding associated data collected should also be made explicit. PDF File: None. The first page of the survey will include the consent details, which will make it clear for participants that:

a. Their participation will be completely anonymous and confidential.

b. Their participation is voluntary, and if they begin the study, they can withdraw before submitting their responses. Yet, after submitting the response, it would be hard to identify the participant response, as no identifiable information will be collected to identify a particular participant.

c. The survey questions should not cause any discomfort.

What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out. Please also confirm (where appropriate) that your supervisor has seen and approved both your planned study and this associated ethics application. PDF File: None. PDF File: None.

a. Participants will be told that by completing and submitting this survey, they are indicating their consent to participate in the study.

b. Participants will be asked to answer some demographic questions and some other questions related to their social networks' behaviour and perception.

c. Participants will be presented with images of sample Facebook posts and requests and will be asked how they would respond to these requests if they receive them in their own accounts.

d. Completing the survey should only take about 15 minutes.

What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.

a. The researcher will abide by the provisions of the General Data Protection Regulation (GDPR).

b. The data will be processed and analysed fairly, with limited purposes, and not kept longer than necessary.

c. Data will be stored on Strathclyde university secure network space with password protected files.

How will the data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to describing how personal or sensitive data will be handled and how GDPR regulations will be met.

a. The data will be analysed and processed based on the research focus.

b. The data will be compared with other sources such as related articles, and results from other empirical studies. This comparison will support the reliability of the present study.

c. A report of the findings of this study might be published as a journal article or conference proceedings. Yet, the collected data will not include any information that could identify any individual participant.

How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed. PDF File: None.

a. The collected data will be seen only by the researcher and the research supervisor.

b. Data will be stored for a maximum of three years after the conclusion of the researcher's present study degree.

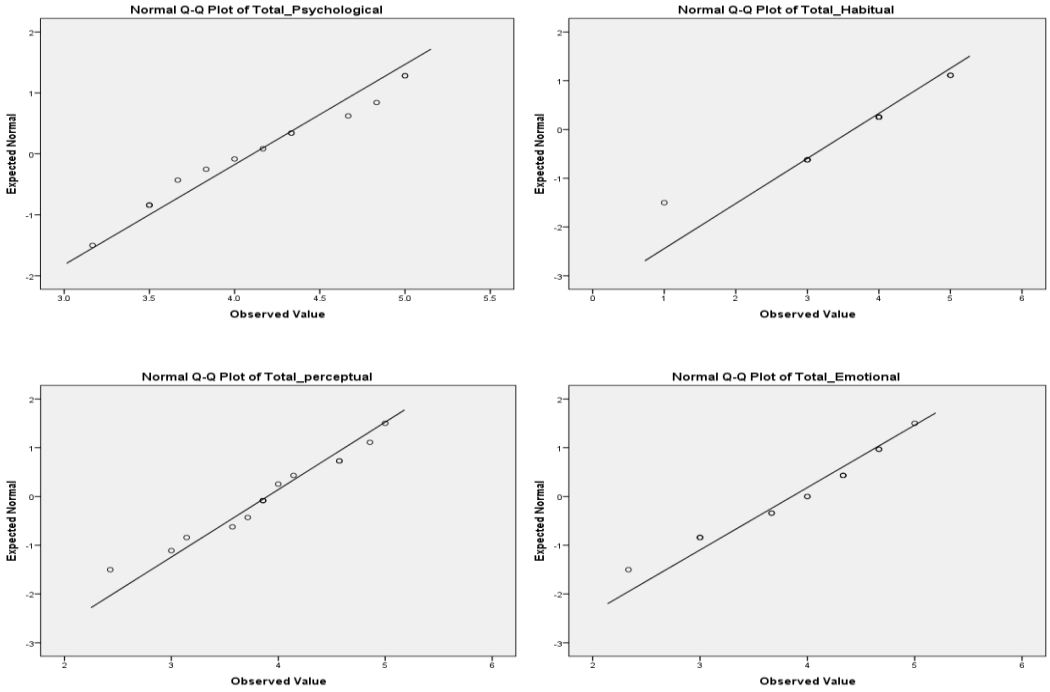
Appendix H. Scenario-Based Experiment (Pilot Test Results)

Table H.1 Pilot study reliability and factor analysis results

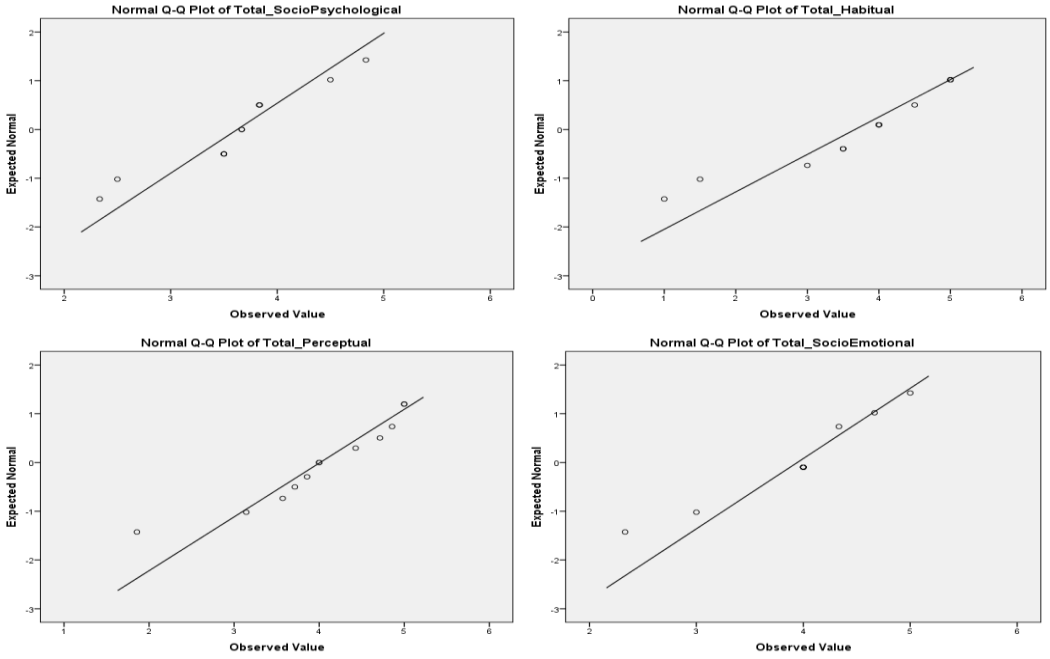
Factor	Item	Loading	Factor	Item	Loading
Involvement Cronbach's Alpha=.70	Freq_com	.793	Trust Provider Cronbach's Alpha=.945	TP1	.938
	Freq_min	.898		TP2	.745
Severity of threat Cronbach's Alpha=.947	ST1	.858		TP3	.709
	ST2	.943		TP4	.826
	ST3	.892	Trust Members Cronbach's Alpha=.938	TM1	.860
	ST4	.888		TM2	.932
Likelihood of threat Cronbach's Alpha=.886	LT1	.890		TM3	.896
	LT2	.883		TM4	.898
	LT3	.807	Social Motivation Cronbach's Alpha=.833	SM1	.924
	LT4	.766		SM2	.784
Security Awareness Cronbach's Alpha=.920	SA1	.607		SM3	.783
	SA2	.932	Hedonic Motivation Cronbach's Alpha=.854	HM1	.827
	SA3	.917		HM2	.706
	SA4	.902		HM3	.933
Privacy Awareness Cronbach's Alpha=.885	PA1	.721	Information Motivation Cronbach's Alpha=.820	IM1	.744
	PA2	.750		IM2	.797
	PA3	.813		IM3	.858
	PA4	.856	Susceptibility Cronbach's Alpha=.936	Attack_1a	.800
Self-efficacy Cronbach's Alpha=.890	SEF1	.785		Attack_1b	.806
	SEF2	.752		Attack_2	.744
	SEF3	.835		Attack_3	.779
	SEF4	.902		Attack_4a	.966
Cybercrime experience Cronbach's Alpha=.905	PE1_It	.879		Attack_4b	.968
	PE2_Ph	.894			
	PE3_OF	.879			
	PE4_Har	.849			

Appendix I. Experts' Review (Normality of Distribution Test)

First Round of Experts' Review



Second Round of Experts' Review



Appendix J. Initial Factor Analysis

Table J.1 Initial EFA (Perceptual Perspective)

Rotated Component Matrix[a]						
	Component					
	1	2	3	4	5	6
SEF1			.752			
SEF2			.778			
SEF3			.668			
SEF4	.318		.770			
SA1	.624					
SA2	.718					
SA3	.771					
SA4	.721					
PA1	.778					
PA2	.596					
PA3						.827
PA4						.837
PE1_It				.720		
PE3_OF				.806		
PE2_Ph				.780		
PE4_Har				.746		
LT1					.798	
LT2					.880	
LT3					.816	
LT4			.336			
ST1		.704				
ST2		.906				
ST3		.829				
ST4		.792				

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 6 iterations.

Table J.2 Initial EFA (Socio-Emotional Perspective)

Rotated Component Matrix[a]					
	Component				
	1	2	3	4	5
HM1			.808		
HM2			.766		.321
HM3		.436	.459		
IM1					.741
IM2					.839
IM3				.747	
SM1		.341		.636	
SM2			.495		
SM3				.806	
TP1	.452	.610			
TP2	.330	.845			
TP3	.346	.813			
TP4	.589	.596			
TM1	.777				
TM2	.787				
TM3	.861				
TM4	.861				

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Appendix K. Cross Loadings

	CCEXP	Hedonic	Involvement	Likelihood	Num_Con	Privacy	SNEXP	Security	Self-efficacy	Severity	Social	Susceptibility	TrustM	TrustP	KnownFR
Attack_1a	0.318	-0.018	0.364	0.071	0.003	-0.101	-0.279	0.028	-0.020	-0.086	0.298	**0.866**	0.148	0.402	-0.178
Attack_1b	0.334	0.046	0.270	0.057	-0.012	-0.129	-0.315	0.024	-0.033	-0.104	0.311	**0.839**	0.171	0.399	-0.184
Attack_2	0.259	-0.012	0.231	0.092	-0.018	-0.077	-0.223	0.037	-0.012	0.003	0.228	**0.806**	0.195	0.337	-0.129
Attack_3	0.195	0.015	0.235	0.019	-0.067	-0.083	-0.184	-0.019	-0.040	-0.096	0.182	**0.739**	0.095	0.335	-0.168
Attack_4a	0.132	0.033	0.205	0.035	-0.058	-0.019	-0.199	0.042	-0.045	-0.105	0.153	**0.725**	0.146	0.262	-0.191
Attack_4b	0.086	-0.021	0.215	0.021	-0.090	-0.035	-0.190	0.008	-0.043	-0.113	0.166	**0.721**	0.174	0.271	-0.208
CON_SCALE	0.096	0.018	0.210	-0.024	**1.000**	-0.136	0.104	0.041	0.133	-0.013	0.107	-0.044	0.033	0.039	0.044
Freq_com	0.187	-0.006	**0.907**	0.033	0.167	-0.082	-0.118	0.072	0.008	-0.038	0.259	0.321	0.152	0.259	-0.048
Freq_min	0.157	0.035	**0.847**	0.113	0.207	-0.015	-0.051	0.177	0.109	0.026	0.208	0.253	0.130	0.281	0.036
HM1	-0.022	**0.867**	-0.058	-0.080	0.015	-0.029	-0.043	-0.033	-0.012	0.077	0.183	-0.053	0.048	0.054	-0.032
HM2	0.094	**0.904**	0.072	-0.025	0.016	-0.035	0.033	-0.009	0.048	0.073	0.307	0.062	0.155	0.191	-0.050
KnownFriends	-0.044	-0.047	-0.012	-0.069	0.044	-0.102	0.302	0.021	0.173	0.098	-0.104	-0.221	-0.042	-0.073	**1.000**
LT1	0.256	-0.090	0.073	**0.821**	-0.041	0.130	-0.102	0.066	-0.116	0.270	0.013	0.162	0.023	0.072	-0.161
LT2	0.243	-0.026	0.092	**0.915**	0.018	0.095	0.040	-0.007	-0.118	0.315	-0.034	0.073	-0.058	0.025	-0.050
LT3	0.117	-0.035	0.035	**0.853**	-0.041	0.113	0.108	0.013	-0.050	0.324	-0.130	-0.057	-0.066	-0.025	0.024
PA3	-0.005	-0.012	-0.069	0.100	-0.123	**0.878**	-0.091	0.284	0.122	0.247	-0.140	-0.034	0.034	-0.003	-0.155
PA4	-0.068	-0.052	-0.037	0.127	-0.117	**0.883**	-0.030	0.245	0.182	0.204	-0.246	-0.143	0.067	-0.014	-0.026
PE1_It	**0.862**	-0.066	0.185	0.147	0.024	-0.074	-0.163	0.083	-0.013	-0.002	0.215	0.339	-0.014	0.205	-0.031
PE2_Ph	**0.704**	0.029	0.104	0.194	0.164	-0.044	-0.009	0.090	0.110	0.105	0.115	0.111	-0.036	0.115	0.070
PE3_OF	**0.736**	0.161	0.137	0.235	0.134	0.098	-0.057	0.101	-0.065	0.104	0.196	0.162	0.032	0.101	-0.108
PE4_Har	**0.723**	0.122	0.144	0.209	0.062	-0.066	-0.081	0.037	-0.026	0.071	0.187	0.174	-0.058	0.081	-0.040
SA2	0.060	-0.032	0.132	0.002	0.089	0.270	-0.004	**0.884**	0.330	0.113	0.097	0.036	0.191	0.216	0.059
SA4	0.116	-0.008	0.104	0.044	-0.018	0.259	-0.029	**0.881**	0.325	0.090	0.057	0.010	0.149	0.215	-0.023
SEF3	-0.069	0.018	0.036	-0.141	0.109	0.187	0.090	0.290	**0.895**	0.201	0.068	-0.073	0.216	0.243	0.169
SEF4	0.047	0.022	0.070	-0.057	0.130	0.125	0.048	0.375	**0.902**	0.137	0.147	0.002	0.134	0.271	0.142
SM1	0.136	0.283	0.215	-0.058	0.028	-0.189	-0.096	0.051	0.071	0.013	**0.890**	0.282	0.174	0.334	-0.055
SM3	0.300	0.210	0.260	-0.047	0.166	-0.199	-0.096	0.104	0.144	-0.018	**0.869**	0.236	0.197	0.270	-0.130
SN_exp	-0.129	-0.002	-0.100	0.022	0.104	-0.068	**1.000**	-0.019	0.076	0.092	-0.109	-0.303	-0.073	-0.145	0.302
ST2	0.012	0.124	0.024	0.293	-0.004	0.279	0.022	0.108	0.200	**0.914**	-0.017	-0.044	0.101	0.104	0.056
ST3	0.110	0.092	0.002	0.305	-0.010	0.210	0.105	0.077	0.162	**0.884**	0.040	-0.139	0.033	0.067	0.105
ST4	0.053	0.009	-0.055	0.340	-0.020	0.195	0.119	0.122	0.138	**0.871**	-0.027	-0.096	0.056	0.048	0.101
TM1	0.016	0.072	0.142	-0.037	-0.065	0.082	-0.081	0.203	0.159	0.050	0.180	0.209	**0.836**	0.518	-0.024
TM3	-0.043	0.120	0.120	-0.014	0.080	0.051	-0.051	0.157	0.206	0.074	0.189	0.146	**0.914**	0.501	-0.015
TM4	-0.031	0.123	0.169	-0.058	0.069	0.022	-0.064	0.157	0.152	0.067	0.192	0.170	**0.916**	0.505	-0.072
TP1	0.171	0.140	0.310	0.061	0.050	-0.004	-0.098	0.208	0.260	0.067	0.312	0.369	0.530	**0.842**	-0.014
TP2	0.181	0.133	0.305	0.018	0.039	0.007	-0.138	0.247	0.257	0.082	0.326	0.401	0.488	**0.923**	-0.100
TP3	0.134	0.110	0.196	-0.009	0.016	-0.029	-0.150	0.192	0.243	0.068	0.278	0.382	0.499	**0.890**	-0.078