Individuals' Motivations for Responding to Phishing Emails: a Saudi Arabian Case Study

AHMED ABDULLATIF ALYAHYA

Department of Computer and Information SciencesUniversity of Strathclyde

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

Doctor of Philosophy

2022

DEDICATION

This work is dedicated to my loving parents for their continuous support and directions. They are big believers in me and would always love to see me successful in my life as well as career. Also, this work is dedicated to my beloved wife where words cannot describe her patience, encouragement, scarification, and enthusiasm to see me succeeding on this journey. Moreover, I was super lucky to have my first son last year. His presence made me motivated at all times, therefore, he is a big part of my dedication. Finally, I would also like to dedicate this work to my brothers, for their endless support throughout my journey.

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:

ACKNOWLEDGEMENTS

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

Secondly, my deepest and sincere gratitude and unrestrained appreciation go to my direct supervisor Dr. George R.S. Weir, for his ultimate support, outstanding ideas, and endless advice throughout my research's years. I have been very lucky to have him as a supervisor and to work with him. Further, I extend my gratitude to my second supervisor Dr. Sotirios Terzis, for his constructive feedback during my research's years. My sincere gratitude to my fellow PhD students, academics and staff in the department of Computer and Information Sciences at the University of Strathclyde for their valuable advice, support, and assistance throughout this journey.

I would also like to extend my deepest appreciation and gratitude to my parents for believing in me and for their prayers, endless love and support throughout my life. My sincere thanks to my brothers for their encouragement and support over the years. I am blessed, lucky and proud to have a wonderful family. I cannot begin to express my gratitude to my beloved wife, Aisha, for her immense support, care and cooperation. The accomplishment of this thesis would not have been possible without her assist and encouragement.

Special thanks to my friends Bader Almari, Othman Alyahya, Majed Alshammari, Mohammed Alojail, Mansour Alyahya and Abdulrahman Alkhateeb for their support and companionship throughout my PhD studies.

I am sincerely grateful to those who voluntarily participated in my research survey. Finally, thanks for my sponsor King Faisal University and Saudi Cultural Bureau for their great efforts.

ABSTRACT

The use of email has been exploited by cybercriminals, as a means of carrying out their cybersecurity attacks. 'Phishing' – a form of social engineering attack – is a well-known example of just such a cybersecurity attack; cybercriminals persuade a victim to respond to their emails by presenting themselves as an official person or entity. As this type of persuasion comes in different forms, using different strategies aiming to get a positive response from an intended victim, the current study focuses on different Social Engineering Persuading Strategies (SEPS), which are: Authority; Social Proof; and Scarcity. This study concentrates on decreasing the risk of responding to phishing emails, through the study of the Theory of Planned Behaviour (TPB). The key factors in TPB are Attitude, Subjective Norms, and Perceived Behavioural Control; these influence an individual's behavioural intention in responding to phishing emails, across different SEPS. The current study aims to evaluate TPB, as a tool for explaining user behavioural intentions when responding to phishing emails. A quantitative online survey was used for collecting data from undergraduate students at King Faisal University (KFU) in Saudi Arabia. Data analysis was performed by applying multiple linear regression analysis (MLRA), and confirmatory factor analysis (CFA). The principal finding was that TPB explains 53.8% of the variance in behavioural intention to respond to phishing emails under the Authority strategy, 51.8% under the Social Proof strategy, and 49.8% under the Scarcity strategy. Additionally, the study found that only two TPB factors (Attitude and Subjective Norms) have a statistically significant impact on individuals' behavioural intention under SEPS; Perceived Behavioural Control only has a significant impact on individuals' behavioural intentions under the Authority strategy – it did not have a significant impact under Social proof or Scarcity. The attitude was found to be the strongest predictor of an individual's behavioural intention under the Authority and Social Proof, while the Subjective Norm factor was found to be the strongest predictor under the Scarcity strategies. Additionally, the TPB model was found to have a good model fit when applied to the intention to respond to phishing emails. This means the TPB model might work well when applied to explain an individual's behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS.

Table of Contents

List of Figures

Table of Tables

List of Abbreviations

AGFI	Adjusted Goodness of Fit Index
APWG	Anti-Phishing Working Group
AVE	Average Variance Extracted
ATT	Attitude
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
FA	Factor Analysis
GFI	Goodness of Fit Index
GOF	Goodness-of-Fit
IN	Intention
KFU	King Faisal University
KSA	Kingdom of Saudi Arabia
MLRA	Multiple Linear Regression Analysis
NFI	Normed Fit Index
PBC	Perceived Behavioural Control
RMSEA	Root Mean Square Error Approximation
SEM	Structural Equation Modelling
SEPS	Social Engineering Persuading Strategies
SN	Subjective Norms
TLI	Tucker-Lewis Index
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action

List of Publications

Alyahya, A. and Weir, G. (2021) ‘Understanding responses to phishing in Saudi Arabia via thetheory of planned behaviour’, *National computing colleges conference.* Taif, Saudi Arabia.

CHAPTER 1. Introduction

This chapter provides an introduction to the thesis and makes the problem statement for the current research. In addition to this, it details the research aim, the research objectives, and the research questions. This chapter then goes on to explain the thesis hypotheses, scope, target group, contributions, and structure.

1.1 Research Background

With the advent of technology, there are numerous ways to communicate, through phone, text message, and email; communication via email is the most common medium used nowadays. Moreover, communication via email has become a crucial part of day-to-day life. Email is a widely used communication medium not only in professional and academic environments but also in non-professional environments. Additionally, email is increasingly popular and is preferred over memos or other bulletin notices in various organisations. Even people living in the same residential area prefer to communicate via email when sending various documents, as the other messaging systems have limitations on document size (Ayob and Weir, 2021).

Email is a process of sending and receiving digital messages through the internet (Alkahtani, Dawson, and Lock, 2015). The internet has become universal, thereby increasing the number of users from all age groups. The internet is now a crucial part of people's daily life, and an excellent tool for many purposes, such as collecting and distributing information, serving economic needs, giving education, and entertainment. This background gave opportunities to cybercriminals, and this led to the emergence of various malicious activities. The resulting attacks are causing security breaches that damage individuals and organisations in various industries (Martin, Borah and Palmatier, 2017). Therefore, organisations invest in advanced and sophisticated technologies to prevent cybercrimes. However, no matter how advanced these technologies are, the hackers can exploit the weakest link in the information security chain, which is the human (Abass, 2018; Aldawood and Skinner, 2018; Connolly, Lang and Tygar, 2014; Okere and Niekerk, 2012; Symantec, 2006). Cybercriminals are well aware of the fact that the best technique to manipulate a human being into giving away their security details is through various interactions, and IT professionals refer to this as Social Engineering (Gartner, 2002).

Social Engineering is one of the cybercrimes where the hacker successfully bypasses the security, and gains access to the system and networks to exploit human vulnerability. 'Social

Engineering' was defined by Hadnagy (2011, p. 7) as 'the act of manipulating a person to take an action that may or may not be in the target's best interest. This may include obtaining information, gaining access, or getting the target to take certain action'. Examples of social engineering I.e. persuading victims to download and open a malicious email attachment, and trying to persuade targets to reveal sensitive information. There are different types of social engineering attacks; however, phishing is the most common and fastest-growing form of social engineering (Griffin, 2017; Jamil et al., 2018; Taib et al., 2019). In addition to this, one of the top ten cybersecurity challenges is phishing (Upadhyay, 2020).

Verizon Enterprise (2013) provided data breach statistics, after analysing about 47,000 security reports from 19 worldwide organisations. There were around 621 confirmed data breach incidents. Of these social engineering actions, 79% were attacked through phishing. In recent years, the world's most common cyberattack is phishing (IBM, 2020). It was defined in 2014 by the APWG as a form of cyberattack where the phisher persuades the target into doing particular actions like clicking on a malicious URL, downloading a malicious attachment, and visiting a bogus web page. In simple words, it is a practice of sending emails that seem to be from trustworthy entities to acquire confidential information from the targets like their passwords and credit card details. A report published by CISCO in 2021, mentioned that 67.5% of persons that click on a malicious link are probable to input their private information on a phishing website. In addition, according to Tiwari (2020), phishing sites identified in the first quarter of 2020 were 165,772, which increased from the 162,155 witnessed in the fourth quarter of 2019. Elnaim and Al-Lami (2017) recognised phishing as the most widespread form of social engineering. In addition, the researchers argued that phishing email is the most common type of social engineering attack. It has been mentioned by (FireEye, 2019; Chanti and Chithralekha, 2020) that email remains the most popular convincing method of phishing attack, because communication via email has become a crucial part of day-to-day life. In addition to this, Hadnagy and Fincher (2015) stated that phishing emails are estimated to comprise up to 90% of the 300 billion emails sent every day. Furthermore, in the third quarter of 2018, according to the APWG, 151,014 was the number of removed phishing websites, 270,557 was the number of reported phishing emails, and 777 was the number of brands targeted by the attackers (Aljeaid, 2020). It has been said by Aljumah and Ahmed (2021, p. 1) that one in each 100 emails is a phishing email, which is considered an extremely high number. The current study focuses on the phishing email, as it is one of the more widely recognised

forms of social engineering (Avast, 2020; Elnaim and AlLami, 2017; National Crime Agency, 2019; panda.com, 2019), is the most prevalent social engineering type facing the world (IBM, 2020), and contributes to 90% of data breaches (Retruster, 2019).

Phishing attacks are not constant, and they do not always have the same shape and procedure; they progress over time (David, 2020) and use different techniques to persuade the victims to respond (Cialdini, 2007; Gragg, 2003; Stajano and Wilson, 2011). In addition to this, cybercriminals have become more creative with the techniques and persuading strategies of phishing attacks, in order to avoid detection and increase their success rate (Jayatilaka and Arachchilage, 2021; Nick, 2019). It is crucial that the user should understand the various cybercriminal strategies that are employed to persuade victims to respond to emails, and be knowledgeable enough to detect email attacks that aim to gather a user's confidential information.

The persuasion of individuals can be understood by evaluating successful social engineering attacks. Persuading a victim to reveal confidential information is the key pillar of phishing attacks (Taib et al., 2019). Therefore, the psychological persuasion strategies suggested by Cialdini (2007), in the area of human persuasion and marketing, can also be applied to phishing (Akbar, 2014; Muscanell, Guadagno and Murphy, 2014). The persuasion strategies used by cybercriminals (or SEPS, as previously mentioned (Ferreira, Coventry and Lenzini, 2015)) are used because they increase the success rate of phishing attacks (Akbar, 2014; Atkins and Huang, 2013; Lin et al., 2019; Zielinska et al., 2016). SEPS are further discussed in Section 2.3.

Cialdini has identified six core principles that impact decision-making skills, such as responding to an email or a conversation. These are commitment and consistency; scarcity; authority; social proof; reciprocity; and liking. The current study explores three of these principles, namely, authority, social proof, and scarcity, for two reasons. The first reason concerns a study conducted by Taib et al. in 2019. They reported that three previous studies, comparing the three main proposed persuading strategies – Stajano and Wilson (2011), Gragg (2003), and Cialdini (2007) – showed a strong overlap. Taib et al. (2019) concluded that the three strategies in question – namely authority, social proof, and scarcity – were suitable for use in studying phishing. Secondly, email communication does not require a mutual relationship; an interaction is not required between the receiver and sender when responses are made to phishing emails (Butavicius et al., 2015).

Phishing emails are still a serious problem for several countries around the world. The Kingdom of Saudi Arabia has no immunity to phishing; reports show that the KSA in the first three months of 2020 recorded about one million phishing attacks (AlMindeel and Martins, 2020). The same reports also mentioned that this was the biggest number of social engineering attacks to be logged in the Gulf Cooperation Council (GCC) region. It has been reported by Arab News (2019) that users in the Kingdom of Saudi Arabia (KSA), in recent years, have reported more than 30 million phishing emails. In addition, about 90% of malware was distributed by email, as hackers discovered a new technique to spread fake invoices and scams (Arab News, 2019). According to the Saudi Arabian Monetary Authority, the number of phishing emails that requested a user's confidential bank details has increased, with the fraudsters disguising themselves as government authorities (Arab News, 2020). Furthermore, a report published by Cyren in 2020 stated that a significant increase in phishing email attacks is expected in the KSA in the coming years. Saudi undergraduate students aged 18-25 years constitute a suitable population selected for this study (the selection of Saudi undergraduate students aged 18-25 years is discussed further in Section 1.6)

Tiwari (2020) reported that the failure or success of phishing emails relies on an individual's responses to the email, and disclosure of their information. Furthermore, different researchers mentioned the importance of understanding human behaviour with regard to responses to phishing emails because it creates effective protection mechanisms to avoid phishing attacks (Albakry et al., 2020; Jayatilaka and Arachchilage, 2021; Tiwari 2020).

Therefore, the current research evaluates one of the popular theories used in understanding human behaviour, known as the 'Theory of Planned Behaviour' (TPB) (Bulgurcu, Cavusoglu and Benbasat, 2010; Ifinedo, 2011; Sommestand and Hallberg; 2013) to explain individuals' intentions of Saudi Arabian undergraduate students when responding to phishing emails under SEPS. TPB affirms that behaviour is controlled by the individual's intentions, and the theory comprises three main constructs that influence these intentions; namely, attitude (ATT), subjective norms (SN), and perceived behavioural control (PBC). TPB is further discussed in Section 2.5.

This thesis employs the Theory of Planned Behaviour (TPB) for several reasons. The theory of planned behaviour (TPB) is a behavioural decision-making theoretical framework that is well-validated and has been applied in predicting individual behaviour (Javadi et al., 2013). In addition, the TPB model is one of the most popular and influential models in studying the actions of humans. According to Lin (2010), the model has been used in clarifying most individuals'

behaviour. Additionally, the TPB model has been applied in several studies and has proved to be a powerful predictor of behavioural intention, in various fields and geographic locations (Tolliver, 2016; Yousafzai et al., 2010). Furthermore, a number of studies discovered strong support for the theory of planned behaviour usage (Alajmi, 2010; Sadeghi and Farokhian, 2011; Tsai et al., 2010). According to Armitage and Conner (2001), TPB is the most widely used social psychological theory, as it explains and predicts user behaviour in any given scenario. The possibility of predicting intention and behaviour is increased by the TPB model (Dunn et al., 2011).

The TPB provides a complete model of behavioural antecedents and a structure for extension of the model of previous research (Bobek et al., 2007). According to Johnson (2017), the TPB is considered to be a complete theory when compared to other social behavioural theories. The other mentioned that there are different social behavioural theories such as TRA (Theory of Reasoned Action), TAM (Technology Acceptance Model), and PMT (Protection Motivation Theory) which are considered to be incomplete. For instance, TRA is said to be an incomplete theory, as it essentially focuses on just two factors (Attitude and Subjective Norms) that explain individual behavioural intention to respond to phishing emails. However, TPB goes beyond TRA with an extra factor of Perceived Behavioural Control (PBC) (Ajzen, 1991; Fishbein and Ajzen, 1975).

Additionally, a study published in 2018 (Nasir et al., 2018), confirms that TPB is still prevalent as the most significant theory in the field of information security compliance compared to other behavioural theories such as PMT (Protection Motivation Theory) and GDT (General Deterrence Theory). The author also found that the independent factors of TPB are the strongest predictors of the dependent factor in almost all information security compliance in comparison to other theories such as PMT and GDT. TPB is a well-established theoretical framework, and is applied to many study areas, including but not limited to: analysis of accidents and prophecies (Efrat and Shoham, 2013); ecological psychology (Chan and Bishop, 2013; Donald et al., 2014; Greaves et al., 2013); dietary nutrition (Dawson et al., 2014; Mullan et al., 2015); fitness psychology (Michie and West, 2013); hospitality management (Chen and Tung, 2014); nursing (Yami, 2015); social psychology (Ajzen and Sheikh, 2013); sports and exercise (Prapavessis et al., 2015); transportation (Castanier et al., 2013); consumers' online behaviour (Pavlou and Chai, 2002); smoking behaviours (Rise et al., 2008); and food selection behaviours (Wong and Mullen, 2009). In addition to this, the TPB has been displayed to be a successful predictor of information

security compliance intention (Sommestad et al., 2015), and is a widespread model used in the area of information security (Lebek et al., 2014).

This demonstrates that TPB is a great theory in explaining individual behavioural intention to perform a specific behaviour. Therefore, the current thesis draws upon TPB as the theoretical framework to underpin its research, as it might help in explaining and predicting the individual's behavioural intention to respond to phishing emails.

1.2 Research Aim and Objectives

The current study aims to improve dealing with phishing emails through analysing individual behavioural intentions. To do so, this study evaluates the Theory of Planned Behaviour (TPB) to explain the behavioural intention of Saudi Arabian undergraduate students under SEPS. To accomplish this research aim, the following steps were followed.

- Carry out an inclusive review of the existing literature relevant to this study.
- Analyse the TPB factors and SEPS applied to phishing emails.
- Develop a conceptual model to examine the impact of TPB factors under SEPS.
- Offer recommendations to guide subsequent research conducted within this field.

1.3 Research Questions and Hypotheses

The current study evaluated TPB to explain the behavioural intentions of Saudi Arabian undergraduate students when responding to phishing emails under SEPS. The main research question was as follows.

Research Question: To what extent can the TPB explain the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS?

The current research had one main Research Question (RQ) which had three sub-questions. Further, the first sub-question consisted of three hypotheses that examined the influence of TPB-independent factors on the dependent factor under SEPS when responding to phishing emails. The second sub-question focused on showing the factors of TPB that had the strongest influence in explaining the intentions behind individuals' behaviours when faced with phishing emails under SEPS. The third sub-question focused on the goodness of fit (GOF), to examine the conceptual model's fitness when responding to phishing emails under SEPS.

To answer the main question, the relevant aspects of TPB (ATT, SN, and PBC) and SEPS (Authority, Social Proof, and Scarcity) were studied, which led to develop the TPB model. The three sub-questions were as follows.

RQ1.1: To what extent ATT, SN, and PBC impact the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS?

H1: Saudi Arabian undergraduate students' ATT factor impacts the behavioural intention to respond to phishing emails under SEPS.

H2: Saudi Arabian undergraduate students' SN factor impacts the behavioural intention to respond to phishing emails under SEPS.

H3: Saudi Arabian undergraduate students' PBC factor impacts the behavioural intention to respond to phishing emails under SEPS.

RQ1.2: What factors of TPB have the strongest influence in explaining the behavioural intention of Saudi Arabian undergraduate students when faced with phishing emails under SEPS?

RQ1.3: What is the GOF for the TPB model applied to explain the behavioural intention of Saudi Arabian undergraduate students to respond to phishing emails under SEPS?

1.4 Research Design

The current research used online surveys to gather the required data. Moreover, the data collection procedure consisted of closed-ended questions shared via an instrument-based questionnaire and used a quantitative methodology. To interpret the collected data, MLRA and CFA were used for statistical tests.

The survey consisted of nine different phishing emails, using different SEPS in their contents; three emails each for the Authority strategy, Social Proof strategy, and Scarcity strategy. There were ten similar questions for each email, to test the TPB factors; three questions for ATT, two questions for SN, three questions for PBC, and two questions for the Intention factor. The utilisation of the online survey was a suitable data-gathering technique for the current study, since it delivered a convenient method to collect the wanted target population in a short period, and was cost-effective (Collis and Hussey, 2009).

1.5 Research Contributions

1.5.1 Contribution to Knowledge

Evaluating TPB in the context of phishing attacks, to better understand user behaviour when encountering phishing emails.

1.5.2 Contribution to Practice

Presenting recommendations and guidelines to develop the education and training curriculum for Saudi University students' preparatory years. At present, the curriculum does not include curriculum cybercrimes, its forms, or new tricks used by cybercriminals. Students in this stage are required to be fully educated about the risks of cybersecurity attacks before they step out into the workplace.

1.6 Research Scope

Globally, there are nearly five billion internet users (Datareportal, 2020), making the internet an essential component in day-to-day life. In addition, youths mainly, are always connected to the internet, and Saudi youth are no exception, with youths spending more than thirty hours a week on the internet (Alotaibi and Mukred, 2022). According to Hong (2012) and Boodaei (2012), the chances of clicking on a malicious link increase as the individual spends more time on the internet. Additionally, according to Sheng et al. (2010) and Kumaraguru et al. (2010), the probability of being attacked by phishers, for the age group 18-25 years, is quite high. Previous studies have revealed that the younger population is more vulnerable to cybersecurity attacks such as phishing (Sheng et al, 2010; Kumaraguru et al., 2010; Alzahrani, 2015; Algarni et al., 2017).

It has been mentioned by Datareportal (2021) that about 93% of the KSA population use the internet, and 72% are active on social media. According to Alotaibi and Mukred (2022) and the Ministry of Economy and Planning (2014), more than two-thirds of the KSA's population are under the age of 30. This age group is the largest segment in Saudi society, which makes the KSA a young community. In addition, it has been mentioned by (Alsanad, 2018) that 40% of university students in Saudi Arabia had experienced victimisation, with 57% of targets using social media. Furthermore, several researchers stated that university undergraduate students are the most vulnerable to phishing emails (Kumaraguru et al., 2010; Sheng et al., 2010; Whiteman, 2017). Hence, university students constitute an appropriate population choice for the current research. The study's participants included undergraduate students aged 18-25 years.

1.7 Thesis Structure

This thesis includes six chapters. Chapter 1 shows the background information about the research context, and then explains the problem statement, aim, objectives, research questions, research hypotheses, research contributions, research scope, and study limitations. Chapter 2 shows a comprehensive review of existing works relevant to this study. It starts by discussing

social engineering and its strategies and then moves on to talk about attacks, with more focus on phishing. After that, the theoretical framework of this study is discussed, and the chapter ends with an overview of Saudi culture. Chapter 3 discusses the conceptual framework and development of the hypotheses. It develops the hypotheses through the lens of TPB and SEPS. Chapter 4 discusses the research methodology by presenting a summary of the research philosophy, approaches, strategies, and instruments, followed by a detailed description of the data analysis techniques. Chapter 5 presents the data analysis and research findings for the statistical methods phase of the research, and for testing the research hypotheses as part of the research investigation. Chapter 6 discusses and explains the study's results, theoretical and practical implications, and limitations; in addition to recommendations for future work, and provides a conclusion.

CHAPTER 2. Related Work

This chapter highlights a crucial review of the literature related to the topic of the research. Additionally, this chapter studies the related theoretical work in the fields of Social Engineering and User Behaviour. Social Engineering includes phishing attacks, while User Behaviour theories include TRA and TPB. The chapter will provide background information for the reader on these topics. Additionally, it will provide background information on the KSA.

2.1 Social Engineering

Social engineering is defined as several methods that are utilised to get information to avoid security, via the manipulation of people weaknesses (Bezuidenhout et al., 2010). In addition, social engineering includes gathering data, gaining access, or getting the victim to take a particular action. Kevin Mitnick, a famous social engineer, defined social engineering as 'the manipulation of a person or persons to reach an objective by abusing the victim's emotions, gullibility, charity, or trust' (Al-abdan, 2020, p. 13). Additionally, social engineering has been defined by Harl (1997) as the science and art of getting individuals to obey your requirements. Social engineering attacks aim at deceiving humans to disclose confidential and valuable information (Kalnins et al., 2017). Research published by (Arana 2017; and Breda et al., 2017) revealed that the biggest threat to cybersecurity is via social engineering attacks. In order to prevent social engineering attacks, individuals require periodic training, as the attackers constantly adopt new ways to exploit human vulnerabilities (Krombholz et al., 2015; Puneeth et al., 2015).

A study was conducted by Chitery et al. (2012) on a group of employees who might be targeted by social engineering attacks. The results of their study demonstrated that about 41% of new employees, 17% of IT professionals, 23% of clients and customers, 12% of partners and contractors, and about 7% of top-level management authorities fell prey to social engineering attacks. In addition, their results proved that any person, at any given time, might be vulnerable to social engineering attacks, as the primary focus of the attackers is humans. Social engineering can be the most dangerous method, and according to Abass (2018), human nature is one of the reasons, along with the habit. Human beings tend to follow particular default habits without thinking. Hackers can notice these habits and use them in tracking potential victims (Gulati, 2003).

A study conducted by Orgill et al. (2004) aimed to measure the awareness of internet users about social engineering. The researchers, disguised as employees from the organisation's computer support department, enquired about different information such as usernames, passwords,

etc. The outcomes of the study displayed that about 80% of the participants provided their usernames, while nearly 60% provided their passwords.

A study was conducted by (Fagoyinbo et al., 2011) at Federal Polytechnic, Ilaro, Ogun State, Nigeria, which has about 40 employees. The study aimed to measure the awareness levels in regard to protecting oneself against social engineering attacks. The results of the study demonstrated a high-level lack of awareness and protection against social engineering attacks. Therefore, the researchers recommended spreading awareness among the employees.

Another study was conducted by (Karakasiliotis et al., 2006) to assess the awareness of users through the lens of social engineering, by using email. The researchers provided a combination of legitimate and illegitimate emails, and the participants were asked to distinguish between the two sets. The results of the study demonstrated that around 179 individuals, about 36% of the participants, were able to recognise authentic emails; on the other hand, around 45% of the participants effectively recognised the inauthentic emails. However, the participants were unable to provide convincing reasons for identifying illegitimate email messages.

Bakhshi, Papadaki and Furnell, in 2008, conducted a study to examine the receptivity levels, of the workers of the University of Plymouth (UK), towards social engineering. A link was messaged to participants instructing them to update their software. The results of their study demonstrated that around 23% of the participants fell prey to this phishing experiment.

From the above definitions and studies, it can be seen that social engineering primarily exploits the lack of awareness in recognising social engineering attacks. It also employs verbal skills, and psychological or textual tactics, in order to gain the trust of and communicate with the victims. The numerous methods include communication by email, phone, in person, or via social networking sites. These communications are initiated, not only to gain the victims' trust but also to obtain their confidential information.

2.1.1 Social Engineering Categories and Phases

Social engineering attacks, depending on the perspective, can be broadly classified into various categories. With respect to the entity involved, the categories can be classified into two kinds (Fatima and Naima, 2019) – direct and indirect. Direct attacks can be subdivided into human-based, social-based, and physical-based. Indirect attacks can be subdivided into computer-based and technical-based. Each of these subdivisions will be discussed below, in sections 2.2.1.1

through 2.2.1.5. Section 2.2.1.6 details combinations of attacks, while 2.2.1.7 explains attack phases.

In general, direct attacks involve physical interaction, such as a discussion or visual contact. In indirect attacks, the hacker performs the plan by sending an email including downloadable attachment, a URL, or SMS message.

2.1.1.1 Human-based

Human-based social engineering attacks use human communication and collaboration to gather the required information. One of the methods used in human-based social engineering attacks is Impersonation. In this type, social engineers disguise themselves as high-level executives or leaders to access computer files. Many a time, the employees at the end of the hierarchy are respectful of their managers and bosses, therefore they provide access to their confidential information. (Infosec, 2013; Bhusal, 2021). Because this type needs human interaction, a limited number of persons can be influenced (Fatima and Naima, 2019).

2.1.1.2 Social-based

Social-based needs human interactions where the hacker exploits the emotional and psychological vulnerabilities of the target (Fatima and Naima, 2019, Patil and Devale, 2016). Vishing is one of the methods that is conducted via telephone. The social engineer in Vishing appears friendly to win the trust of the victim. In addition, the social engineer uses a number that is spoofed so that the call is shown to be from a reliable and well-known source (Frauenstein, 2021).

2.1.1.3 Physical-based

This type includes physical actions to collect information regarding the target. Dumpster Diving is one of the popular techniques where the social engineer manually goes over the organisation's trash to determine if any of the information in the trash is valuable and helpful. The gathered information is sorted which might include personal data of the organisation manual, workers, suppliers, notices to the employees, company policy, client's details, and credentials for login. Once the information is sorted the social engineer performs spear phishing (discussed in section 2.1.2) attacks where the gathered precise details on the organisation are used to perform the targeted attack on the victims (Frauenstein, 2021).

2.1.1.4 Computer-based

Computer-based social engineering refers to the use of computer software that strives to gather the desired data. There are various methods to carry out computer-based attacks which are followed by social engineers. An example of computer-based attacks is a pop-up window. In such an attack, a pop-up window will appear on the victim's screen, repeatedly informing them about the connection loss or alerting them about the virus detection. When a victim reacts to pop-up windows, a malicious program is executed that forwards login details to attackers (Fatima and Naima, 2019; Bhusal, 2021). Since it does not contain human interaction, numerous attacks can happen in seconds (Fatima and Naima, 2019).

2.1.1.5 Technical-based

These attacks are executed over the internet and attackers use websites, search engines, and social networking sites as methods for collecting information about their victims. This is made easier if the targets kept their information publicly exist on such websites. Some forensics software can be used to collect information from different sources on the victim (Fatima and Naima, 2019; Frauenstein, 2021).

2.1.1.6 Combinations

Social engineering attacks use a mixture of the above mentioned classifications. For instance, the attacker may scan the dumpster near the company, to gather data about the organisation; such as names, email addresses, or phone numbers of the CEO, Directors, or Managers (Physical-based attacks). Based on this information, the attacker builds a social relationship and exploits the victim's emotions (Social-based attacks). Upon building a trustful relationship, the attacker sends an email with a scam hyperlink or downloadable attachment, which collects the victim's confidential information (Technical-based attacks).

2.1.1.7 Phases

Social engineering attacks are not similar in nature; however, they do follow a common pattern with similar phases. Mitnick and Simon (2003) described four phases in their attack model, namely, Research, Developing Rapport and Trust, Exploiting Trust, and Utilising Information (Figure 1). The Research Phase is also known as the 'information gathering phase' as the hacker gathers the target's information. In this phase, to accomplish the goal of the social engineering attack, the attackers explore and collect details regarding their target prior to carrying out their attack. The probability of success is dependent on the information-gathering phase even though it

requires a lot of time. Different information-gathering tools exist and social engineers are familiar with those tools. The data-collection technique might require technical skills and soft skills to exploit the psychology of humans. Social engineers make any given system vulnerable by using incomplete information by looking into various sources to complete the gathered data. The social engineer studies the data collected and develops actionable steps to exploit the victim.

The Developing Rapport and Trust Phase involves building a relationship with the victim through face-to-face communication or emails. The essential components of this phase include good rapport and winning the trust of the victims. In this phase, the social engineer commences the communication to develop a friendly bond with the target by having conversations that appear to be harmless or sending emails to gather the required information. The social engineer initiates the attack by having conversations that create circumstances where the target's weaknesses are unknowingly discussed, resulting in building trust with the target. Social engineers disguise themselves as well-wishers, financial institutions, or government sectors (Bhusal, 2021).

The Exploiting Trust Phase is where the attacker exploits the emotions of the victim, and extracts confidential information or incites security lapses. Here, the victims are exploited as per the collected data in the previous phase. This is performed to bring out more confidential information. The social engineer utilises various manipulation techniques that force the victim to reveal their desired information by making the victim emotional in order to achieve their goals. The target discloses their information to the social engineer without feeling guilty as the social engineer has built a level of trust with the target. The attackers maintain the trust and emotional state of the victim to prevent them from contacting the cybersecurity agencies or educating themselves on the social engineer attacks (Bhusal, 2021). Finally, in the Utilising Information Phase, the social engineer uses the data collected to accomplish their plan. Here, the social engineer ends the communication swiftly or slowly with the victim. The social engineers remove the proof or details of the crime whilst the target is unaware (Bhusal, 2021).

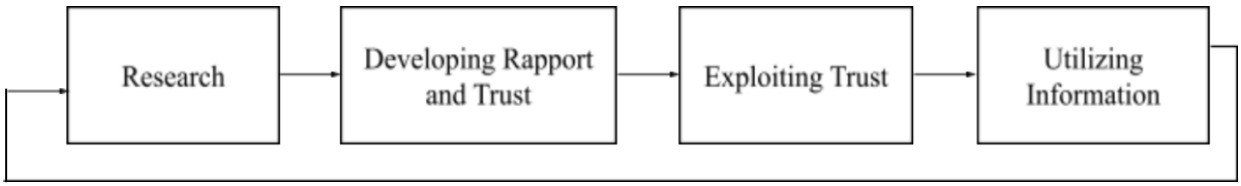


Figure 1 : The Social Engineering Attack Cycle. Adapted from Mitnick and Simon (2003).

2.1.2 Social Engineering Types

There are several types of social engineering. Phishing is the most popular one (CISCO, 2021). It is a social engineering form that, via the use of numerous approaches, aims to impact the victim of the attack in order to disclose private information. This private information is used by the hacker to harm the prey (Al-abdan, 2020; Mika et al., 2016; Nalin et al., 2016). This type is discussed more in the next section. Another form of social engineering 'Tailgating' or 'piggybacking' is used in order to gain access to restricted areas; cybercriminals may pose as delivery personnel or others who may require temporary access (Conteh and Schmick, 2016). 'Pretexting' is a type of social engineering driven by a fabrication scenario, trying to confirm and take private information from a victim (Conteh and Schmick, 2016). In a 'watering hole attack', the user's trust is capitalised on by collecting data from frequently-visited websites. The attacker does not aim to instal malware on the frequently-visited sites, rather they exploit trustworthy websites that might be visited by their target (Abass, 2018). Lastly, 'reverse social engineering attack'; in this type, the communication is initiated by the victim, as the attacker has tricked the victim into contacting the attacker. This technique creates a position where the attacker is the only rescuer for the victim; this is accomplished by creating a form of technical authority or administrative task, whereby the victim may start to ask for assistance and receive commands from the hacker (Abass, 2018).

2.2 Phishing

The term 'phishing' was coined in the 1990s because of harmful activities conducted by individuals, through email, to obtain confidential information, login credentials, and credit card details (Rekouche, 2011). It is a form of social engineering, usually executed through email, in which phishers perform as reliable entities, with the intention of affecting the receivers (victims or targets) to download and open an infected attachment or click on a bad URL (Parsons et al., 2013; Butavicius et al., 2015). Moreover, it has been defined by the APWG (2014), as a form of targeted email attack, where the hacker lures the target into performing particular activities, like clicking on a malicious URL, visiting a bogus web page, or downloading a harmful attachment. Figure 2 illustrates how the attacker (phisher) executes the phishing attack (Campos, 2021).

According to Hadnagy and Fincher (2015), phishing emails are estimated to comprise up to 90% of the 300 billion emails sent every day. In addition, phishing emails deceive individuals

by making the individuals believe that they are disclosing their confidential information to an authentic source. It is been mentioned by FireEye (2019) that emails remain the most popular persuasive technique for phishing attacks. A recent report published by CISCO (2021) mentioned that 96% of all phishing attacks come through email. Through their design, the attackers (phishers) mimic authentic institutes to convince their targets to comply with their needs. Phishing emails are designed to exploit human emotions and respect for higher authority, either for networking purposes or for compassionate reasons (Nabie and Paul, 2016). To rise reliability, phishing emails often copy the content and design of real emails sent by trustworthy organisations.

Phishing is one of the widely occurring forms of cyberattacks which is growing and is a serious threat to internet users as it is performed to obtain sensitive information (Jain and Gupta, 2018; Lastdrager, 2014; Mohammad et al., 2015; Varshney et al., 2016). In addition, phishing activities advanced over time, since attackers spoofed websites to obtain user information via deceptive message tactics (Alsayed and Bilgrami, 2017; Rekouche, 2011; Gupta et al., 2018). In the past decade, hackers adopted new phishing tactics whereby the victims remained susceptible to manipulation. The existing literature has demonstrated humans' inability to capture phishing attacks online; as a result, 90% of people became victims of phishing attacks (Kleitman, Law and Kay, 2018). In addition to this, academics have shown that phishing emails often use persuasive techniques in order to convince the victim to respond to the emails (Atkins and Huang, 2013; Akbar, 2014). Therefore, to decrease this threat, it is vital to recognise the different forms of phishing emails, the design of phishing emails, the strategies or tricks used with phishing emails, and the factors that influence individuals in responding to these attacks.

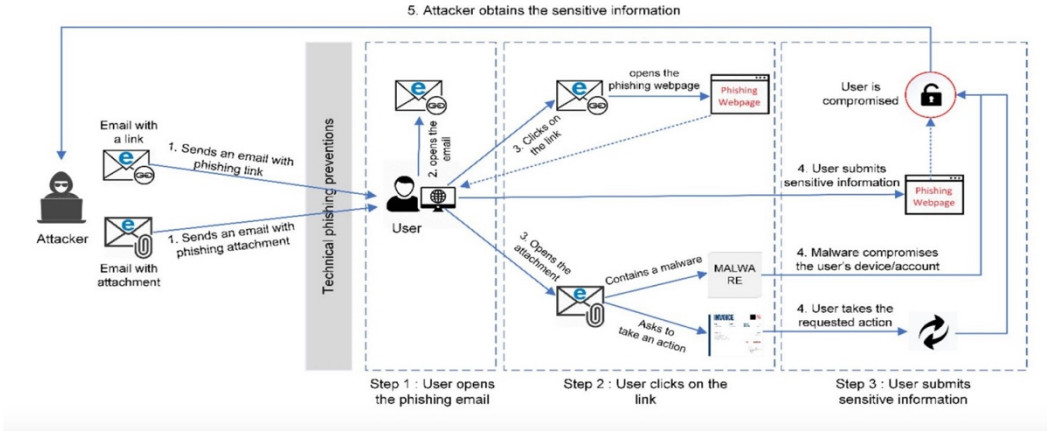


Figure 2 : How a Phishing Attack is Executed (Source: Campos, 2021)

2.2.1 Types of Phishing

There are several forms of phishing attacks. One of the most common forms is the 'Mass Phishing' email; this refers to emails that are sent to a wider audience in huge numbers (Rashid, 2017). In this form of phishing, there are chances that one out of thousands of users might fall prey to phishing emails (Sophos, 2005). Mass phishing is a common form of phishing technique used by phishers; this is basically because it is quick and easy (Pure Cloud, 2021). 'Spear phishing is another type of phishing; this type, aimed at specific individuals or companies, is intended to collect personal information, which helps in increasing the likelihood of accomplishment (Anthony, 2019). 'Whaling' is a form of spear phishing that is designed to target senior executives and high-profile businesses. If these executives fall prey to phishing attacks, the cybercriminals can easily access confidential data or financial details, when compared to targeting an entry-level employee; in the latter case, they would not have access to the same confidential information (Anthony, 2019). Another form of phishing is 'vishing'; in this type, the victim is given a phone number, or follow-up calls are made on a particular activity (Orman, 2013). For example, during the tax season in the United States, individuals receive innumerable calls from phishers pretending to be tax department representatives, asking for the payment of taxes, and attempting to collect confidential information. In 'Smishing', the victim is tricked into giving their private information via a text or SMS message (Orman, 2013). For instance, the hacker might request the authentication code received by the victim to access any social media or messaging platform, such as WhatsApp. The authentication code is used by the hacker to sign into the victim's account and collect private information.

2.2.2 Phishing Email Design

Wang et al. (2009) examined about 200 phishing emails; the results showed that phishing emails are designed very well, to minimise individuals' doubts and induce them to comply with the request. It is suggested by the Elaboration Likelihood Model (ELM) (Petty and Cacioppo, 1986) that the message argument's quality highly impacts the attitude of the receiver toward the acceptance of the message. In addition, the term 'quality of the message argument' denotes the persuasive strength of the argument embedded in the message (Bhattacherjee and Sanford, 2006).

The approval of the message is required for the phishing attack to accomplish. For instance, a phishing email might contain information for the users regarding their account being suspended, as they have violated copyright laws. They are then asked, if it is a mistake, to perform an urgent

action by clicking on an embedded link. It has been discovered by (Wang et al., 2009) that the design of phishing emails emphasises the quality of the message argument. By carefully designing the phishing email, the acceptance level is increased (Alseadoon, 2014). Wang et al. (2009) identified some design features to improve the trustworthiness of phishing emails. These design features are discussed below and summarised in Table 1.

Email title: A good-looking email title may increase the motivation of the receiver to open the phishing email. For example, when a user receives an email from a social network website such as Twitter, with the title 'Urgent: Copyright Infringement', the word 'Urgent' in the email's title may increase the user's curiosity, thus resulting in opening and reading the email. The key purpose of the title of the phishing email is to hearten the user to open and see that email.

Email argument quality: As discussed, this indicates the strength of the argument entrenched in a message (Bhattacherjee and Sanford, 2006). The quality of argument raises the probability that the argument embedded in the message will be agreeable. If receivers accept the argument, the email's message will be responded to and the required information will be provided.

Message appearance: Copyright information and well-designed images will increase the credibility of the message. It has been stated by Sheng et al. (2010) that users tend to determine the legitimacy of a website through its design, and the phishers easily replicate it.

Assurance mechanism: Signs guaranteeing the security or privacy of information increase the trust of users, and decrease any perception of risk, like loss of private information or money (Lee and Rao, 2007). Grazioli (2004) stated that users whose decisions are based on assurance cues are at higher danger of becoming targets.

Table 1 : Key Design Features (Wang et al. (2009))

Dimension	Features
Email title	Urgency, Impact, Company name.
Email argument quality	Event, Courtesy, Response action request, Justification, Urgent, Penalty, Impact.
Message appearance	Authentic-looking email sender, Copyright, Company logo, Personalisation, Media type, Email signatory, Typo, Third-party icon for trustworthiness.
Assurance mechanism	Help link/feedback, Https link, Authentication mechanisms, Anti-fraud/privacy statement, Third-party icon for assurance, SSL padlock, General security lock.

2.2.3 Phishing Email Aspects

According to AlHamar (2010), there are three main aspects of a phishing email: the sender, or phisher; the receiver, or victim; and the email message itself. These aspects are cleverly used by phishers when applying SEPS, and these usages are individually detailed below.

2.2.3.1 The Sender

Phishers create a valid email account and may add the target's name to the account (Forte, 2009), with the phisher impersonating an authoritative figure trying to gain confidential information by making the victim believe the authenticity of the email (Honeynet Project and Research Alliance, 2005).

2.2.3.2 The Receiver

The phishers need to have valid email addresses in order to deliver the phishing emails. Generating a mailing list might be done simply by searching for valid email addresses, purchasing email addresses from the internet, or developing an algorithm to retrieve email addresses from websites through the search option (Bielski, 2004; Forte, 2009). Forte (2009) emphasised not providing explicit references, in discussion forums, to their mailbox. Nagy and Pecho (2009) discussed how social network sites are exploited by phishers, due to a lack of awareness and the instant reactions of the users; which results in providing confidential information, making the user profile vulnerable. Upon identification of email addresses, the phishers utilise spam tools to send emails to the victims (Bielski, 2004).

2.2.3.3 The Message

Phishers design the email message carefully, as discussed earlier, to make the receiver believe the email is from a reliable source (Bielski, 2004). In addition, the attackers trick their victims into sharing private information either on the replicated login page of the email message or by providing them with a link that leads to a fraudulent web page. The phishers might also direct the victim to interact with an automated online communication method, such as email or SMS, or using the phone (Emigh, 2005).

Phishers might manipulate users by making them emotional, and exploiting their feelings towards a cause or donation. They might use different visual tricks to deceive the victim, thus making it hard to identify the phishing email (Dhamija, Tygar and Hearst, 2006). The message might be displayed in a trivial manner, by the user of client support; this requires updating the user record. The email will always possess a sense of urgency, requiring instant provision of confidential information. For instance, the attackers might warn the target that the delay in responding to the email might result in a consequence, such as the cancellation of an account. Additionally, the phishers might utilise a source of surprise, like mentioning the possibility of the target winning a prize (Dhamija, Tygar and Hearst, 2006).

The vital targets of phishers are the reputed designers; emails from well-known designer brands are rarely questioned. The phishers create a replica of the designer's website and post content to extract users' confidential information. The Anti-Phishing Working Group (2006) conducted research demonstrating that 148 brands became the target of phishers, and about 92.6% of the total phishing attacks were on financial institutions. Phishers convince the users that the fake webpage is an authentic page; this is accomplished by hiding the hyperlink address, using URLs similar to the originals, and hiding the URL by displaying the address bar with partial information, concealing the real host destination address (Anti-Phishing Working Group, 2006).

Additionally, different scholars have stated that hackers take advantage of individuals' trust in security updates, to manipulate them through the use of visual tricks (Dhamija, Tygar and Hearst, 2006). The hackers replicate the security icon by just displaying a picture in the site's content. This means the display of the lock icon does not imply a secured website (Herzberg and Jbara, 2004). Moreover, phishers utilise visual tricks to manipulate the target in the browsing location bar, changing it with a false bar, so the attacker is prevented from viewing the actual phished URL, which is one of the key security pointers (Ye et al., 2005; Felten et al., 1997). Individuals mostly do not notice alterations in the address location, as they occur frequently (Herzberg, 2008). There are chances the bogus site may contain a high-assurance security certificate (Franco, 2005). The phishers are able to project a fake site, which consists of an SSL (Secure Socket Layer) certificate that is forged by the use of a vulnerable hashing algorithm, widely utilised by cryptographic functions (Stray, 2008).

2.2.4 Phishing Susceptibility

Phishing susceptibility is fundamentally crucial, as it measures a company's or a user's vulnerability to phishing attacks. Chen and Rao (2020) defined phishing vulnerability in terms of a user who might fall prey to various illicit or deceitful activities. In addition, phishing vulnerability has been defined by Sommestad and Karlzén (2019) as the likelihood of a person undertaking an action that is requested via a misleading message. In addition, Dodge and Rovira (2012) classified phishing vulnerability as a victim clicking on a doubtful link because they are not able to recognise the fraudulent scam. Moreover, phishing susceptibility has been defined by (Kleitman et al., 2018) as failure to recognise a phishing email. From the above definitions, it is clear that phishing susceptibility is a user response based on a lack of awareness of phishing.

Phishing can be successful in deceiving individuals and this is displayed in several studies. For instance, a previous study conducted by (Dhamija et al., 2006) indicated that individuals are vulnerable to phishing attacks, as the significance of browser indications are not valued. Additionally, in a study conducted by (Alsharnouby et al., 2015), the outcome displayed that users only recognised 53% of phishing websites. Many users may not consider security indicators, and they are mainly dependent on the content of the website in evaluating the legitimacy of the website. According to Whiteman (2017), college students are the most susceptible to phishing attacks. Users perceive phishing emails to be sent by trusted sources, and thereby disclose confidential information (Dhamija et al., 2006). It has been stated by (Sheng et al., 2010) that individuals tend to judge the legitimacy of a website by its look, which phishers can easily copy. A study by Bielski (2004) mentioned that email messages are designed professionally by phishers, to manipulate the victim into thinking that the email seems to be from a real source. It has been stated by Forte (2009) that individuals are more susceptible to emails that appear from institutes or other sources with which they share a strong relationship, and they are then less probable to question the authenticity.

Alseadoon et al. (2012) conducted an experiment by sending phishing emails to determine which users were more vulnerable. The finding was that users with less email experience are more susceptible to phishing email attacks. Additionally, a study by Halevi et al. in 2013 analysed the relationship between personality traits and phishing susceptibility. The authors stated that recognising these personality traits might help protect people from phishing attacks. Additionally, the researchers studied how personality traits impacted the users' behaviour on social media such as Facebook. The scholars found that the main factor affecting the issue of replying to phishing emails, is neuroticism, and individuals who achieve a high score on the openness element tend to post more information on social media such as Facebook. Wardman et al. (2009) proposed the necessity to improve individual knowledge about phishing, after showing the vulnerability of individuals to phishing attacks.

A study conducted by Odara and Sanders (2011) aimed to assess the phishing attack awareness of individuals from different countries. An online survey was conducted to study the participants, who were given a number of fake and real emails. Then, they were requested to decide which were legitimate. The outcomes of the study found that only 43% of the legitimate emails were identified correctly (Odara and Sanders, 2011). As previously discussed, another study, conducted by (Alsharnouby et al., 2015), stated that when the participants were presented with real

or fake websites, just 53% of the participants recognised the phishing websites correctly. This emphasises the fact that, while users find it difficult to detect real or fake emails, the websites are also accurately designed to trick the targets.

A study conducted by Parsons et al. (2015) identified the signs that differentiate between real and fake emails. The authors stated that the decisions made by the participants were based on poor indicators. Besides, the researchers reported that the participants were affected by the urgency of an email. Moreover, Parsons et al. (2015) mentioned that the individuals impacted by the urgency had a higher tendency to become victims of phishing attacks. Therefore, the scholars suggested that the users need to be aware of the risks related to fast or urgent replies.

Benenson and Landwirth (2017) explained the causes behind the clicking behaviour of users. The authors experimented by sending an email, with a link to non-existing pictures of a supposed gathering, from a fake personality. The scholars asked the participants some questions about why they clicked or did not click the link. The results showed that the causes for clicking were the following: curiosity, known sender, context, natural behaviour, and fear. In addition, the researchers explained what each factor represented. Firstly, 'curiosity' is understood to be the victim's curiosity 'about the pictures, [and their interest] to see the content' in the email. The 'context' relates to the circumstances of the individual facing the attack, and can be understood as the 'perception [that] the message fits the situation'. 'Known sender' relates to the familiarity of the victim, whereby there is an implicit reason of supposition or certitude that one knows the source of the email. Additionally, 'fear' is explained as nervousness that a hacker might have pictures of the target, and 'natural behaviour' refers to the behaviour of victims where they 'clicked without thinking, [acting] impulsively'. On the other hand, the reasons for not clicking were found to be unknown sender, situation context, message type, link type, and bad experience. While 'unknown sender' is self-explanatory, suspicion of fraud is a supposition that the message is deceitful, and might include malicious software. In addition, 'Situation context' is the perception that the message does not fit the case. 'Message type' is the unknown message, not addressed by the name', and 'link type' is a link that looks doubtful, whereas 'bad experience' is the disagreeable experience in a similar condition. From this study, it is evident that there are many underlying elements that impact the clicking behaviour of individual users when confronted with suspicious emails.

It has been demonstrated by Anawar et al. (2019) that in order to evolve countermeasures for phishing it is essential to know the individual's behaviour towards the phishing emails. The previous study recommended that worker characteristics presented a risk to the enterprise's security (Anawar et al., 2019). There is a high chance that the phishers analyse employees' email interests and habits in order to perform phishing attacks. This increases the phishing susceptibility likelihood (Zaki et al., 2017). Further, the literature indicates a fluctuation in phishing susceptibility with users' demographic factors (e.g. age and gender), as they determine the influence of phishing susceptibility (Anawar et al., 2019). In addition, it has been found by Sebescen and Vitak (2017) that fresh graduates in an organisation are more vulnerable to phishing. More senior workers at a workplace also have greater chances of phishing vulnerability (Sebescen and Vitak, 2017). Bandi's (2016) outcomes indicated that older individuals are less riskier, in terms of online security behaviour, than younger individuals.

2.2.4.1 Demographic Factors in Phishing Susceptibility

Several scholars have studied the relationship between phishing vulnerability and demographic factors (Dhamija and Tygar, 2005; Algarni et al., 2017; Byrne, 2010; Costa, Terracciano and McCrae, 2001; Darwish, Zarka and Aloul, 2012; Dawn et al., 2019; Dhamija, Tygar and Hearst, 2006; Halevi et al., 2013; Jagatic et al., 2007; Milne et al., 2009; Robert, 2018; Sheng et al., 2010; Silic and Back, 2016; Kumaraguru et al., 2010). Sheng et al. (2010) found there was a relationship between phishing vulnerability and demographic elements; age and gender were the main demographic factors that predicted the susceptibility to phishing. In terms of age, these scholars found that individuals in the age group 18-25 were more susceptible when compared to other age groups. It has been stated by Alseadoon (2014) that individuals in the age group 18-25 were more probable to be risk takers.

Albadi and Weir (2018) found that young users of the internet are more vulnerable to social engineering attacks such as phishing. Similar results were shown by Airehrour, Vasudevan Nair and Madanian (2018), who reported that persons in the age group 28-38 years are less susceptible to phishing attacks. It has been mentioned by Taib et al. (2019) that researchers found that younger users are more vulnerable to phishing emails, particularly when they are exposed to scarcity-based emails (Jagatic et al., 2007; Coronges et al., 2012; Sheng et al, 2010). However, Mohebzada et al. (2012) found older users are more vulnerable to phishing emails than younger users. In addition,

Dawn et al. (2019) conducted a study to find if there are age differences in phishing vulnerability. The researchers found there are no age variances in phishing vulnerability.

In terms of gender, Sheng et al. (2010) discovered that females are more vulnerable to phishing than males. This might reflect that females are more possible than males to show agreeableness, and this might impact their susceptibility (Costa et al., 2001). Darwish et al. (2012) argued that females have a sympathetic personality, and some literature showed that females are more vulnerable to phishing attacks than men. In addition, the researchers found that women click on links in phishing emails more than men, and they continue to provide information to phishing websites more than men. Similar findings were concluded by Team (2014) who stated that women are more vulnerable to phishing attacks than men, as they are more open towards social media usage, and more liable to reply to junk ads. Moreover, Kumaraguru et al. (2009) and Silic and Back (2016) also found that females are more vulnerable to phishing attacks when compared to males. Nevertheless, a study conducted by Robert (2018) found that gender did not have any impact on participants' susceptibility to phishing, while age and education did.

2.3 Social Engineering Persuading Strategies (SEPS)

There are numerous theories on persuasion strategies (Cialdini, 2007; Gragg, 2003; Stajano and Wilson, 2011). However, Cialdini's psychological persuasion strategies are considered to be 'the most widely accepted classification of psychological persuasion strategies' (Butavicius et al., 2015, p. 2). As previously discussed, the relevant three of Cialdini's six strategies, in this context, are authority, social proof, and scarcity.

2.3.1 Authority Strategy

Authority is described by Bullée (2017) as a propensity to perform the requests of authoritative figures. It is a human tendency to respect and follow the instructions received from higher powers (Cialdini, 2007; Modic and Lea, 2013; Whitty, 2013). Cialdini (2007) stated that authority is based on the notion that individuals are more probable to reply to someone's request if that somebody is in a position of power. In addition, the principle of authority explains that human are ready to obey the instructions or suggestions of an individual they foretake as an authoritative figure (Hadnagy, 2011). In almost every society, the principle of respecting and obeying with authority is instilled since infantile. Following instructions from authority is the basis of an understanding of power; the decisions affect the entire society.

Authority is the most common and effective persuasion strategy (Akbar, 2014). In the realm of technology, the authority level in any email is a crucial factor in persuading the user's response. Guéguen and Jacob (2002) used a replicated phishing attack to show when contributors were more probable to respond to an email requesting them to fill up a survey. For instance, an email from a higher scientific research authority captured more attention when compared to an email from an undergraduate student. A study conducted by Ferguson (2005) also showed the efficiency of the authority strategy. In that study, more than 500 students were sent an email that appeared to be from a colonel, instructing the participants to click on an embedded URL. Although signs in the email indicated that the demand was illegal, 80% of the participants clicked on the URL within the email, possibly since the email seemed to be from an authoritative individual.

A study was carried out with the students at a university in the KSA, by producing an exact copy of their website. Almost 200 students agreed to get involved; they were informed to the effect that the experiment was to study the behaviour of users when encountering phishing attacks. In addition, the study included a trusted teacher, since out of respect, the students trust their instructors and finish their designated duties. Moreover, the teacher gave the command to the students to log into the website of the university. The result of this experiment found that almost 90% of the students inserted the information just to follow the teacher's command, going by the interface of the website, and not examining the URL and logo correctly. Additionally, another 5% had some uncertainty about the website verification; but, out of trust in and respect for the teacher, they inserted their identifications. Furthermore, the residual 5% questioned the genuineness, and rejected to insert the information (Alghazo and Kazimi, 2013).

It has been demonstrated by Butavicius (2015) that participants were more likely to respond to an email pretending to be from an authoritative figure, such as a manager, or university official. In cybercriminal activities (such as hacking or phishing emails), no face-to-face contact exists, and the attacker is more dependent on authority taken from different higher positions. For example, an attacker can present themselves as a government representative, such as the ministry of health, with the intention to collect the victim's confidential details and send an email requesting an action to view the precautionary steps to protect themselves from COVID-19.

A number of phishing emails have been analysed by Akbar (2014) and Atkins and Huang (2013). In their studies, authority was the most common strategy in persuading the participants to execute a certain activity. Bullée et al. (2015) conducted an in-person experiment, rather than using

email. The authors found that authority did not influence the vulnerability of users towards information disclosure. The clothing of the social engineer was varied to portray different levels of authority, where official clothing denoted high authority and informal clothing represented low authority. According to a study conducted by Guéguen and Jacob (2002), authority signs in an email signature enhanced the pact with a simple email request, showing that authority could be more powerful when indicated through a powerful position, instead of clothes.

In addition to this, numerous studies found that the authority strategy is the most effective in persuading internet users to perform a certain action, such as clicking on URLs, or downloading attachments (Butavicius et al., 2015; Halevi et al., 2015). Because authority is the number one persuasion strategy (Bullée, 2017), it is logical that phishers often use this strategy as the main practice. It is notable, therefore, that individuals who obediently respond to authority are more probable to respond to email requests than individuals who are more hesitant about authoritative entities.

Hadnagy (2011) identified three authority categories that he believed to be more in alignment with social engineering attacks. These were: legal authority – this is built on the lawful system and the authorities are law enforcement personnel, like police officers, attorneys, and judges; organisational authority – this is defined by the organisation's hierarchical structure, with the chiefs (e.g. the CEO) representing the higher authorities; social authority – this includes national leaders, such as Presidents, Prime Ministers, and Kings (Hadnagy, 2011).

As mentioned in Denno's study (2016), that Cialdini has said that 'we are often as vulnerable to the symbols of authority as to the substance' (2007, p. 220). He also states that '[t]here are several kinds of symbols that can reliably trigger our compliance in the absence of the genuine substance of authority... titles, clothes, and trappings of authority' (Cialdini, 2007, p. 221). Attackers comply with authority and symbols in order to influence victims into taking the requisite actions to execute their intentions. For instance, hackers, when executing their phishing attacks, use authority as their principle when impersonating an organisational authority; they request the completion of a specific request, such as changing a password, by providing their corrupted link.

2.3.2 Social Proof Strategy

Social proof is a psychological effect that guides people to copy others' behaviour. Copying what other individuals feel is seen as an easy, simple, and quick way to solve problems or make decisions (Nudgify, 2021). Cialdini describes social proof by saying that we view a

particular behaviour as right in a given situation to the degree that we look at others doing it (Cialdini, 2007, p. 116). Cialdini further states that when we are uncertain of ourselves, when the situation is vague or not clear, we are most probable to look to and agree with the actions of others as right (Cialdini, 2007, p. 129).

When people are not able to make decisions, they look around for recommendations. It is in human nature to follow the peer's lead, and their standards are often adopted and presented as one's own. Social proof is about believing what other individuals are doing or believing in similar or ambiguous situations. This also means humans trust humans, who possess the same nature or level of understanding; for instance, the actions and decisions made by family and friends.

When an individual faces a situation where they are unable to decide, they look around and study the decisions made by other people. This is acceptable as long as they are studying the decisions of people they trust such as friends and family. However, if people blindly follow societal trends rather than their own instincts, there are chances they might encounter consequences that last for long. The worst aspect of this tendency is that it leads to a phenomenon called pluralistic ignorance (Cialdini, 2007).

Pluralistic ignorance refers to the adoption of a particular trend simply because the majority is following it. For instance, individuals might disregard a person struggling to get back on their feet after a bike crash, when no one around is helping. However, if the same individual is being helped by others, there will be a snowball of people trying to see what is going on and help as much as possible. This might escalate to the degree that they might be ordered to leave in order to avoid a traffic blockage (Cialdini, 2007).

Humans find it easy to adopt the decisions made by others. In terms of cybercrimes, cybercriminals have closely studied this behavioural pattern, and they therefore create situations in which the victim is required to seek the help of others and rely on their actions. For example, in cybercriminal activities such as phishing, the attacker might present a product that was reviewed/purchased by the victim's friends. The victim, out of confidence and trust in the friends, might purchase the product and fall prey to the attacker. Here, the basic reason was the recommendation from near and dear ones, and the biased outlook towards the product, without questioning the authenticity or genuineness of the product.

Stajano and Wilson (2011) described social proof as a common scamming technique that encourages people to take risks just because others are willing to bet on the matter. For example,

during an auction, the seller hires fake bidders to increase the bid on an item. Later, the decisions about the auction are made by the seller, while the fake bidders inspire others to increase their bids. In a similar way, scammers also create fake social media accounts, to convince their victims that they share opinions with others.

Research by Modic and Lea (2013) discovered that victims accepted fraudulent offers solely because their peers responded. The scammers pretend to have a good relationship with their victims so they can accomplish their scamming tasks. Furthermore, the scammer might prevent the individuals from discussing the subject with others, and add a policy of cancellation if the 'success' is revealed to others. This is because the discussion of scams is a threat to the scammer's anonymity. For example, in the lottery, the winner is asked not to disclose their victory, in order to avoid double claiming the results.

Numerous studies found that the social proof strategy is successful strategy in persuading individuals to perform a particular action (Akbar, 2014; Butavicius et al., 2015; Taib et al., 2019; Atkins and Huang, 2013). A study conducted by Taib et al. (2019) demonstrated that a large-scale phishing attack was carried out on a multinational monetary institute. In this study, the social proof was the most efficient strategy.

2.3.3 Scarcity Strategy

The scarcity strategy can be explained as individuals finding objects and chances more attractive if they are rare, scarce, or not easy to acquire (Hadnagy, 2011, p. 195). This strategy is commonly used in different fields to impact individuals to take action in situations where they might not normally do so. Scarcity is dependent on the desire which is created due to the lack of items or opportunities. This effect, as explained by Cialdini, is due to the fact that 'the idea of potential loss plays a large role in human decision making. In fact, people seem to be more motivated by the thought of losing something than by the thought of gaining something of equal value (Cialdini, 2007, p. 238).

It was suggested by De Martino et al. (2006) that individuals face a fear of loss, and this is used to encourage their actions. Thus, the fear of loss is an excellent application of the scarcity principle; it focuses on a limitation, of quantity (e.g. 'only three items in stock') or time (e.g. 'limited time offer'). With the set limitation, the individual might fear the loss of the opportunity, and instantly accept the offer (Cialdini, 2007).

The shortage of resources, and the increase in the product's demand, rises the value, making it more wanted. Time is shown as a stressful element; as it affects the market that views time to be in limited supply, therefore an individual does not have time to ponder on their actions (Cialdini, 2007). Chowdhury, Adam and Skinner (2018) mention that time pressure is one of the significant factors behind insecure individuals' cybersecurity behaviour; the authors conducted interviews with experts in cybersecurity, with one of them commenting that 'when we are under time pressure, we do not make the best decision'. An email might present a particular product as being available only for a limited time, and offer a timely reduction, making it valuable and in-demand (Cialdini, 2007). For example, when a user receives an email that presents a particular product with a 70% discount for only 24 hours, due to the time pressure, the user – without thinking or checking the origin of the email – may click on the link within the email. An experiment was conducted on college students who decided the taste of the cookies based on the quantity present in the jar – the fewer the cookies, the more appealing. Similarly, in cybercriminal activities such as phishing, the attacker places a limited time offer in emails to take advantage of the victim's desire. The other common tactic is sending an email with a 24-hour time limit to protect the account by clicking the link; however, failure to do so will lead to the deactivation of the account (Microsoft, 2020).

As explained in the report by F5 Labs (2017), there was an increase of more than 50% in phishing and fraud incidents between October and December. During special periods such as New Year, Christmas, or travel seasons, hackers send emails with coupons, sales, and exciting offers, pressuring users to give up confidential Information. Cybercriminals make sure their offers are unique, in order to urge the user towards an immediate action. Stajano and Wilson (2011) studied various types of methods used by hackers, and presented the victim's behavioural pattern. It was discovered that the hacker uses urging clauses, such as 'one-time offer' or 'limited sale'. In other scenarios, the hackers urge the victim for confidential information in order to prevent the blockage of their account. On the other hand, Fisher et al. (2013) mentioned that a scam might have a reverse effect, which awakens the victim and prevents them from falling prey to the hackers.

2.4 Anti-Phishing Solutions: Non-technical (Awareness) Solutions

The infrastructure can be protected by security controls and advanced technologies that will lower the influence of phishing; however, protecting the individuals requires awareness and education as it might make the users less vulnerable (Downs et al., 2007; Ollmann, 2004) Several

researchers studying phishing vulnerability concluded a need to spread awareness on phishing threats, as it might improve user protection (Downs et al., 2007; Dhamija, Tygar and Hearst, 2006; Kumaraguru et al., 2007; Herzberg, 2009). Forte (2009) concluded that it is complicated to employ technical measures to keep away from phishing, as the hackers aim to directly attain goals if the user is made vulnerable. Thus, it is important to educate and spread awareness among users, to always verify the authenticity of the received emails.

2.4.1 Recommendations and Best Practices

Some researchers provided appropriate recommendations for the best practices to countermeasure phishing attacks. Winder (2009) suggested logging off of suspicious phishing web pages as soon as the user becomes curious about its authenticity. Further, the user should report the experience to the appropriate cyber department which should analyse the situation and spread awareness regarding the web pages and phishing tactics. In addition, it has been mentioned by (Qi et al., 2009) that users should be careful to open doubtful links and/or download attachments sent with the extension (.exe) as this extension is usually infected with malicious software. Forte (2009) studied phishing attacks that focus on creating a new phishing site that resembles an original site and recommended various precautionary steps to avoid phishing attacks. Tally et al. (2006) concentrated on presenting real-time phishing data collection to validate broadcasts, which enables the creation of a global archival system, that enables the discovery of the scope and features of phishing attacks, and predicts the target chosen for phishing attacks. This project was named 'Phisherman', and it suggested and demonstrated the essence of creating a single repository that consists of all phishing incidents reported by different individuals; this might help companies, researchers, and the legal system to study phishing patterns and find different solutions to preventing phishing attacks. It is difficult to gather information from the organisations, especially financial institutions, as the records of any reported phishing attacks have to be kept confidential by law. Moreover, studying phishing attacks is hard as it requires in-depth analysis to achieve a grasp of phishing patterns and techniques. Wu et al. (2006) suggested a necessity for spreading awareness and educating users on how to avoid phishing attacks.

Butler (2007) aimed to spread awareness and educate internet users on threats caused by phishing attacks and a proposed anti-measure framework. Further, Butler (2007) provided an overview of phishing attacks, patterns and techniques used by the phishers and suggested proactive measures to avoid phishing attacks. Moreover, he suggested remedial actions that might decrease

the consequences through which an individual suffers from a well-planned and effective phishing attack. The researcher suggested the necessity for appropriate anti-phishing education in order to safeguard internet users from phishing email attacks. To sum up, the suggested steps and measures by innumerable researchers found the intense need for the users to be educated and some publications reiterate the existing articles and literature.

2.4.2 Recommendations on Detecting Phishing Emails

Literature that suggests crucial practices and recommendations offers several steps to detect phishing attacks and recommends different patterns and methods to avoid phishing attacks. The following section presents a high-level summary of best practices collected from the existing literature that shows how to keep away from phishing email attacks.

Users should focus on the following email patterns

- Ideally, institutions do not collect confidential information via email as it is vulnerable to threat (Butler, 2007).
- An email that addresses the user as 'Dear valued customer' might be a phishing email as organisations send an email with formal greetings followed by the name of the customer (CISCO, 2021; Dhamija, Tygar and Hearst, 2006).
- Any user should focus on the content of the email and carefully study it might contain grammatical errors or misspelled words. An official email is well-drafted by experts to avoid any errors and to clearly convey the message with appropriate formal language (CISCO, 2021; Furnell 2007; Harrison et al., 2016; Jakbosson, 2007; Parsons et al., 2015).
- Phishing email consists of urgency and requests the user to instantly takes an action so the phishing attacks are successfully carried on (CISCO, 2021). For instance, In 2020 when the Coronavirus (COVID-19) pandemic broke out, there were several phishing emails circulating with precautionary steps to be taken. The steps were in an attachment which actually was a software virus to corrupt the system. During the pandemic, the KSA witnessed phishing email attacks purportedly from the Ministry of Health, prompting users to download an attachment to protect themselves from the COVID-19 attack.

Users should focus on deceptive website links

- Phishers hide the fake website's URL and make it difficult for the phishing targets to recognise the authentic URL (Ollmann, 2004). The authentic address is visible in the browser's location or in a message that opens when moving the cursor over the link.

- As the users are unaware of the authentic domain name pattern, the URL is not properly read, which leads to falling prey to phishing attacks. Several phishing attacks purchase incorrect domain names that are not relevant to the organisation; however, they appear to be authentic web pages (Herzberg, 2008).
- Phishers with experience develop URLs that resemble authentic URLs and make it hard for the users to spot the difference instantly. In addition, the attackers aim to purposely use an illegal hostname that resembles the authentic hostname by swapping the characters or minorly altering the words. A study conducted by the APWG (2006) demonstrated that around 48% of phishing URLs resemble authentic URLs making it hard for users to detect phishing attacks. For instance, the most popular sites such as paypal.com, Microsoft.com and apple.com had phishing web pages with a minor change to the name – paypaL.com, microsift.com or verify-microsoft.com, and appple.com.
- Phishers use hidden URLs to conceal the real destination of the webpage. This results in embedding the phishing content at the end of the long URL in the address bar. This pattern is used to conceal the real destination host of phishing attacks (Sophos, 2005).

Authentic website security indicators

- Studies have shown that authentic URLs are protected by Secure Socket Layer/ Transport Layer (SSL/TLS) security commonly used cryptographic protocols, which is a clear indication the website is not a phishing webpage. Moreover, the URLs to authentic web pages begin with 'HTTPS', which is easy to detect in the address bar (Herzberg and Jbara, 2004). By carefully looking for address bar keywords, phishing attacks might be avoided.
- The authentic websites consist of a lock near the status area or address bar. Once the user clicks on the lock icon the security certificate of the website is displayed. According to (Herzberg and Jbara, 2004) it is crucial to guarantee the certificate is reliable and is appropriately assigned to the webpage that is being used.
- It is recommended by the researchers that the users pay close attention to the security alerts displayed by the browsers (Herzberg and Jbara, 2004).

In conclusion, phishing email attacks can be avoided by users not taking any action against suspicious emails or web pages. The phishers study the geographic locations culture, human behaviour patterns and also the pre-set notion of the society. Through this study, the phisher employs new patterns/tactics to successfully carry out phishing attacks. Few researchers

mentioned the unavailability of proper phishing attacks information and patterns (Emigh, 2005; Merwe et al. 2005; Robila and Ragucci, 2006), therefore, it is suggested to spread awareness and educate oneself on the possible phishing attacks.

2.4.3 Phishing Education and Training

Internet users are the primary targets of phishing emails; therefore, high importance should be given to protecting them from such attacks. Users should be aware that a simple act of just opening any given email might result in phishing attacks. There are chances an individual might fall prey to phishing attacks without understanding or making an effort. Phishing emails might consist of links to malicious attacked files that not only harm the user's computer but also compromise the user's security. Therefore, users should be educated on improving the ways to detect phishing emails by providing appropriate phishing detection training and developing educational courses.

Information security awareness can be spread widely by taking the initiative to educate individuals about anti-phishing. Anti-phishing education has been the key anxiety of several institutions. The Anti-Phishing Working Group (2005) has created a phishing awareness site in order to assist in decreasing the risk to individuals of incorrect trust decisions. Several scholars (Butler, 2005; Consumer Reports, 2006; Emigh, 2005) have pointed out the significance and efficiency of teaching the user to prevent phishing.

The internet users have to be aware of the risks and threats of identity theft via phishing and should recognise how to protect their sensitive information from hackers by using security practices properly. In addition, the internet users should have the ability to identify phishing attacks and how to respond to them appropriately. Attackers' skills and abilities are growing and they are becoming more complex and advanced due to the existing methods used to deceive the internet users. Therefore, internet users have to always update their awareness of phishing attacks and their security practices (AlHamar, 2010).

It has been argued by Merwe et al. (2005) that education is not considered a part of the literature as the research helps prevent technical intrusions and phishing attacks. Even though some security experts argue that educating users in regard to security is not an efficient method for protection (Evers, 2007), other researchers (Kumaraguru et al., 2007) recommended developing detailed, well-designed, deeply researched security education courses.

Although there are innumerable anti-phishing education courses, the users are either unaware or disregard such courses (Kumaraguru et al., 2007; Whitten and Tygar, 1999). This creates a sense of urgency for developing educational courses which create enthusiasm and enhances the users' phishing knowledge and awareness.

Anton et al. (2004) recommended that educating the users might worsen or cause a threat to the users when conducting online activities rather than protecting their activities. In addition, other researchers (Kumaraguru et al., 2007) suggest creating simple phishing detection methods that spread awareness and educate users. Here, the need to identify complex security courses can be avoided. Downs et al. (2007) recommended the necessity of educating the users as it will increase users' knowledge of phishing instead of spreading warnings and overwhelming the users with the related risks (Downs et al., 2007). This also recommends that education needs to be efficient and easy to understand rather than creating a sense of threat and anxiety in the user.

The learning literature insists that actual problem-solving activity is necessary to acquire increased well-understood learning (Brown et al., 1989; McLellan, 1996). Therefore, extra effort is required in developing practical training in order to resolve phishing problems, by studying a user's motivation and problem-solving skills.

The key aim of the current study is to evaluate TPB to explain the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS. The following section discusses the theoretical framework of this study followed by an overview of Saudi culture.

2.5 Theoretical Framework

A theoretical framework is a single formal theory where a study is designed around a theoretical framework. It is the primary means whereby the research problem is analysed and examined. The theory of reasoned action (TRA) and the theory of planned behaviour (TPB) are, together, the theoretical framework for the current study, as they use a way for examining the decisions of individuals when doing particular behaviours (Burak et al., 2013). Specifically, TRA and TPB (Ajzen, 1985; Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975) posited that beliefs about outcomes of behaviours and perceived beliefs of persons are antecedents of attitudes and intentions of behaviour (Burak et al., 2013).

2.5.1 Theory of Reasoned Action (TRA)

Ajzen and Fishbein in 1975, introduced the theory of reasoned action (TRA). According to Siponen et al. (2014), two factors represent motivational factors in the TRA of reasoned action, which are attitude toward the behaviour and subjective norms. According to the authors of this theory, the two main variables of the TRA are determinants of individual intentions toward a particular behaviour. In addition, TRA is based on the assumption that a person's intention towards a given behaviour is close to the antecedent of that behaviour. In addition, intentions of individuals can be figured by their attitudes and the subjective norms relate to the behavioural performance (Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975).

Academics give support for the attitude toward the behaviour, in the existing literature (Baloglu et al., 2016; Chatterjee et al., 2015). Ajzen and Fishbein (1980) used TRA and supposed that attitudes towards behaviour arise from the beliefs towards that behaviour. Further, they assumed that attitudes are a mixture of beliefs regarding the characteristics of a certain attitude and evaluations of the characteristics. Moreover, the individual's intention plays a crucial role in TRA model, and is considered as the major predictor of an individual's intention towards performing an act (Ajzen and Fishbein, 1980).

According to Yazdanmehr et al. (2015) 'subjective norms' refers to individuals' beliefs regarding what the individuals think those significant people to them (for example, family and friends) expect. TRA has been progressed by TPB, to include an additional factor in predicting individuals' intentions, called Perceived Behavioual Control (PBC) (Ajzen, 1991).

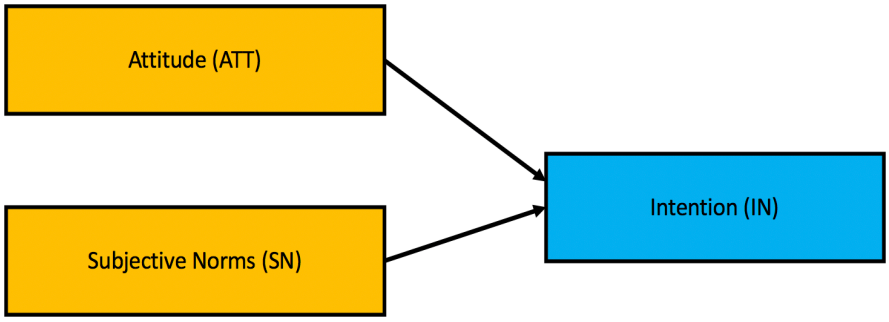


Figure 3 : Theory of Reasoned Action model (TRA)

2.5.2 Theory of Planned Behaviour (TPB)

Ajzen was involved in developing the Theory of Reasoned Action (TRA), and also developed the Theory of Planned Behaviour (TPB) (1991), which is an expansion of TRA. According to the author, TPB was developed to explain a diversity of individuals' behaviours in

different environments or contexts. TPB seeks to predict a person's attempt to execute a certain behaviour. In addition, Murnaghan et al. (2010) mentioned that the purpose of the theory is not just to predict the behaviour of individuals but also to explain it. The theory states that the behaviour is controlled by the individual's intention. Consequently, according to the author, from the given intention, a certain behaviour can be predicted (Ajzen, 1991). Furthermore, the individual's behavioural intention is impacted by the three main factors, which are Attitude (ATT), Subjective Norms (SN), and Perceived Behavioual Control (PBC) (Kwan and Bryan, 2010). In TPB, the three main mentioned constructs were defined by the author of the theory, Ajzen (1991), as antecedent constructs of intention. ATT is defined as a feeling towards a behaviour, SN refers to the perceptions of societal expectations about a person's behaviour, and PBC refers to an individual's perceptions of volitional control with regard to a given intention (Ajzen, 1991; Johnston and Warkentin, 2010). It has been stated (Javadi et al., 2013) that the more favourable the ATT, SN, and PBC, the stronger should be the intention of individual in performing a certain behaviour.

In TPB, the behavioural intentions are supposed to be the greatest predictor of an individual's attempt to execute a particular behaviour. A meta-analysis of about 190 studies linked to TPB supported the predictive power of the theory, and discovered that the theory accounted for about 27–39% of the behavioural intention (Armitage and Conner, 2001). Additionally, a meta-analysis of 422 studies conducted by Sheeran (2002) discovered that the TPB accounted for about 28% of the behavioural intention. Moreover, studies have displayed the predictive power of the theory constructs on intention, with a range of 39% according to Armitage and Conner (2001), and 50% for intention according to Hagger et al. (2002). A systematic review discovered that TPB is roughly as perfect at predicting intentions and behaviour related to information security studies (such as compliance with information security policies) — approximately 40% of the variance in intentions has been clarified in survey research (Sommestad and Hallberg, 2013). Therefore, meta-analyses of correlational studies have recommended that intentions are moderately to highly associated with behaviour (Cohen et al., 2003). The popularity of the TPB is indicated by the number of citations made. According to Sommestad and Hallberg (2013), there were more than 23,000 citations made in 2013. Additionally, the number of citations increased in 2014 to more than 27,500 (Beduz, 2014).

TPB has three key independent factors that influence behavioural intention (intention is the dependent factor of TPB). The three main independent factors are Attitude (ATT), Subjective Norms (SN), and Perceived Behavioural Control (PBC). ATT, SN, and PBC are an individual's beliefs in any provided scenario (Sommestad and Hallberg, 2013). ATT is determined by behavioural beliefs – an individual's belief about the result of a given behaviour. This is based on the probability that certain behaviours result in certain outcomes. SN is determined by normative beliefs – perceived social pressure. PBC is determined by control beliefs – an individual's beliefs about the presence of variables that might work towards or delay execution of the behaviour (Ajzen, 2001). The following section provides an insight into the TPB factors, independent and dependent.

2.5.2.1 Attitude (ATT)

Attitude is the first construct in TPB, and Ajzen (1991) defined it as a favourable or unfavourable evaluation a person holds with respect to certain behaviours. ATT is the overall evaluation of a person's good or bad behaviour (Fishbein and Ajzen, 1975). Attitudes are formed through integrating the beliefs of behaviour and evaluating the outcome (Ajzen, 1991). Attitude possesses various scales of measurement that might be measured using different adjectives, like good or bad, advantageous or harmful, useful or useless, important or unimportant (Ajzen and Fishbein, 1980). Based on a person's belief, the attitude is determined; for instance, a positive perception has a positive attitude.

Attitude is a decisive factor in behaviour patterns that decide if a situation should be accepted or avoided. For example, when a user decides to accomplish a task (e.g., intention towards information security policies compliance), the attitude plays a significant role in deciding the response (Bulgurcu et al., 2010; Ifinedo, 2011; Sommestad et al., 2015). A significant amount of intended behaviour is explained by attitude (Arpaci and Baloglu, 2016; Burns and Roberts, 2013; Jafarkarimi et al., 2016; Kumar et al., 2008; Lee and Kozar, 2008; Ng and Rahim, 2005; Safa et al., 2016; Yao and Linz, 2008; Zhang and McDowell, 2009). Therefore, according to the Theory of Planned Behaviour (TPB), attitudes will have a significant impact on users' intentions (Ajzen, 1991).

2.5.2.2 Subjective Norms (SN)

Subjective norm is the second construct in TPB and represents the social pressure on the individual in deciding if a particular behaviour should or should not be performed (Ajzen, 1991;

Yazdanmehr and Wang, 2015). In other words, an individual who is motivated by others feels a sense of obligation to perform the behaviour that conforms to perceived social pressure (Hernandez and Mazzon, 2007). In addition, SN is determined by the perception of a person's normative belief, that motivates a certain behaviour and its compliance. Furthermore, SN is a prerequisite to a person's intention in doing a specific behaviour (Ajzen, 1991). In this scenario, the individual is more concerned about others' approval or disapproval when deciding whether or not to perform a certain behaviour (Yoon and Kim, 2013). Based on their beliefs of what others think about the individual, their intention to execute a behaviour has a positive or negative effect (Armitage and Conner, 2001; Yazdanmehr and Wang, 2015).

The influence of SN, or societal pressure/expectations on individuals, plays a critical role in shaping their intentions. In other words, the perception shaped by a person relating to their normative beliefs is built via the behavioural anticipations of that individual based on their social circle. In addition, the influence of family and friends on an individual impacts their conscious and subconscious decision-making process.

Fishbein and Ajzen (1975) illustrated that subjective norms are considered to evaluate the impact of the surrounding social environment. Therefore, it is crucial to differentiate between social influence, injunctive norms, and descriptive norms, as they are considered to form different motivational bases (Deutsch and Gerard, 1955). Injunctive social norms come under the category of subjective norms, as they emphasise social pressure, whereby the individual is more concerned about gaining approval from others, regardless of their opinions, view-points or comfort levels. Descriptive norms can be explained as a perception of others, their attitude and behaviour in the provided field of interest.

2.5.2.3 Perceived Behavioural Control (PBC)

PBC is the independent factor that differentiates the Theory of Planned Behaviour (TPB) from the Theory of Reasoned Actions (TRA) (Ajzen, 1991). This construct is influenced by the individual's salient control beliefs (Ajzen, 2002). According to Blythe (2015), the PBC construct is similar to a construct named self-efficacy. PBC relates to the ability of a person, or their perceived capacity, to enact a particular behaviour in relation to their intention. This can be reframed as the effect of 'control' variables that to a large part influence the decision-making standards undertaken by a person when choosing to follow a certain course of action. These variables, predominantly referred to as 'control factors', will dictate the levels of behavioural

control assigned to the undertaking of a particular course of action or activity. Additionally, multiple control factors can be present at a given time, and the perception of an individual as to which variable is more powerful influences their decision to take action in line with the degree of control within a given factor (Schifter and Ajzen, 1985).

PBC assumes that the more a person believes in the chances and resources they possess to perform a behaviour effectively, the greater their intention will be to execute that behaviour (Ajzen, 2002). PBC is driven by an individual's belief in their ability to execute a certain behaviour (Ajzen, 2002). In addition, this factor includes internal factors (information, expertise, abilities, feelings, and coercion) and external control elements (sources, chances, and dependence on others) which might affect the behavioural intentions. PBC not just affects the dependent factor of intention, but has displayed some correlational role in the actor showing real behaviour (Ajzen, 1991).

2.5.2.4 Intention (IN)

Intention is the dependent element in the Theory of Planned Behaviour (TPB). In addition, intentions are supposed to gather the reasons behind an individual's motivational factors that influence their behaviour. This indicates how much an individual is willing to put in the effort, and plan, to exert a given behaviour. Generally, if the intention is stronger, there is a high chance a person might execute a given behaviour. According to Rezaei et al. (2018), the more one intends to involve in a certain behaviour, the more probable will be its execution.

TPB asserts intention as a behaviour that determines the performance of the actual behaviour of an individual (Dinev and Hu, 2007). Intention is taken as a pointer in evaluating the efforts of a person to do a particular behaviour (Ajzen, 1991). In addition, intention captures the motivational elements which impact an individual's behaviour (Ajzen, 1991). As discussed earlier, the independent factors (ATT, SN, PBC) influence the dependent factor, IN (Randall and Gibson, 1991). Research studies performed to validate TRA and TPB found that there is a strong correlation between an individual's behavioural intention and real behaviour (Ajzen, 2002). The following figure shows the Theory of Planned Behaviour (TPB) model.

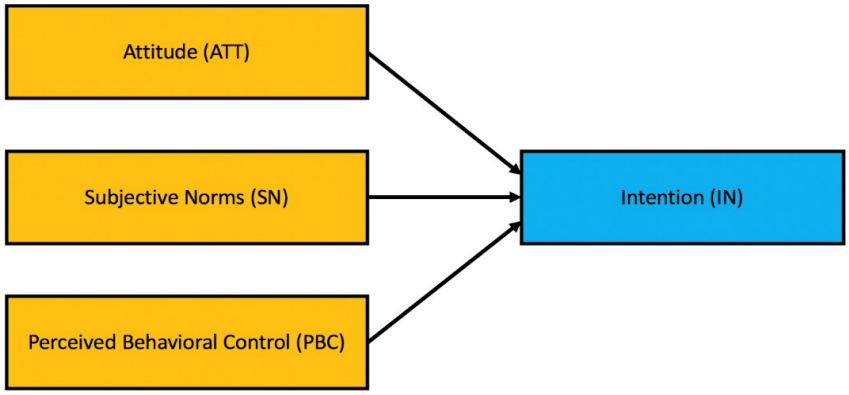


Figure 4 : Theory of Planned Behaviour model (TPB)

To sum up, the Theory of Planned Behaviour factors, attitude, subjective norm, and perceived behavioural control work to develop a behavioural intention to impact an individual's intention to perform an action. The most favourable of the factors, according to Ajzen (1991), is the beliefs evaluated positively based on any behaviour; the thoughts others think are crucial and to be performed as well as the perceived control one has over it; the greater an individual's intention to participate in the behaviour the positive the results. The direct antecedent to any behaviour is intention as with any provided sample of degree which has control over a certain behaviour the individuals are to perform their behaviour based on their intentions. As per the theory, intention (e.g., 'I will purchase products online') is determined by attitudes toward the behaviour (e.g., 'purchasing products online is a good idea'), subjective norms (e.g., 'people who influence me prefer purchasing online products'), and perceived behavioural control (e.g., 'I am able to purchase online products'). Therefore, from the above statement, the factors are interdependent and influence an individual's intention to purchase products online. If the individual believes purchasing the online product is good and people who are important to him/her prefer to purchase a product online and he/she is able to purchase a product online, the greater the intention is influenced the positive the result.

The Theory of Planned Behaviour (TPB) main constructs (ATT, SN, and PBC) determine the effect of the individual's behavioural intention that plays a deciding factor in performing a certain behaviour. In the current study, intention represents the desire and possibility of an individual to respond to phishing emails. For instance, a person with a positive attitude, subjective norms, and perceived behavioural control over the behaviour, will have a determined behavioural intention to implement that behaviour (Ajzen, 2002). Consequently, Ajzen's theory of planned

behaviour model was adopted to predict and explain the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails. The next section discusses culture in general and Saudi culture in particular.

2.6 Culture

According to (Dadfar et al., 2003) the term "culture" originates from a Latin term called "cultura", which indicates that culture is part of people's activities. In general terms, most people of a particular nation share a common culture. According to Hofstede (1993), culture influences individuals' ways of thinking and behaving. Additionally, Hofstede (1984, p. 21) defined culture as 'the collective programming of the mind which distinguishes the members of one human group from another'. According to Alkahtani (2018), and Simon and Yaras (2000), it is a mixture of people's saying, thought, and making their costumes and traditions, art, language, usual agreeable attitudes, values, feelings, and written and non-written rules. In addition, it has been stated by Dadfar (1990) that culture is what individuals think, have, and make in their culture. It has been mentioned by Al Izki (2018) that, according to Alvesson (2002), the concept of culture has different meanings, including: collective forms of notions and understanding; beliefs and values; signs and meanings; norms and principles; emotions and feeling; patterns of behaviour; and practices and structures. There is an agreement that culture works at several levels like individual, organisational and national levels (Chen et al., 2012; Pizam, 1993). Hofstede and Minkov (2010) believed that the most essential level is the national level. National culture might have an influence on people's behaviour, which affects their responses to various incidents in life, such as encountering a phishing email.

National culture is a common belief system that exists among people's behaviour in the same society. Although there may be different groups of people from different backgrounds, national culture is a 'large frame' of thought and inherited belief (Larsson and Risberg, 1998). According to Beck and Moore (1985), national culture is the assumptions, beliefs, and values that people develop in early infancy and these attitudes distinguish one group from another. Indeed, national culture can be viewed as a guideline that people use in their everyday life.

There are wide variations in culture between countries, like geography, ethnicity, religion, gender, and generation; all define the national culture of an individual's country (Hofstede, 2005). Therefore, what one country or culture finds more acceptable might not be received in the same method by another culture or nation. This point has been emphasised by Alas (2006, p. 237) as

follows: ‘What one ethnic group thinks about what is right or wrong depends on culture and environmental circumstances and is different across the cultures’. In addition, national culture has been defined by Ali and Brooks (2008) as a shared set of norms, values, and practices, that forms people behaviour within that culture. Hofstede (Hofstede, 1993; Hofstede-Insights, 2021) has classified national culture into six dimensions that distinguish one culture from another. These six dimensions are Power Distance, Uncertainty Avoidance, Individualism vs Collectivism, Masculinity vs Femininity, Long Term vs Short Term Orientation, and Indulgence. These six dimensions are discussed in the following subsections.

2.6.1 Power Distance

According to Hofstede, power distance is defined as the extent to which the less powerful members of an institution or organisation within a country accept that power is distributed unequally (Hofstede-Insights, 2021). Hofstede discovered that some countries, such as Arab countries, are categorised as ‘high power distance’, where the less powerful members respect the hierarchy and accept the instructions from more powerful members (Hofstede-Insights, 2021).

2.6.2 Uncertainty Avoidance

Hofstede defined uncertainty avoidance as the method that a particular culture deals with the fact that the future can certainly not be recognised: should we attempt controlling the future or just let it occur? (Hofstede-Insights, 2021). In cultures with a higher uncertainty avoidance ranking, individuals are more concerned about ambiguity. The reflection of this can be seen in cultures that are most rule-oriented and less willing to accept organisational changes (Hofstede-Insights, 2021). For example, Arab countries are ranked by Hofstede-Insights (2021) as highly risk-averse, and therefore less likely to engage in situations reflecting high levels of uncertainty. Indeed, high risk is associated with a higher level of uncertainty.

2.6.3 Individualism vs Collectivism

Individualism is defined as ‘the degree of interdependence a society maintains among its members’ (Hofstede-Insights, 2021). In individualistic societies, people care more about themselves and their family, whereas in collectivist societies, people are more inclined to the groups that can carry influence over behaviours and norms. Under Hofstede’s model, more Eastern countries are shown to be highly collectivist societies, scoring much lower than their Western counterparts on the ‘individualism’ dimension. Therefore, in a collectivist society, people are more

likely to share information with one another and perhaps share more than their individualist counterparts.

2.6.4 Masculinity vs Femininity

According to Hofstede, this dimension is defined as the extent to which individuals of a society differentiate and emphasise traditional gender and work roles (Hofstede-Insights, 2021). Men are supposed to be assertive, tough, and focused on physical success, while women are assumed to be humbler and concerned with the quality of life. According to Claes and Ruiz-Quintanila (1998), 'masculinity' cultures deal with challenging work, high-level careers, competition among colleagues, and earnings. Additionally, 'feminine' culture deals with consultation, skill development, and networking.

2.6.5 Long Term vs Short Term Orientation

This dimension explains how societies preserve links from their past to deal with the challenges of the present and future (Hofstede-Insights, 2021). Short-term orientation societies expect quick outcomes; therefore, they do not have the desire to save for the future and focus on the present, while long-term orientation societies don't expect quick results. They focus on future through savings and investments in projects with long-term benefits.

2.6.6 Indulgence

According to (Hofstede-Insights, 2021), indulgence is defined as the extent to which individuals attempt to control their needs and wishes based on the method they were raised. This dimension explores the willingness of a society to realise their desires and indulge in more spontaneous activities. More indulgent organisational cultures will value employee autonomy and encourage innovative and entrepreneurial behaviour, while restrained organisational cultures emphasise structure and rigidity; thus, they restrict employees from expressing themselves more freely (Hofstede-Insights, 2021).

Various definitions of national culture can be summarised as a set of beliefs, values, and attitudes, which are shared, interpreted, and transmitted over time within a collective group, making it unique and distinguishable (Bik, 2010). Arab countries share the same cultural characteristics. Althakhri and Rees (2008) characterise Arab culture as robustly group-oriented, high power distance, and strong uncertainty avoidance. One of the Arab cultures, Saudi culture, will be discussed in the following subsection.

2.7 Saudi Culture

Each region or country has its own culture, and consequently its style of living. Saudi society is primarily based on religion, followed by the tribal system. According to Alkahtani (2018), the culture of Saudi Arabia has been affected by its tradition, history, and the religion of Islam, which make Saudi Arabia dissimilar to other societies. In addition, Saudi Arabia holds a single position in the Islamic world, as it is the home of two great Holy Mosques, Makkah and Madinah, which every Muslim looks up to (Al-Rasheed, 2001). Furthermore, Saudi culture is defined by the teachings of Islam, which include traditions, social manners, obligations, and the responsibilities of the culture as a whole. The individual's place in society is impacted by kinship and tribal systems, which determine the success or failure of tradition as well as the areas of activity. In addition, the system of tribal has a main influence on the workplace culture (AlShehry et al., 2006).

Saudi culture is driven by the teachings of Islam, which defines the moral principles and society's behaviour as per the Quran, Muslim's holy book, and the Sunnah, teaching and practices of the prophet Muhammed. In addition, more information about the principles, rules, and regulations can be studied by reading the translated copy of the Quran (Dawood, 2003). Sharia law, a legal system, is created from the Quran and is a unifying force that has a deep impact on Arabic countries. The Muslim community is a brotherhood that treats everyone equally and disregards the health or wealth or class of the individuals. The common saying is that ethics come from religion (Hofstede, 1998).

Family relations are highlighted greatly by the Sunnah and Quran. Therefore, family plays a crucial role in Muslim societies. According to Hofstede, Saudi culture is a collectivist society in which individuals are bound to groups (Hofstede, 2001, 2011; Hofstede-Insights, 2021). In addition, the culture is deeply rooted in family bonding, where the individuals look up to their elders or cousins while making a decision. The opinions and perceptions of other close relations matter the most, more than the individual's own opinion. Therefore, in such societies, when an individual is faced with a phishing email, the receiver is more inclined to the views of others. In such cases, there is a high probability that the individual might fall prey to phishing emails, as the elders or other close family members might not be aware of the scam emails.

In addition to this, Hofstede explained that Saudi culture is power-driven, and in virtue of power distance, all individuals in the society cannot be considered to be equal (Hofstede, 2001,

2011; Hofstede-Insights, 2021). The Kingdom of Saudi Arabia follows a hierarchical order in organisations or other management, whereby individuals receive work or orders from higher-level authorities. If someone receives a phishing email from an attacker disguised as a higher authority, the receiver – without a thought – will respond to the email, out of respect or pressure from the organisational policies and cultural norms.

According to Hofstede (2001), every culture maintains connections with its history while dealing with future and present challenges. In addition, the author states that such societies have two existential goals, differently prioritised. Normative cultures favour maintaining norms and traditions, and they view with suspicion any change in societal norms and behaviours. On the other hand, cultures with a practical approach focus on developing modern education and are more open to new ideas and perceptions.

2.7.1 Phishers and Study of Saudi Culture

Saudi Arabia very much resembles the culture of one of its neighbouring countries – Qatar (Hofstede-Insights, 2021). A study conducted by AlHamar (2010) aimed to decrease phishing emails risk in Qatar through an efficient awareness framework. In AlHamar's 2010 study, interviews were conducted on Qatari culture. As the cultures of the KSA and Qatar are conservative, it is very easy to manipulate the victims, as by studying just one country's culture the phisher can place phishing attacks on two countries. Qatar and the KSA are more inclined toward religious and Islamic beliefs (Dawood, 2003). The citizens of these two countries follow Islamic beliefs, which preach being good, holding moral beliefs, treating others with kindness, affection, and care, and being honest and trustworthy. Therefore, the phishers misuse the trust of the users from these geographic locations, to conduct their phishing attacks and violate the emotions, beliefs, and trust of individuals. Moreover, the interviewees mentioned the phishers study the culture of Qatar when conducting a phishing attack, and the users easily fall prey to the attack, as they feel safe and protected in the Qatar environment (AlHamar, 2010). As mentioned above, similar attacks are conducted on the KSA, as its culture resembles that of its neighbouring country.

The KSA's culture is described as normative in nature, as it is strongly concerned with maintaining family traditions, culture, and values. If an individual comes across a phishing email, they have a pre-set notion and responses toward the email. The email is seen as easy, direct, and simple, therefore the individual responds to the phishing email and falls prey; or, it is difficult to

comprehend and understand, therefore no response is given to the phishing email. The family traditions/culture might include not responding to unknown emails, and avoiding any communication. Thereby, people might be saved from phishing activities. Hence, the user behaviour and responses are based on the perceived notions set by the culture. According to Hofstede (Hofstede-Insights, 2021), Saudi Arabia and Qatar have power distance and collectivism with similar values. As mentioned above, the power distance is more focused on authoritative figures, who make the laws and set the rules. In such scenarios, when an individual receives phishing emails from high-level authority figures, there is a high chance the user will respond to the email out of trust for the manager. On the other hand, collectivist societies are more close to each other and prefer working as groups. Therefore, the phishers exploit the entire group, by sending emails referring to their friends participating in a survey, or suggesting group volunteering activities.

2.8 Chapter Summary

This chapter discussed and presented related work reviews for the current study. The chapter started by discussing social engineering, focusing mainly on phishing email attacks. Additionally, this chapter discussed three of the SEPS (namely, Authority, Social Proof, and Scarcity) that phishers use when sending their phishing emails to persuade their victims to respond. Furthermore, anti-phishing solutions, mainly the non-technical (Awareness) solutions, were debated in this chapter.

This chapter also discussed the theoretical framework; it started by discussing TRA, then moved on to discuss the main framework for the current study which is the Theory of Planned Behaviour (TPB). It explained the key factors of TPB (ATT, SN, and PBC) and how they influence individual behavioural intentions.

In addition to this, Saudi culture is explained in this chapter; an overview of Saudi culture is discussed, additionally to talking about the cultural factors of the KSA, and how phishers study these cultural factors and exploit them in performing their attacks. The next chapter develops the hypotheses for this study.

CHAPTER 3. Development of Hypotheses

3.1 Introduction

This chapter presents the research hypotheses of the present study. The key objective of this chapter is to develop the hypotheses based on the Theory of Planned Behaviour (TPB) framework and Social Engineering Persuading Strategies (SEPS) discussed in the previous chapter. In this chapter, Section 3.2 proposes study construct definitions for TPB, Section 3.3 describes the development of the hypotheses, with respect to the research model and strategies (TPB and SEPS), and the last section, 3.4, provides a summary of this chapter.

3.2 Proposed Study Construct Definitions for TPB

The current study draws upon the Theory of Planned Behaviour (TPB) as the theoretical framework to underpin the current research, as it might help in understanding user behaviour in different scenarios, such as responding to phishing emails. The following are the definitions derived for the three independent constructs of TPB that are employed in this study:

- Attitude towards the behaviour is an individual's mindset (for example: their thoughts, feelings and self-understanding, motivations, and perceptions) for the information security in their organisation (Ajzen, 1991). Attitude is strongly associated with intention by TPB (Ajzen, 1991; Chatterjee et al., 2015). This proposes an argument that there is an influence of attitude towards the intention to respond to cybercrime activities, such as phishing emails.
- Subjective norms refer to the socialisation behaviour of the individual whose behaviour is determined by the beliefs of those important to the individual, on how they should act (Ajzen, 1991; Yazdanmehr and Wang, 2015). TPB proposes that the beliefs of others influence intention with respect to performing a certain behaviour (Chatterjee et al., 2015). This proposes a suggestion that there is an influence of subjective norms towards intention to respond to cybercrime activities such as phishing emails.
- A belief in the individual's ability to undertake certain behaviour drives PBC (Ajzen, 2002). This belief is based on the performing behaviour and the required skill set that is in the control of the individual, and the extent to which it yields the expected results (Ajzen, 1991). This proposes that there is an influence of perceived behaviour control towards intention to respond to cybercrime activities such as phishing emails.

The following definitions are drawn for the dependent variable of TPB that is applied to the current study. In the current study, intention represents an individual's preference and

likelihood to undertake any information security behaviour or cybercriminal activities (e.g., phishing). Intention is a pointer that demonstrates the level of effort a person is willing to put forward while performing a behaviour (Ajzen, 1991). Intention captures the motivating factor that influences the behaviour of an individual (Ajzen, 1991). The motivating factors are represented by the three independent factors (ATT, SN, and PBC) (Randall and Gibson, 1991).

As per the theory, intention (e.g., 'I will stop replying to unknown emails') is determined by attitudes toward the behaviour (e.g., 'replying to unknown emails is problematic'), subjective norms (e.g., 'most people such as myself do not reply to unknown emails'), and PBC (e.g., 'I am sure I can control replying to unknown emails') (Teodor et al., 2017). Fishbein and Ajzen (1975) confirmed in the progress of TRA that intention is a strong factor of real behaviour. In the current study, it has been recommended that an individual's attitudes toward the behaviour, subjective norms, and PBC have a direct relationship to the individual's intention to respond to cybercrime activities, such as phishing emails.

3.3 Research Hypotheses

After studying and explaining TPB and SEPS, the researcher derived the following hypotheses for the current research. So, the hypothesis formation for this research is based on the constructs of (TPB and SEPS) demonstrated in the previous chapter.

Table 2 : Research Questions and Hypotheses

Research Question	Hypothesis
To what extent ATT, SN, and PBC impact the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS?	H1: Saudi Arabian undergraduate students' ATT factor impacts the behavioural intention to respond to phishing emails under SEPS.
	H2: Saudi Arabian undergraduate students' SN factor impacts the behavioural intention to respond to phishing emails under SEPS.
	H3: Saudi Arabian undergraduate students' PBC factor impacts the behavioural intention to respond to phishing emails under SEPS.

3.3.1 Impact of (ATT) on (IN) to respond to phishing emails under SEPS

It has been explained earlier that attitude represents the individual's belief towards a specific behaviour, to determine if the condition is good or bad, favourable or unfavourable, positive or negative. In other words, the attitude is considered as the evaluation of thoughts,

actions, objects, or people's behaviour, whereby the intention of an individual is a derivative of the attitude they have towards a given activity (Ajzen, 1991; Leonard et al., 2004; Luenendonk, 2019). For instance, if a person believes that a particular behaviour yields positive or favourable results, they are more likely to adopt that behaviour.

In terms of phishing, consider a scenario, where an individual receives a fake email from social media informing them about an illegitimate activity on their account, which led to the closure of the account, and requesting an action via a link. There is a chance users might panic and click the link. Here, the individual might respond based on their belief and attitude, and not consider the consequences of their actions. However, the user might consider questions like, is this email favourable or unfavourable, are such emails useful or not useful, or are such emails important or unimportant? In this first determinant, attitude, a concept is evaluated to study the positive or negative performance of a user's behavioural interest.

The attitude can influence individual intention by rising the motivation of humans to involve in a certain behaviour (Smart, 2012). It has been indicated by Harding et al. (2007) that intentions are determined by the significant belief that arises from the attitude. In addition, Stone et al. (2010) found something similar. An attitude is a way or method adopted to respond to performing certain behaviours, and does not include a generic response. This means that humans are more probable to respond to emails where anticipated outcomes are favourable and predictable, and are less likely to engage in responding to emails whose outcomes are unfavourable and less predictable.

The effect of attitude in information security studies has demonstrated support for a particular behaviour pattern, as demonstrated by many researchers. An example is the influence of attitude on information security policies compliance intention (Bulgurcu et al., 2010; Ifinedo, 2011; Sommestad et al., 2015). There has been immense support between the attitude and anti-spyware adoption (Dinev and Hu, 2007; Lee and Kozar, 2008), in regard to online privacy protection strategies (Yao and Linz, 2008), keeping the anti-virus software updated (Ng and Rahim, 2005), and adopting firewalls (Kumar et al., 2008), as well as using strong secure passwords (Zhang and McDowell, 2009). Other studies, such as Anderson and Agarwal (2010), determined that the attitude factor is related to intention, as it promotes security-related behaviour to protect one's computer from cybercriminal activities. Based on the rich supply of studies

supporting the influence of attitude on user intention, it seems to be a significant factor in information security behaviour.

In TPB, attitude is said to have a strong impact on intention (Ajzen, 1991). This is provided and well supported by Ajzen in his work, followed by other theories such as TAM (Bagozzi and Yi, 2012) and TRA (Fishbein and Ajzen, 1975). Lebek (2014) demonstrated that out of ten information technology studies, eight apply TPB and show a significant relationship between attitude and intention. Further, six of these studies demonstrate a strong correlation at the level of $p < 0.01$. Even in the non-information technology-related studies, eight out of ten cases demonstrated attitude as a crucial predictor of intention (Ajzen and Klobas, 2013; Ajzen and Sheikh, 2013; Castanier et al., 2013; Dawson et al., 2014; Efrat and Shoham, 2013; Greaves et al., 2013; Tipton, 2014; Zemore and Ajzen, 2014).

3.3.2 Impact of (SN) on (IN) to respond to phishing emails under SEPS

SN is another construct in TPB and is described as a belief where most individuals agree or refuse a particular behaviour (Azjen and Fishbein, 1980). SN takes into account the opinions of other people like friends and family, who agree or disagree with a certain behaviour. In the situation where a person receives an email from an inconsistent source, the person might take into account the opinion of those important people, such as family or friends, not to believe the content of such forms of communication. It has been mentioned by Blythe (2015) that if a person thinks that pertinent others are following security steps or recognise that others anticipate them to follow the steps, they are more probable to undertake the security steps. To sum up, ‘subjective norms’ refers to the belief that others approve or disapprove of a given behaviour. It takes into consideration friends and family’s views before engaging in any behaviour.

An example of subjective norms in terms of phishing would be an email from a reputed firm, requesting personal information. In this scenario, the user will consider the opinions of family and friends – did they receive such an email before, did they respond to it, how highly have they spoken about the organisation, and so on. Here, the individual takes into consideration the views and beliefs of others, rather than making their own decisions (Ryan, 1982; Sheppard et al., 1988).

TPB illustrates that the stronger the subjective norm, the stronger the intention of the person to behave well. Some studies demonstrate a significant relationship between the subjective norm and intention (Meiriana et al., 2018). Ajzen and Driver (1992) put forth a correlation between subjective norms and behavioural intention. This is a crucial factor, as it proposes a direct impact

of subjective norms on behavioural intention (Chao, 1998). Bock and Kim (2002) and Ryu et al. (2003) introduced the effect of subjective norms on behavioural intention, as the individual is more concerned about the views and perceptions of family and friends.

Several studies in information security have focused on individuals' perceptions of what they believe significant people anticipate of them, and support the influence of SN on security behaviour (Bulgurcu et al., 2010; Ifinedo, 2011; Ifinedo, 2012; Safa et al., 2015; Siponen et al., 2010; Sommestad et al., 2015). Additionally, some studies have identified subjective norm as the second most major construct (Ajzen and Klobas, 2013; Ajzen and Sheikh, 2013; Castanier et al., 2013; Chan and Bishop, 2013; Chen and Tung, 2014; De Leeuw et al., 2015; Donald et al., 2014; Greaves et al., 2013; Mullan et al., 2015; Tipton, 2014). Research discussing customer behaviour has also supported the role of SN, in the intention to use anti-spyware software (Lee and Kozar, 2008), and in the intention to use firewalls (Ng and Rahim, 2005). Therefore, subjective norms seem to be a significant element of security behaviour.

3.3.3 Impact of (PBC) on (IN) to respond to phishing emails under SEPS

PBC is the third construct of the TPB and is defined as an individual's perception of difficulty or ease towards a certain behaviour (Ajzen, 1991). PBC proposes that the greater a person's belief in regard to the resources and chances to execute certain behaviour effectively, the more they will intend to do the behaviour (Ajzen, 2002). Consider a scenario in terms of phishing, where an individual receives an email from a reputed organisation; if this is presented to individuals with PBC, there are high chances the individual might consider re-evaluating their own response, or determining how easy it is for them to take an action.

Many studies have reported that this new component, PBC, has the ability to anticipate the behavioural intention and the individual's behaviour (Ajzen, 1991; Armitage and Conner, 2001). In a study conducted by Safa et al. (2015), the aim was to alter individuals' behaviour to aware care behaviour in the information security area. The study found that ATT (towards information security) and SN have a significant influence on individuals' behaviour, while PBC does not have an impact on individuals' behaviour. However, several studies in information security supported the influence of PBC on user intention to perform a certain behaviour. For example, it has been mentioned by Blythe (2015) that support has also been discovered for a relationship between PBC and being careful with email attachments (Ng et al., 2009), anti-spyware adoption (Liang and Xue, 2010), virus defence behaviours (Lee et al., 2008), using a firewall (Ng and Rahim, 2005), and

complying with password guidelines (Mwagwabi et al., 2014). Based on the existing studies, PBC seems to be a significant factor in security behaviour.

3.4 Chapter Summary

This chapter discussed the research hypotheses of the current study and the influence of the TPB factors on individuals' behavioural intentions. The current study focused on phishing attacks and examines the impact the TPB factors have in predicting user behavioural intention to respond to phishing emails. A number of hypotheses, testing the effect of the TPB on the individuals' behavioural intention in responding to phishing emails under SEPS among Saudi undergraduate students, were proposed in this chapter. Three hypotheses were developed to test the impact of TPB on the individuals' behavioural intention in responding to phishing emails under SEPS. The following chapter discusses the research methodology used in this study.

CHAPTER 4. Research Methodology

4.1 Introduction

Research methodology is a systematic method to discover an answer for research questions, a solution to a problem. Michael Crotty (1998, p. 3), defined research methodology as 'the strategy, plan of action, process or design lying behind the choice and use of particular methods and linking the choice and use of methods to the desired outcomes'. In addition, research methodology explains and develops various steps required in attaining the objectives of the research (Johnson and Christensen 2004; Tashakkori and Teddie, 1998). The 'research onion' is a concept developed by Saunders et al. (2009), which explains various steps required to carry out the research. The research onion is presented in Figure 5 with minor changes in the presentation format. The 'research onion' is a tool for researchers to plan the research. The previous chapter discussed an inclusive review of existing studies related to the current study. This chapter outlines the research methods used in answering the questions of the research, alongside various research methodologies, and explanations for using those methodologies.

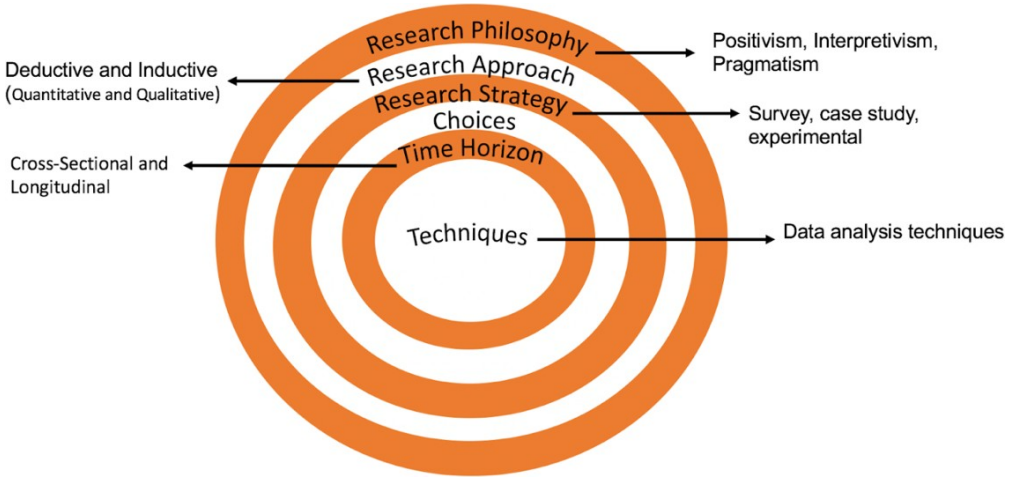


Figure 5 : Saunders' Research Onion

4.2 Research Philosophy

The first level of Saunders' research onion is Research Philosophy. It has been mentioned by Alkahtani (2018, p. 61) that according to Saunders et al. (2007), the philosophy of the research is 'a development of new knowledge and nature of knowledge'. In addition, it has been stated by Klenke (2008) that while doing research it is significant to select the correct research philosophy, since a scholar's psychological suppositions are extremely essential in research. The philosophy of the research should be recognised in the early phases, as it presents and explains the researcher's

choice of data gathering techniques, appropriate strategy of the research, and the approaches used to gather, analyse, and verify the data (Crossan, 2003). According to Saunders et al. (2009), positivism, interpretivism, realism, and pragmatism are common philosophies in research. The majority of Information Systems (IS) research is based on either positivist or interpretivist research philosophies (Galliers, 1992; Orlikowski and Baroudi, 1991; Wynn et al., 2012).

4.2.1 Positivism

Positivism philosophy aims to clarify and empirically confirm current models via formulating hypotheses than can be clarified, mostly in quantitative methods, and via direct observation and generalising the results to larger populations (Guba and Lincoln, 1994). It has been stated by Alkahtani (2018, p. 61) that positivist philosophy can be defined as 'approaches that are founded on a belief that the study of human behaviour should be conducted in the same way as studies conducted in the natural sciences'. In addition, it has been stated by Jackson (2001) that since the late 1970s, the positivist philosophy has been commonly used in most information system studies. Positivism has been identified by several research studies as a crucial information system approach (Themistocleous 2002; Yin 1994). Further, Orlikowski and Bardoudi (1991) supported the positivist approach, as it is used by around 70% of researches in the leading United State information system journals.

The positivist philosophy normally pursues the authentic objective of increasing the phenomena' perception through the researcher's use of independent observation, test, or experience of theories (Galliers, 1992; Myers, 1997). Additionally, the positivist approach (Neville, 2007; Orlikowski and Baroudi, 1991) includes hypothesis, measurements, examinations, deductions, confirmations, and recommendations, including an approved analysis process (Conford and Smithson, 1996; Crossan, 2003).

4.2.2 Interpretivism

Interpretivism philosophy is the opposite of positivism philosophy. According to Badewi (2013), the interpretivism philosophy is based on understanding, watching, and examination, and after that analysis and building of social cases. Table 3 shows a comparison between positivism and interpretivism, in terms of what the scholar should do when selecting one of these philosophies and the approaches used (Easterby-Smith et al., 1991).

Table 3 : A Comparison between Positivism and Interpretivism (Easterby-Smith et al., 1991)

	Research Philosophies	
	Positivism	**Interpretivism**
The researcher should:	Formulate and test hypotheses.	Construct theories and model from data.
Approaches used are:	Deductive approach.	Inductive approach.
	Quantitative approach.	Qualitative approach.
	Using large samples.	Using small samples.

It has been mentioned by Thompson (2015) that positivism prefers using quantitative research methods (e.g., surveys and structured questionnaires) while interpretivists prefer using qualitative approaches (e.g., unstructured interviews or participant observation). The current research aims to evaluate the factors of the Theory of Planned Behaviour (TPB), to explain the behavioural intentions of Saudi undergraduate students when responding to phishing emails under Social Engineering Persuading Strategies (SEPS). Using positivist philosophy is more suitable for the current research for the following reasons. The first reason is, the current research used quantitative research methods, which is more appropriate for positivist philosophy (discussed in the next section). Secondly, the current research uses the deductive research approach, which is more suitable for positivist philosophy, as mentioned by Jacob (2013, p. 23) – '[d]eductive research is the method used for positivism philosophies' (discussed in the next section). Thirdly, the current research used cross-sectional studies (discussed in section 4.7), which is an appropriate method for positivist philosophy (Alkahtani, 2018). Lastly, positivist philosophy is suitable for testing hypotheses, and in the present study the researcher has tested the hypothesis of the model.

4.3 Research Approach

Research design presents an outline of the approaches to be followed, so that it can acquire the information that enables the answering of the research questions (Saunders et al., 2016). The main research approaches adopted by researchers in different fields include deductive/inductive and quantitative/qualitative (Easterby-Smith, 1991; Saunders et al., 2009). The following sections discuss the different approaches used for the current research.

4.3.1 Deductive and Inductive

Deductive and inductive research has been studied by several researchers (Cavaye, 1996; Hussey and Hussey, 1997). Deductive research begins with a social theory that requires further analysis, and tests the implications of the data gathered. This means the research transfers from a more overall level to a specific level. A deductive approach to research is typically related to

scientific investigations. The researcher examines the existing theories, hypotheses, and scenarios, and tests the hypotheses that are discovered or developed from those theories.

Therefore, deductive is defined as ‘top-down’; it starts with a general subject and moves towards a specific area of study. It begins with the theory, defines hypotheses, and examines observations and finally confirmation. This enables the scholar to apply the theories (Hussey and Hussey, 1997).

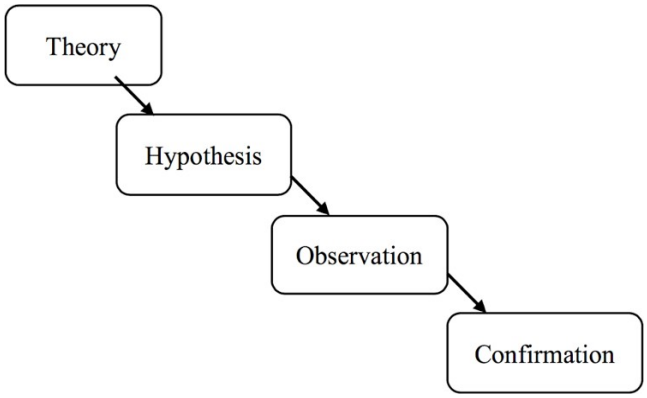


Figure 6 : Deductive Approach (Trochim, 2001)

In an inductive research approach, a researcher initiates the research by gathering data that is related to the research topic. As a substantial amount of data is gathered, the researcher focuses on analysing the data from a macro level. During this stage, the researcher searches for patterns in the gathered data and works to develop a theory that can explain the discovered patterns. Therefore, when a researcher takes an inductive approach, the process begins with a set of observations and moves to a more generalised set of propositions regarding the research. In other words, research begins with data or specific research, and slowly moves towards theory or generalised sets of propositions.

Therefore, the inductive approach is the reverse of the deductive approach, as it begins with the particular and proceeds to the general. It starts from accurate observations, and moves to defining hypotheses and evolving theories (Hussey and Hussey, 1997).

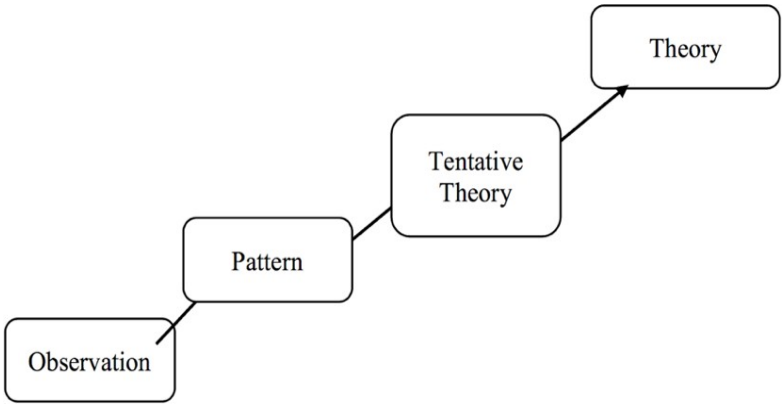


Figure 7 : Inductive Approach (Trochim, 2001)

This thesis uses a deductive approach, due to the fact that it tests a theory. The aim of this thesis is to evaluate the Theory of Planned Behaviour (TPB) with respect to individual behavioural intention when responding to phishing emails under Social Engineering Persuading Strategies (SEPS).

4.3.2 Quantitative and Qualitative

A quantitative approach is a powerful tool for data gathering, widely accepted and utilised in social sciences to study issues such as culture and human behaviour (Babbie, 1998; Bond, 1988; Cameron and Quinn, 1999; Hofstede, 1980; Straub et al., 2001). According to Alkahtani (2018, p. 65), '[q]uantitative approach is based on measurement and analysis of relationships between variables'. Casebeer and Verhoaf (1997) also indicated that the quantitative research approach is usually used when the scholar seeks to examine relationships between factors. Furthermore, Fitzgerald and Howcroft (1998) mentioned that quantitative approaches use statistical and mathematical tools in order to identify facts and relationships among constructs within an area of study. The emphasis of the quantitative approach is on gathering and examining numerical data; it focuses on assessing the scale, frequency, and range of phenomena (Neville, 2007). In addition to this, the quantitative approach is generally highly comprehensive and structured, and outcomes can easily be gathered and presented statistically (Neville, 2007). Quantitative methods originate from scientific research in order to investigate natural phenomena, which is accomplished via data gathering and analysis methods from fieldwork. When the goal is to explain phenomena, Leedy and Ormrod (2015) referred to quantitative research methods as the best approach to study the relationships among measurable variables. In quantitative research, researchers commonly use data-gathering methods that are more structured like structured interviews or surveys (Casebeer and Verhoaf, 1997). Shuttleworth (2008) stated that quantitative is an excellent method for

finalising results and proving or refuting a hypothesis, and it has not changed for centuries. After a statistical analysis of the results, a comprehensive answer is reached, and the results can be debated and published (Al Izki, 2018).

Qualitative methods originate from social science research to study social phenomena, which is accomplished via interviews, case studies, action research, and ethnography. Table 4 compares Quantitative and Qualitative Research Methods (MacDonald et al., 2011; Neuman, 1997; Neville, 2007).

Table 4 : The Differences Between Quantitative and Qualitative Research (MacDonald et al., 2011; Neuman, 1997; Neville, 2007)

Quantitative Research Approach	**Qualitative Research Approach**
This aims to test hypotheses from theories.	The aim is to summarise and detect data.
The data form is numbers from accurate measurements.	Quantification is used, as the data forms are documents, words, observations, and transcripts.
This is a more deductive approach, as the theory is fundamental.	Qualitative research uses an inductive research approach.
It can be replicated, as the research procedures are standard.	It is difficult to replicate, as the research procedures are fixed.
Structured data collection.	Unstructured data collection.
Regarding the sample, generally a large number of cases representing the population of interest. Respondents are chosen randomly.	Regarding the sample, mostly a small number of non-representative cases. Respondents are chosen based on their experience.
Statistical analysis.	Interpretive analysis.

The quantitative method is used in the current research, as it aligns with the deductive method. A quantitative perspective is based on the positivist philosophy, and it is hypothetical, in that it usually starts with research questions or hypotheses based on the analysis of the literature (Patel, 2015). The current research uses positivist philosophy which, again, best aligns with the quantitative method (Johnson, 2017; Tavakol and Sandars, 2014a). Further, this method is more appropriate for the present study due to the fact that it emphasises testing hypothetical generalisations (Hesse-Biber and Leavy, 2011). Additionally, the quantitative approach is more focused on gathering objective and numerical data about subjects' attitudes, beliefs, subjective norms, and perceptions (Denscombe, 2007), which is a better fit for the present research. Further, the most popular methodology for information security applies quantitative methods for socio-behavioural theories (Alaskar et al., 2015). Therefore, in the current research, using a quantitative approach is more suitable than a qualitative approach.

Considering the theoretical perception, an existing theory is applied as a guiding framework for socio-behavioural studies (Lebek et al., 2014). By applying existing theories, studies design the approach towards a subject using a quantitative approach (Turner et al., 2013). A theory consists of independent and dependent factors. Theorists suggest that in some ways the independent factors affect the dependent. In these scenarios, the researchers focus on gathering data on the independent variables. Further, to establish the foundation and discussion for the study, the statistical analysis gathers the data to establish the effect independent variables have on the dependent variables.

According to Daxini (2019), the majority of previous studies which use TPB (Ajzen, 1991; Hyland et al., 2018; Jiang et al., 2018; Lalani et al., 2016; Micha et al., 2015; Morais et al., 2018; Senger et al., 2017; Zeng and Cleon, 2018; Zeweld et al., 2017) adopted a structured survey research strategy (discussed in section 4.5) to gather quantitative data from respondents. This is suitable because the aim of the current research is to evaluate the TPB to explain the behavioural intentions of users when responding to phishing emails under SEPS.

4.4 Research Purpose

The research purpose is to determine the methods and protocols used to successfully answer the research questions (Saunders et al., 2009). There is a wide agreement among academics with regard to research purpose being classified into three main categories – exploratory, descriptive, and explanatory (Robson, 1993; Saunders et al., 2009). However, these might be changed and altered during the research process, which could have more than one purpose; and this is pointed out by Robson (2002).

Exploration is normally an initial stage in a series of phases that are required in a study. These phases are required as it enables the researcher to study the design, determine further execution of the undertaken research, discover unique features regarding a study, and develop hypotheses to be investigated (Grinnell, 2001). The exploratory nature of research can be understood from the descriptor; if researchers are going to perform exploratory research, they are going to explore. In exploratory research, a researcher can take some well-defined theories and try to apply them to a particular phenomenon to see if these theories fit the phenomenon (MeanThat & Authentic Data Science, 2016). For example, a researcher can take a socio-psychological theory and try to apply it to phishing attacks. Moreover, exploratory research is suitable for persistent phenomena, that enable testing the feasibility of a detailed study, and developing different ways

that can be used for the study to better generate specifically focused research questions and hypotheses that might enable any further investigations (Babbie, 2013; Royse, 2011). According to Alkahtani (2018), exploratory research takes place when there are few or no previous studies existing. Additionally, Alkahtani (2018) stated that exploratory research is the development of hypotheses.

While exploratory research concentrates on exploring a certain social phenomenon and asking questions about that phenomenon (Johnson and Clark, 2006), descriptive studies are preferred to demonstrate a comprehensive picture of the phenomenon (Gray, 2014). The main aim of a descriptive study is to deliver details on a particular situation, human being or event to demonstrate the relation between various objects and how frequently and naturally they occur (Blumberg, Cooper and Schindler, 2005). However, descriptive studies cannot provide in-depth clarification of the occurrence of an event, and are more suitable for researches that are yet to be explored, and relatively newer than existing research (Punch, 2005). Descriptive studies are often criticised for not being able to explain why a particular phenomenon has occurred. Therefore, if a situation has in-depth information regarding an event, an explanatory or exploratory research approach is preferable.

Explanatory research is defined by Glicken (2003) as the type of research that tries to provide significant and precise conclusions from the considerable amount of information already available. Explanatory research is more focused on the root cause of, and reasons for, the occurrence of a problem or issue. It provides evidence that supports or disagrees with an explanation or prediction. This type of research is undertaken to conduct, discover, and report any existing relationships between various sides of the phenomenon in any given research. In addition, this type of research tends to be deductive and quantitative in nature. Therefore, explanatory studies explain the relationships between variables of the research, and explain why things happen. For the current research, using both exploratory and explanatory methods are appropriate as it uses a well-defined socio-behavioural theory, namely TPB, and applies it to responding to phishing emails. The main aim of the current research is to evaluate TPB to explain individual behavioural intention when responding to phishing emails.

4.5 Research Strategy

In order to define the questions of the research and achieve the objectives of the research, a general plan called the research strategy is used (Saunders et al., 2009). In addition, a research

strategy is a generalised plan for the overall research process direction (Saunders et al., 2009). The research strategies include different types, which are case study, experimental, ground theory, action theory, and survey (Alkahtani, 2018; Robson, 1993).

By using different data collection techniques in a natural setting, case studies focus on the intricate clarification of either single-case or multiple related cases (Hesse-Biber and Leavy, 2011). On the other hand, experimentation in an unnatural setting focuses the inquiry on empirical methods (Denscombe, 2007). The ground theory is an inductive approach, with the aim to make or progress a theory from gathered data (Alkahtani, 2018). In addition to this, according to Alkahtani (2018), action research solves an issue by engaging the studied population to work together as a group to improve their method of handling problems. According to (Neuman, 2014) survey is the most widely data-collecting research strategy. It is a deductive approach and refers to the gathering of information from a sample of individuals via their responses to questions (Schutt, 2001). In the quantitative approach, the survey is a common method and is often used in discovering individuals' attitudes; it is also used to allow the researcher to recognise and clarify the variability in phenomena, and to study and clarify the correlations between variables (Saunders et al., 1997). Additionally, it delivers quantitative or numeric descriptions of attitudes or views of a population, by examining a sample of that population (Creswell, 2014). It has been stated by Schutt (2001) and Saunders et al. (1997) that survey research through questionnaires is often the only means existing for evolving a representative picture of the attitudes of a large population. In order to test the suggested hypotheses in the present study, case study, experimentation, ground theory, and action research would seem unsuitable; while the survey strategy is more suitable for testing the proposed hypothesis (Smith, 2015). In addition to this, researchers prefer quantitative approach surveys (i.e. measuring main variables and analysing results with quantitative statistical techniques), and connecting this quantitative information with concepts and theory (Al Izki, 2018); therefore, using a survey strategy is more suitable for the current research.

Although the survey strategy has some disadvantages (Denscombe, 2007), as it concentrates on data accumulation and data description rather than on theory, it has more advantages, as mentioned by Fricker (2008). Survey's advantages include less cost and less effort to manage, better response, and greater precision. Collis and Hussey (2009) also stated that surveys can be conducted in a time-constrained environment and are cost-effective. Moreover, surveys through the internet provide access to a wider audience to collect samples, which results in

improved quality of data and more generalised research findings (Robson, 1993). This enhances the flexibility of administration and questionnaire collection (Bryman and Bell, 2007). The subsequent analysis and data interpretation facilitated the implementation of statistical procedures by using a specific study to understand individuals' attitudes, perceptions, and subjective norms toward the behavioural intention of Saudi Arabian undergraduate students to respond to phishing emails under Social Engineering Persuading Strategies (SEPS). To sum up, the survey approach helped to gain insight into individuals' opinions and beliefs in regard to responding to phishing emails.

4.6 The Research Instrument

4.6.1 Data Collection Method for Survey Research

The empirical data-gathering technique is followed to determine the most appropriate research strategy (Yin, 1994). In data collection, it is significant to differentiate between primary and secondary data. Primary data are gathered by a scholar for a particular goal; in the case of the current research, the academic collected data from university undergraduate students with the purpose of analysing the factors that influenced the students' behavioural intention in responding to phishing emails. On the other hand, secondary data are data that previously available, and were gathered by others for different purposes, e.g. data for government databases and organisation documents.

It has been stated by Sapsford (2006) that there is no single greatest method of data gathering; the technique selected depends on the nature of the research question, and the exact questions the academic wants to ask respondents. In addition, the purpose of all such techniques is to acquire reliable and valid data. Hence, a decision is required about the appropriate data type, in regard to research procedure and theoretical framework.

Researchers obtain data for their studies by choosing self-administered questionnaires or interviewer-administered questionnaires. Self-administered questionnaires are finished by the respondents, while interviewer-administered questionnaires are logged based on the respondents' answers in interviews (Mitchell and Jolley, 2013). The current study adopted self-administered questionnaires as the main data-gathering instrument, because of time and monetary constraints. The key advantage of using this type of questionnaire is that it allows the gathering of data from a larger audience in a timely manner (Saunders et al., 2009). In addition, questionnaires are the most

common method of data collection and provide academics with quantitative data (Dornyei, 2001, cited in Alshumaim and Alhuassan, 2010).

In addition, self-administered questionnaires allow for anonymity, and help obtain honest answers, quickly, easily, and affordably (Vaus, 2002). The respondents are confident and comfortable to express their perspectives, as it is an anonymous survey and this eliminates social bias (Gosling et al., 2004). During the collection process, there are few ethical issues, because there is no communication between the respondents and the researcher. There is a chance that the respondent might not be heard or studied carefully, simply because there is no interaction (Mitchell and Jolley, 2013). Basically, the researcher cannot help the participant with any unclear questions. To overcome this hurdle, the questions are designed to be simple and understandable. The other disadvantage is the low return rate of the questionnaire (Mitchell and Jolley, 2013). Therefore, the researcher's questionnaire was short, simple, and easy to understand, thus increasing the rate of participant response (Vaus, 2002). Table 5 discusses the advantages and disadvantages of using a questionnaire (McClelland, 1994; Wright, 2005).

Table 5 : Advantages and Disadvantages of Questionnaire (McClelland, 1994; Wright, 2005)

Advantages of Questionnaire	**Disadvantages of Questionnaire**
Attitudes, intentions, and motives included.	As there is no human interaction involved, a two-way communication cannot be established to verify/clarify the questions.
Anonymity.	Due to lack of interactions, the data collection cannot be edited or changed.
Survey can be conducted remotely.	Cannot be modified or changed through data collection, hence it is not a flexible tool.
No time pressure on respondents.	The response rate could be low, due to some participants choosing not to answer the questionnaire.
Enables gathering responses from wider audiences in a constrained time frame.	The queries regarding the questionnaires cannot be clarified; as a result, a lot of assumptions might be made by the users.
Respondents can complete the questionnaire in less time.	Needs large sample responses.

4.6.2 Survey Design

A questionnaire is usually utilised in quantitative research for data gathering, with the outcome consisting of numeric descriptions of trends, attitudes, and target population opinions (Al-Izki, 2018). It is imperative to have a well-designed questionnaire in order to acquire valid and reliable data. According to Mitchell and Jolley (2013), a well-designed questionnaire is not only easy to complete, but it is also easy for researchers to interpret and analyse. Data collected through

questionnaires enable the researcher to accomplish the aims and objectives while taking statistical requirements into consideration about the sample population's nature and attributes (Saunders et al., 2009).

It has been stated by Cohen et al. (2007) that researchers should use accurate phrasing in the questionnaire; not complicated language and words, in order to permit participants to completely understand the questions, and to ensure the scholars can get the needed information. Meanwhile, unclear questions should be avoided, in order to prevent possible confusion.

In the current research, the type of question used was closed-ended, which presents options for the provided questions. The respondent chooses from the provided options when answering the questions. Using closed-ended questions increase the rate of response, as it does not require writing any opinions, and it is easy to understand (Denscombe, 2007). Moreover, it enables the coding and decreases the chances of editing the captured data, thus avoiding the cost and time which might be required by data processing and analysis (Vaus, 2002). The answers were evaluated based on the Five Likert scale, which was initiated by Rensis Likert in 1932. In addition, this technique evaluates the attitudes of the survey respondents and is widely used in research. The scale consists of five responses: Strongly Disagree=1; Disagree=2; Neutral=3; Agree=4; Strongly Agree=5. The survey questions in the current research offer answers in the range of 1-5. The participants were required to choose from the provided 5 answers to each question.

The data collected from the survey was considered for bias and dealt with in the following ways. The responses were taken from different schools (engineering, medicine, business, and computer science) and were not biased toward one school. In addition, the survey questions were framed in a clear, concise, and understandable manner to provide proper information to the participants as they were from different fields of education and any hypothetical questions were avoided.

The development of the questions for this survey was based on the literature, and the guidelines provided by the author of TPB, Icek Ajzen. The survey questionnaire studied the factors that influenced behavioural intention of Saudi Arabian undergraduate students to respond to phishing emails under SEPS. The survey consisted of two sections, as described below.

4.6.2.1 Demographic Factors

This was the first section in the survey, and was designed in order to collect demographic information about the participants. It comprised three questions covering age, gender, and field of

study. The first question asked the participants to identify their gender. The second question asked the participants to identify their ages. The age group divided into four groups: younger than 18; 18-21; 22-24; and 25 or older. The third question asked the participants about their field of study. The field of study responses were Business Administration, Computer Science and Information Technology, Engineering, or Medicine. The survey questions are available in Appendix A.

4.6.2.2 Phishing Emails under Social Engineering Persuading Strategies (SEPS)

The second section of the survey, Phishing Emails, consisted of nine different phishing emails under SEPS; three emails each for the Authority strategy, Social Proof strategy, and Scarcity strategy. There were ten questions for each email type, to test the influence of the TPB factors: ATT (three questions); SN (two questions); PBC (three questions); and IN (two questions). The survey questions are available in Appendix A and explaining each scenario is available in Appendix F.

Attitude questions:

- I believe responding to these types of emails is good for me.
- I believe responding to these types of emails is useful for me.
- I believe responding to these types of emails is important for me.

Subjective Norms questions:

- People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails.
- People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organisation and think I should respond to these types of emails.

Perceived Behavioural Control questions:

- If I want to, I could seek the advice of people.
- For me, the decision to respond or take action is my own.
- For me, the decision to respond or take action is easy.

Intention questions:

- I would respond to the email.
- I intend to respond to the email.

4.6.3 Survey Sampling

According to Bhattacherjee (2012), a population consists of various analyses with different features the researchers aim to examine. The unit of analysis could be a country, company, group,

person, or any other unit that a researcher wants to study. It is not possible to gather data from all the existing sources to solve research problems and discover solutions (Graziano and Raulin, 1997). Therefore, it was suggested to take smaller units (which are also referred as samples) of data from any given population (Al-Izki, 2018).

The participants in the present study were selected to evaluate the impact of TPB factors on behavioural intention when responding to phishing emails under SEPS. In addition, the targeted participants were all Saudi undergraduate male and female students studying at King Faisal University (KFU).

KFU is located in the eastern province of Saudi Arabia, in a city named Al-Ahsa which is about 24% of the Saudi Kingdom. It is one of the largest educational bodies in the eastern province of Saudi Arabia because of its diversity, knowledge, development, and improvement centres for professional and administrative expertise. So far, the university has offered 47 different Bachelor's level programs, more than 40,000 students are registered in the bachelor programs, and different research units that comprise scientific and applied fields with 11 supporting deanships and 26 administrative centres. (KFU, 2022)

As mentioned earlier, university undergraduate students have been identified as the users who are most susceptible to phishing emails (Kumaraguru et al., 2010; Sheng et al., 2010; Whiteman, 2017). Besides, Alsanad (2018) mentioned that 40% of university students in Saudi Arabia had experienced victimisation. Moreover, the cybercriminals hacked KFU database in 2019 (Nabbout, 2019).

All of the participants in the current research were informed that their contribution was completely voluntary. In addition, the participants were able to withdraw at any time. Additionally, in order to protect the rights of the sample contributors, a consent form was sent to them, and the participants were required to sign the form, which ensured their anonymity and confidentiality. The consent form is available in Appendix B. Moreover, the participants were informed that there were no known dangers related to taking part in the study.

4.6.4 Survey Distribution

The current research employed online surveys using Google Forms as the use of an online survey instrument via a web-based survey platform was a suitable data gathering technique for the current study, since it delivered an appropriate method for collecting the wanted target population in a short period. In addition, this technique also made it appropriate for the respondents to take

part in the survey, as their answers could be logged and gathered conveniently, from their home computers.

4.6.5 Survey Data Collecting and Data Coding

The data was collected through Google Forms and any missing data were checked and cleaned by the researcher, before uploading the data to the SPSS software. SPSS is a computer software statistical package tool, used to analyse, retrieve, store, and code the data collected through surveys. In addition, to guarantee the data were properly inserted into SPSS, the data were cleaned again via a manual process of error checking. The researcher further verified the number of valid, missing cases and labels for each factor before analysing the data. This included running frequency tables for all variables, to verify data accuracy, as suggested by Pallant (2010). The data were cleaned by removing the unanswered or skipped questions. In addition, descriptive statistical tests were used in analysing these questions. This type of analysis offers information about percentages and frequencies.

4.7 Data Collection Timeframe (Time Horizon)

Time Horizon is one of the layers in the research onion presented in Figure 5. Time Horizon can be divided into two types – Cross-Sectional and Longitudinal. Cross-Sectional focuses on the data collation at a given point in time (Gray, 2014). Furthermore, this type focuses on the time frame, which is limited (Saunders et al., 2009). However, the longitudinal type focuses on the data collected within an extended time period (Gray, 2014). Moreover, it focuses on observing the theory or experiment for a long time period (Saunders et al., 2009).

The current research used a cross-sectional time horizon, since the research was based on a limited time frame while being independent of the research strategy (Saunders et al., 2009). Additionally, cross-sectional studies are concise, simple, and affordable (Johnson and Clark, 2006), while longitudinal time frames are unrealistic and inapplicable (Saunders et al., 2009). One might argue that data collection takes weeks; however, once the data are reported and analysed by the researcher, the time horizon is classified as cross-sectional.

The other reason for using a cross-sectional time horizon was that the current study compared data collected from a wide audience, with no change over time (Gray, 2014). In a longitudinal study, the data not changing might be considered as a major failing; changes are the key premise of longitudinal studies (Easterby-Smith et al., 2012). In simple terms, cross-sectional data are not measured by social phenomena that arise before or after data collection. Although the

cross-sectional time frame has its limitations, it has advantages that are useful for this thesis, which provide insight into TPB's independent and dependent factors under SEPS, and set a foundation for future researchers to further analyse the responses.

4.8 Pilot Study

Fraenkel et al. (1993) noted that the pilot study can be defined as a small-scale study that is executed before conducting the real examination, with the aim of attempting to show any areas of fault or weakness in the research plan. Additionally, the pilot study can play a significant role, before conducting a large-scale study. In addition, in order to guarantee the questionnaire was well-designed, and to explore areas of improvement, a pilot study was used to analyse the questionnaire's quality (Hair et al., 2010). This helped the academics in measuring the reliability and validity of the survey (Saunders et al., 2012) and provided a mechanism for pre-testing the questions.

There are many advantages of applying a pilot study before implementing the main research. It has been indicated by Teijlingen and Hundley (2001) that carrying out a pilot study is very significant due to the fact that it can act as a warning device to display if there are any mistakes or unsuitability with the instruments of research. In addition, it has been demonstrated by Al-Sharif (2014) that the other advantages of conducting a pilot study contain guaranteeing that the procedures of the research are appropriate and applicable, creating a pure picture of the effort needed in the main study, and enhancing the research quality by evaluating its questions. Additionally, one more significant benefit of conducting a pilot study is to familiarise the academic with the processes of the research. Furthermore, all aspects of the pilot study assist the academic to be more self-assured and guaranteed that the tool assesses what it was intended to measure.

The pilot process was conducted on undergraduate students at KFU in Saudi Arabia, to study the impact of TPB factors on behavioural intention when responding to phishing emails under SEPS. The students were in their proprietary education years, and had a good understanding of the English language. Ten male and female students were selected, randomly, to give their views on the content of the survey. The researcher presented the three emails for each SEPS strategy (Authority, Social Proof, and Scarcity) together in one question, and then asked the participants to answer the ten questions measuring TPB factors. This raised concerns and confusion among the participants as the pilot questionnaire had three scenarios in one question and under them there were ten questions. The participants were not sure which question was for which presented

scenario. This resulted in the loss of the participant's focus in reading each scenario accurately leaving them doubtful and confused. Based on this feedback, the survey was changed to have one question for each SEPS email.

4.9 Statistical Techniques

Statistical techniques are tools that enable researchers to analyse data, test research hypotheses, and answer research questions. According to Saunders et al. (2009), the extant literature on research methods recommends that data analysis in a study should be conducted in a way that clearly reflects the responses of respondents and successfully answers the research questions. In the current study, to answer the research questions, the MLRA and CFA statistical techniques were used. In addition, in the current study, the data gathered from the survey questionnaire were analysed using a quantitative approach, in which well-known statistical software packages were applied, namely IBM SPSS version 28 and IBM Analysis of Moment Structure (AMOS), version 28.

4.9.1 Multiple Linear Regression Analysis (MLRA)

Multiple linear regression is a widely used multivariate regression process intended to measure several independent factors (or predictors) in order to account for the variance of a single dependent factor (Jung and Kim, 2014; Mertler and Reinhart, 2017). Pallant (2005) recommended multiple regression analysis as the most widely used technique, that enables one to understand the variance of the dependent variable and independent variable. Furthermore, the MLRA technique explains the unique variance of the dependent element by each independent variable (Pallant, 2005). MLRA is used to test the correlation between independent variables (predictors) and dependent variables (Nathans et al., 2012). In addition to this, it establishes a relationship between dependent and independent elements in order to predict independent elements' variances from the dependent variable (Mertler and Reinhart, 2017). It has been stated by Pallant (2005) MLRA is not only one method, but a family of techniques that can be used in exploring the correlations between one dependent factor and a number of independent factors.

MLRA was used in this study for several reasons. Firstly, to find the impact of the independent TPB factors on the dependent factor (Epule et al., 2011). Secondly, researchers frequently use MLRA in information systems studies in overall (Ayatollahi et al., 2013; Chen et al., 2014; van Deursen and van Dijk, 2013), and they suggested its use in studies investigating the Theory of Planned Behaviour (TPB) (Beville et al., 2014; Hankins et al., 2000; MacFarlane and

Woolfson, 2013; Sommestad et al., 2015; Tipton, 2014). Thirdly, MLRA is a common data analysis technique in similar present studies, applying socio-behavioural models to information security (Al-Mukahal and Alshare, 2015; John et al., 2015; Klein and Luciano, 2016; Said et al., 2014).

To analyse the data, IBM SPSS software version 28.0 (IBM Corp., 2021) was used, and the data were loaded to test the hypothesis for MLRA. As it best aligned with the current study's research question, the 'Enter' method (Mertler and Reinhart, 2017; Nathans et al., 2012) was used. In addition, to analyse and interpret the information, model summary, ANOVA, and coefficients tables were utilised. Furthermore, the model summary consisted of R, R squared (R2), and R squared adjusted (R2adj) values. The variance measurement values predicted the combination of how well the independent factors predicted the dependent factor (Nathans et al., 2012). R2 values, as per Lowry and Gaskin (2014), should be high, within the following ranges: for substantial, .75, moderate, .50, and weak, .25 (Hair et al., 2011; Sarstedt et al., 2014).

The ANOVA table helped in interpreting the linearity model degree, and importantly the model predicts the dependent variable. This is provided through the F test and significant values (Mertler and Reinhart, 2017). Said et al. (2014) and Sommestad et al. (2015) predicted the significance to be $p <= .05$. The coefficients table determined the coefficient beta value (B) to represent the gradient direction of the dependent and independent variables (Nathans et al., 2012; Nimon and Oswald, 2013). To enable the interpretation of each independent variable of the model, the table consisted of t and p values providing significant values for the coefficient (Mertler and Reinhart, 2017). In addition, it has been suggested by Lowry and Gaskin (2014), Said et al. (2014), and Sommestad et al. (2015) that coefficients should be substantial, with the value range of $p <= .05$.

The data analysis reports were descriptive table formats accompanied by scholarly debate, results clarification, and implications. In addition, the data analysis and interpretation of the results helped in the rejection or acceptance of study hypotheses. As the current study used TPB in explaining user behavioural intention when responding to phishing emails, multiple linear regression established a correlation between the independent factors (ATT, SN, and PBC) and the dependent factor (IN), to predict and explain the independent variables' variances from the dependent variable (Mertler and Reinhart, 2017).

4.9.2 Factor Analysis (FA)

FA is widely applied in several domains, like education, psychology, and information security, and is adopted as the method of choice for interpreting self-reporting surveys (Bryant et al., 1999). In addition, FA minimises a large number of elements into a smaller set. Moreover, FA provides constructive validity evidence of self-reporting measures (Gorsuch, 1983; Hair et al., 1995; Tabachnick and Fidell, 2001; Thompson, 2004). There are several tests used in FA, such as Kaiser-Meyer-Olkin (KMO) test, Bartlett's test of Sphericity, and Communality test. This will be discussed in the next chapter.

FA can be classified into two types – Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) (Williams et al., 2010). These methods are applied to research methods that either require confirmation for prior established theories, or the establishment of a correlation between the patterns or variables. EFA is used when there are no anticipations from the number or nature of elements. In addition, EFA allows the researcher to discover the key factors to invent a model from the large latent set of dimensions which are mostly represented by item sets (Pett et al., 2003; Swisher et al., 2004; Thompson, 2004). On the other hand, CFA, which belongs to the Structural Equation Modelling (SEM) family, is applied in testing a well-structured model. It is used to disapprove or approve the measurement theory. In addition, the Confirmatory Factor Analysis (CFA) is a deductive approach (Miksza and Elpus, 2018). CFA consists of various assumptions and expectations that are based on the priority model and the theory of constructs to determine the theory that best fits the model (Williams et al., 2010). CFA has become established as a significant tool of analysis for several areas of behavioural and social sciences (Kline, 2010). CFA is more suitable for the current research, as it is a deductive approach used to test an existing theory such as the Theory of Planned Behaviour (TPB).

To assess and analyse the CFA of the model in the current study, IBM AMOS software version 28 was used. AMOS was chosen due to its ease of use within a graphic interface, its unique capabilities to assess and analyse models within complex multivariate relationships, and its popularity among scholars in previous related studies (Byrne, 2013; Hair et al., 2006; Tabachnick and Fidell, 2000). Additionally, the findings offered by AMOS can be interpreted and drawn in graphical form, as well as presented in tables and text. The following section discusses CFA.

4.9.2.1 Confirmatory Factor Analysis (CFA)

CFA is another type of FA technique which is included in SEM and is used for measuring the models (Byrne, 2010). SEM is a confirmatory method that is used in delivering an inclusive means of validating the constructs in the measurement models (Awang, 2015; Byrne, 2010; Hair et al., 2010). According to Hair et al. (2006), the flexibility and comprehensiveness of SEM in executing data analysis make it the most commonly used statistical technique. Additionally, to examine the hypothesised relationship with a model's construct, SEM is recommended (Byrne, 2009; Hair et al., 2006). One of the key aspects behind the choice of SEM for data analysis was that it permitted the researcher to explore causal relationships between variables using FA (Hair et al., 2010).

CFA belongs to the family of SEM techniques and it has become established as a significant analysis tool for many domains of the social and behavioural sciences. In addition, CFA enables researchers to test and identify theories against hypotheses, as it explains the analysis conducted on the retrieved data (Adams et al., 2007; Kline, 2010). To evaluate the model using CFA and goodness-of-fit (GOF) criteria indices, reliability, convergent and discriminant validity had to be tested (Hair et al., 2010).

In CFA, there are a number of GOF criteria indices that reflect how fit the model is to the data at hand, and most SEM researchers (Bentler and Wu, 2002; Hair et al., 1998) suggested evaluating the models by observing more than one of the GOF indices. There are three fit classifications namely Absolute fit, Incremental fit, and Parsimonious fit (Awang, 2015). The model fit categories, their explanations, and their levels of acceptance are illustrated in Table 6, 7, and 8.

Table 6 : GOF Indices for Absolute fit category (Awang, 2015)

Category	GOF index	Index full name	Explanation	Level of acceptance	Reference
Absolute fit	Chi-Square ($\chi 2$) or (CMIN)	Discrepancy Chi Square	Explains the dissimilarity in the estimated model's covariance matrices and the data. The ratio of $\chi 2$ to the degrees of freedom is the difference. The main aim of using CMIN is the decrease in large sample sizes of $\chi 2$ inflation. (Byrne, 2009; Hair et al., 2010). Chi-sequare is highly sensitive to sample size (Iacobucci, 2010; Hoe, 2008; Hair et al., 1996; Shah and Goldstein, 2006; Byrne, 2009; Hair et al., 2010). Awang (2015) mentioned that it is not applicable for large sample size which is greater than 200.	Acceptable:<5 Good: <3	(Wheaton et al.,1977; Garver and Mentzer; 1999; Awang, 2015)
	RMSEA	Root Mean Square Error of Approximation	RMSEA is the value of the absence of the model fit per a degree of freedom. According to (Ainur et al., 2017) RMSEA is influenced by sample size.	< 0.08	(Garson, 2006; Browne and Cudeck, 1993; Garver and Mentzer; 1999; Awang, 2015).
	GFI	Goodness of Fit Index	GFI is a measure of fit among the observed covariance matrix and the hypothesised model (Baumgartner and Hombur, 1996). It is less sensitive to sample size than Chi- square (Aldhaban, 2016).	> 0.90	(Joreskog and Sorbom, 1984; Baumgartner and Hombur, 1996; Awang, 2015)

Table 7 : GOF Indices for Incremental fit category (Awang, 2015)

Category	GOF index	Index full name	Explanation	Level of acceptance	Reference
Incremental fit	AGFI	Adjusted Goodness of Fit	AGFI modifies the GFI, which is influenced by the size of sample (Iacobucci,2010; Aldhaban, 2016).	>0.90	(Tanaka and Huba, 1985; Baumgartner and Hombur, 1996; Awang, 2015)
	CFI	Comparative Fit Index	In Quantitative SEM research, CFI is considered as one of the most eligible models with statistical index between 0 and 1. Since it is not impacted by the size of sample, it is considered as a crucial study for fit index (Ainur et al., 2017; Bentler, 1990; Tabachnick and Fidell, 2007; Hooper, Coughlan and Mullen, 2008; Byrne, 2010).	>0.90	(Bentler, 1990; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015; Joreskog and Sorbom, 1984)
	TLI	Tucker-Lewis Index	TLI scales the wellness of the estimated model in relation to the other baseline model using an incremental fit measure (Byrne, 2010; Hair et al., 2006). It is less influenced by sample size (Ainur et al., 2017)	>0.90	(Bentler and Bonett, 1980; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015)
	NFI	Normalised Fit Index	An incremental measure of GOF for a statistical model, which is not impacted by the number of variables in the model (Bentler and Bonett, 1980).	>0.90	(Bollen, 1989; Awang, 2015)

Table 8 : GOF Indices for Parsimonious fit category (Awang, 2015)

Category	GOF index	Index full name	Explanation	Level of acceptance	Reference
Parsimonious fit	Chi-square/df	Chi Square/Degree of Freedom	Based on the Proportion among the degree of freedom Chi-square.	<3.0	(Marsh and Hocevar, 1985; Garver and Mentzer, 1999; Hoe, 2008)

4.10 Research Validity and Reliability

Even though the validity and reliability concepts are closely related, they demonstrate variation in their properties during the use of the measurement instrument. In general, the measurement instrument might be reliable although it might not be valid; however, if the

measurement is valid it might also be reliable. It should be noted that reliability by itself does not stand as a valid criterion by which to ensure validity. Therefore, the researcher has to examine both the validity and the reliability of the measurement tool that is being used (Sürücü and Maslakçı, 2020).

4.10.1 Validity

Validity was defined by Hair et al. (2010) as the degree to which a measure precisely represents what is assumed. Furthermore, according to Saunders et al. (2009), the extent to which a data gathering tool assesses what it intends to measure is referred to as validity. That is, validity focuses on accuracy of the data gathering instrument. In order to determine the validity of the measuring tool, different types of validity have been suggested (Oluwatayo, 2012; Sürücü and Maslakçı, 2020). Construct validity is one of the types that is generally accepted to have particular importance in research (Sürücü and Maslakçı, 2020). Additionally, it is commonly used in research and is based on the relationships between variables (Sürücü and Maslakçı, 2020).

4.10.1.1 Construct Validity

This can be defined as the degree used to measure a test that requires measurement (Hair et al., 2006). Moreover, Hair et al. (2006) classified construct validity as a focus on the degree to which items should be measured, which represents the designed construct of measure. Construct validity can be classified into two types – Convergent Validity and Discriminant Validity. In addition, Fornell and Larcker (1981) suggested a method for measuring both convergent and discriminant validity based on the Average Variance Extracted (AVE) value; this was acquired from each factor as a technique for determining construct validity. According to Sürücü and Maslakçı (2020), this suggested method has been generally accepted in the literature. Convergent validity is determined when the elements in the measurement model are statistically significant. In addition, the convergent validity can also be proved by computing the AVE of the constructs. In order to achieve convergent validity the value should be 0.5 or higher (Awang, 2015). Discriminant validity is defined as the level where each variable is unique, compared to other variables (Hair et al., 2006). Discriminant validity is accomplished when the AVE square root value is greater than the other values from the construct's correlation.

4.10.2 Reliability

Denscombe (2007) suggested that reliability focuses on the data collection tool that repeatedly returns similar results on the same participants. The researchers will not be able to

properly conclude, formulate or generalise the theories to an increasing number of users without verifying other researchers and practitioners who have the ability to repeat research methods or generate the same findings (Easterby-Smith, Thorpe and Jackson, 2012). The current study used Cronbach's alpha reliability coefficient ($\alpha > 0.7$) to measure the survey questionnaire for internal reliability. The value being greater than 0.7 shows high reliability, which means similar studies may provide similar results in different circumstances (George and Mallery, 2003). Additionally, the researcher explains the description and justification of the methods used in research to gather and analyse the data to ensure replicability and repeatability (Saunders et al., 2009). To avoid misinterpretation or ambiguity in the questionnaire, accuracy and careful phrasing of the questions were ensured, using the reliability for the research outcome. Further, piloting helped to gain enough knowledge in regard to the study's purpose, helping the researcher with a reliable research outcome (Hesse-Biber and Leavy, 2011).

4.11 Ethical Considerations

Ethical approvals are required, as they protect the rights of individuals who participate in the survey. Moreover, they demonstrate that the survey is abiding by the law of the land. The ethics committee of the Department of Computer and Information Sciences at Strathclyde University has given ethical consent to conduct the current study. The participants were aware that the questionnaire involved no risk. All responses were recorded anonymously, and the responses were accessed by the researcher. A cover letter with contact information was delivered to the participants to answer any questions.

It was stated by Mitchell and Jolley (2013) that ethical considerations play a vital role in any research process. Scholars and practitioners, over the years, have suggested various ethical guidelines required for the survey, such as: participation that is completely voluntary; protecting the respondents and making sure they are not harmed; maintaining the confidentiality and not sharing the respondents' personnel details; and analysing, reporting, and identifying the research purpose (Easterby-Smith et al., 2012; Saunders et al., 2009). In voluntary participation, the respondents were clearly informed that their contribution was voluntary and that their participation could be withdrawn at any moment. Therefore, a completed survey was taken as an indication of agreement to contribute in the survey. As for protecting the respondents, the survey did not contain any questions that made the respondents uncomfortable or harmed them in any way (Vaus, 2002). The identity of the respondents was protected by ensuring the responses were kept in a confidential

and protected place, and by only the researchers having access to the raw data (Bryman and Bell, 2007). Further, the respondents were requested not to include any personal information that helped in their identification (Saunders et al., 2009). With regard to the purpose of the study, the respondents were given clear and sufficient knowledge that the results were collected solely for academic purposes. Finally, the researcher made sure that the reports, results, and methods were used exclusively for identifying the problems, weaknesses, and strengths of the study (Adler and Clark, 2010).

4.12 Chapter Summary

This chapter discussed the research philosophy to determine what best suits the current research. A suitable research philosophy was selected, and a justification for the selection was provided. This was followed by the research approaches, which discussed the step-by-step plan for data gathering, analysis, and clarification. The research strategy was then discussed, as it provides a direction for the researcher's thought process. Finally, the data analysis technique was explained. Figure 8 illustrates the research methods that were selected for use in the current study.

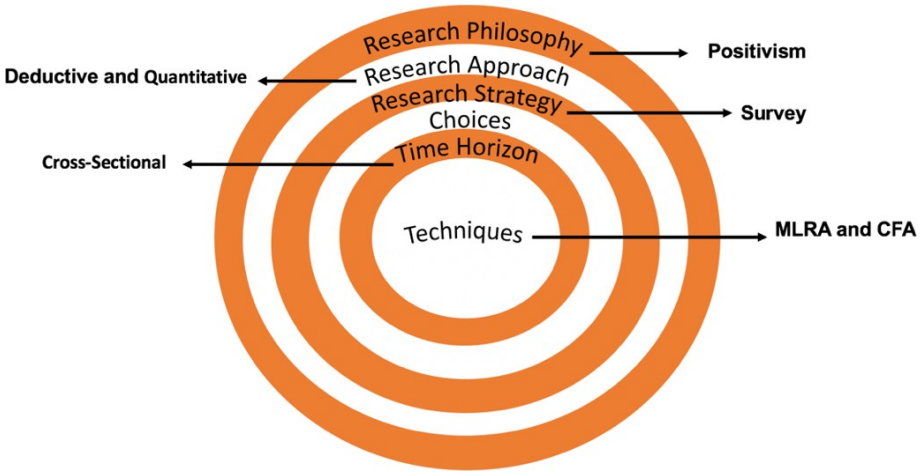


Figure 8 : Choice of Research Methodology

The following chapter, Data Analysis, interpreted the data and explained the results, using IBM SPSS version 28 and AMOS version 28 software.

CHAPTER 5. Data Analysis

5.1 Introduction

The previous chapter discussed the conceptual framework and development of hypotheses. This chapter analyses the collected data from the survey respondents by employing different data analysis techniques such as MLRA and CFA. Validity and Reliability tests were conducted on the data to confirm the survey responses were reliable and valid. To generate appropriate and clear results, data screening methods such as univariate (missing data, outliers, and test for normality) were employed. After the data were analysed using the different techniques, the hypotheses were tested, and the details were provided accordingly.

There were, in total, 563 responses to the questionnaire recorded from the undergraduate students at KFU in Saudi Arabia. Out of the 563, due to missing values, 62 responses were disregarded; therefore, 501 responses were taken into account for the data analyses. FA tests the data adequacy, reliability, and validity, and therefore was used to analyse the collected data. Cronbach's Alpha was used to test the reliability of the data; and to test the data's validity, discriminant validity was used. CFA was used to verify the GOF of the model.

5.2 Preliminary Analysis

The preliminary analysis focuses on the data gathered from survey questionnaires, to examine and filter the data, and to determine the responses to the research hypotheses that will be proposed in the conceptual framework. The gathered data were quantitative and were analysed by SPSS, which is widely utilised in various research categories, such as business, engineering, and social sciences (Zikmund, 2003). Furthermore, descriptive statistical techniques, such as frequencies, and mean and standard deviations in SPSS, were used to analyse the results of different factors to filter the gathered data and further analyse the results.

5.2.1 Demographic Factors Results

The total number of questionnaires sent out to undergraduate students at KFU was 563. In all, 60 responses were incomplete; also, there were two responses choosing only one answer for all of the survey questions. So, 62 responses were deleted. The utilisable number was therefore N=501, which was put into the analysis. Tables 9, 10, and 11 describe the demographics based on gender, age, and field of study.

Table 9 : Demographic Factors Results (Respondent Gender)

Gender	Frequency	Percentage
Male	242	48.3%
Female	259	51.7%

Table 10 : Demographic Factors Results (Respondent Age)

Age	Frequency	Percentage
Less than 18	4	.8%
18-21	89	17.8%
22-24	247	49.3%
25 and older	161	32.1%

Table 11 : Demographic Factors Results (Respondent Field of Study)

Field of Study	Frequency	Percentage
Business Administration	104	20.8%
Engineering	121	24.2%
Medicine	109	21.8%
Computer Science and Information Technology	164	33.3%

The above tables demonstrate that there were more female respondents than male respondents; 51.7% were female and 48.3% were male. Additionally, the age group 22-24 obtained the most responses (49.3%) towards responding to phishing emails. The responses from computer sciences and information technology yielded the highest inputs (33.3%). Charts are also available in Appendix C.

The main reasons for selecting the four fields of studies mentioned in Table 11 is that the language of instruction is English, unlike other KFU field of studies (such as Arts, Agriculture and Food Sciences, Education, etc) where the language of instruction is Arabic. The survey of this thesis is in English, therefore, these fields of study were selected. Besides, the students enrolling in these fields are required to complete preparatory (foundational) years to ensure they have a good understanding of English. Moreover, students from different backgrounds. For instance, a student from computer science might evaluate a cybersecurity situation differently when compared to students from other fields such as medicine. Therefore, these four fields of study were considered in this thesis.

5.2.2 Descriptive Statistics of Scaled Score

This section demonstrates the mean and standard deviation for the TPB independent factors, namely, ATT, SN, and PBC, along with the dependent factor IN. The TPB survey included three emails under SEPS, Authority, Social Proof, and Scarcity, which consisted of three questions

each for the ATT factor. Therefore, nine questions were presented for the ATT factor. Table 12 illustrates the mean and standard deviation for Attitude questions under SEPS.

Table 12 : Mean and Standard Deviation for the Attitude Questions under SEPS

Social Engineering Persuading Strategies (SEPS)	**Theory of Planned Behaviour (TPB)**	
	Independent Factors – Attitude (ATT)	
	Mean	Standard Deviation
Authority	4.10	1.18
Social Proof	3.38	1.33
Scarcity	3.81	1.19

The Attitude factor under the Authority strategy was the highest at 4.10, which indicates an 'agree' from the respondents. The TPB survey included three emails under SEPS, Authority, Social Proof, and Scarcity, which consisted of two questions each for the Subjective Norms factor. Therefore, six questions were presented for the Subjective Norm factor. Table 13 demonstrates the Mean and Standard Deviation for the Subjective Norm questions under SEPS.

Table 13 : Mean and Standard Deviation for the Subjective Norms Questions under SEPS

Social Engineering Persuading Strategies (SEPS)	**Theory of Planned Behaviour (TPB)**	
	Independent Factors – Subjective Norm (SN)	
	Mean	Standard Deviation
Authority	2.27	1.29
Social Proof	2.28	1.24
Scarcity	3.13	1.39

The Subjective Norm factor under the Scarcity strategy was highest at 3.13, which indicates a 'neutral' response from the students. The TPB survey included three emails under SEPS, Authority, Social Proof, and Scarcity, which consisted of three questions each for the PBC factor. Therefore, nine questions were presented for the PBC factor. Table 14 demonstrates the Mean and Standard Deviation for PBC factor questions under SEPS.

Table 14 : Mean and Standard Deviation for the Perceived Behavioural Control Questions under SEPS

Social Engineering Persuading Strategies (SEPS)	**Theory of Planned Behaviour (TPB)**	
	Independent Factors – Perceived Behavioural Control (PBC)	
	Mean	Standard Deviation
Authority	3.17	1.36
Social Proof	3.06	1.30
Scarcity	3.54	1.33

The Perceived Behavioural Control factor under the Scarcity strategy was highest at 3.54, which indicates an 'agree' response from the students. The TPB survey included three emails under SEPS, Authority, Social Proof, and Scarcity, which consisted of two questions each for the dependent factor IN. Therefore, six questions were presented for the IN factor. Table 15 demonstrates the Mean and Standard Deviation for the IN questions under SEPS.

Table 15 : Mean and Standard Deviation for the Intention Questions under SEPS

Social Engineering Persuading Strategies (SEPS)	**Theory of Planned Behaviour (TPB)**	
	Dependent Factors – Intention (IN)	
	Mean	Standard Deviation
Authority	3.85	1.25
Social Proof	2.45	1.47
Scarcity	3.22	1.48

IN factor under the Authority strategy was highest at 3.85, which indicates an 'agree' from the respondents.

5.2.3 Data Screening

In the process of conducting quantitative analysis, data screening is used as a crucial prerequisite step that provides the researcher with guidance to analyse and prepare the data. For instance, it helps to achieve outliers, normality, and look for missing data (Hair et al., 2010). Moreover, data screening helps to remove irrelevant data from the questionnaire responses, thus providing filtered and improved research data (Acton et al., 2009). According to Pallant (2013), data screening is defined as a scenario wherein the researcher has to review all retrieved data against the questions in a survey, to monitor if respondents have failed to answer any question. Before entering the data into SPSS, the researcher studied the data for any missing values. The data was carefully entered into SPSS while observing for any entry errors and missing codes. The following section discusses missing data.

5.2.3.1 Missing Data

Missing data takes place when a respondent does not enter the values for the presented questions, either purposely to protect identity, or through a shortage of time (Tsikriktsis, 2005). In the case of quantitative research, missing data is said to be an issue during the data analysis phase, as the missing values might return incorrect results (Tabachnick and Fidell, 2000). When the traditional statistical methods are applied, the missing data is a remarkable issue, as the software analysis of collected data delays the results and finding the bugs require extra time; this delays the overall research (Allison, 2009).

5.2.3.2 Outliers

The survey of this research work utilised the Likert-Scale, a scale of collecting data in a form of 5-points (1 to 5). In this scale, outliers do not exist even if the results are extreme to 1 or 5 (Gaskin, 2021). Apart from that, no outliers have been found in the outliers. For instance, the targeted group of participants were clearly specified, and no participant out of this group was considered in the study results.

5.2.3.3 Unengaged Respondent

According to Guin et al. (2012), when a participant is choosing only one answer for each question in the survey, this indicates that the participant is not paying attention to the questions, which points out an absence of engagement in the survey. In order to progress the quality of the data, it is suggested to recognise unengaged respondents and remove them from the data set. In this survey, two records were detected for unengaged respondents, and they were deleted from the data set.

5.2.4 Distribution of Data: Normality

Testing the data normality distribution is a necessary guide to whether parametric or nonparametric tests should be used (Tabachnick and Fidell, 2007). In the current research, each measure for the data normality distribution test patterns was analysed using graphical techniques (e.g., histograms) and statistical analysis techniques (e.g., skewness and kurtosis values) (Burns and Grove, 2011; Pallant, 2001; Polit et al., 2001).

According to Tabachnick and Fidell (2007), the most common statistical approaches used for measuring the normality of variables or composite scores are skewness and kurtosis. The skewness test examines to what extent the data distribution is symmetrical, while kurtosis studies the extent to which the data are too high or too levelled (Hair et al., 2017). If the values of skewness and kurtosis are close to zero, statistically, the factors are said to be normally distributed (Pallant, 2001; Tabachnick and Fidell, 2007). The values in the range between -1 and 1 are said to be normally distributed, while the values outside this range are said to be skewed (Bulmer, 1979; Hair et al., 2010; Huck, 2004). The results from the normality assessment are demonstrated in Table 16.

Table 16 : Outlines the Values for Skewness and Kurtosis

SEPS	Item	Skewness	Std. Error of Skewness	Kurtosis	Std. Error of Kurtosis
Authority	ATT1	-.708	.109	-.048	.218
	ATT2	-.904	.109	.316	.218
	ATT3	-.952	.109	.234	.218
	SN1	-.402	.109	-.379	.218
	SN2	-.457	.109	-.465	.218
	PBC1	-.365	.109	-.801	.218
	PBC2	-.903	.109	.261	.218
	PBC3	-.817	.109	.019	.218
	IN1	-.782	.109	.126	.218
	IN2	-.679	.109	.153	.218
Social Proof	ATT1	1.133	.109	.757	.218
	ATT2	.471	.109	-.530	.218
	ATT3	.883	.109	.348	.218
	SN1	.934	.109	.550	.218
	SN2	.639	.109	-.193	.218
	PBC1	.806	.109	-.038	.218
	PBC2	-.518	.109	-1.023	.218
	PBC3	-.383	.109	-1.107	.218
	IN1	.687	.109	-.843	.218
	IN2	.664	.109	-.640	.218
Scarcity	ATT1	.219	.109	-1.085	.218
	ATT2	-.503	.109	-.653	.218
	ATT3	-.105	.109	-.890	.218
	SN1	-.023	.109	-.938	.218
	SN2	-.078	.109	-.972	.218
	PBC1	-.750	.109	.462	.218
	PBC2	-.590	.109	.073	.218
	PBC3	-.965	.109	.437	.218
	IN1	-.211	.109	-1.211	.218
	IN2	-.153	.109	-1.093	.218

Table 16 illustrates the skewness and kurtosis of all the emails presented to the respondents. There are three questions each for ATT and PBC, and two questions each for SN and IN. All these factors have a relation with SEPS. The values in the range between -1 and 1 are said to be normally distributed, whereas the values outside this range are said to be skewed (Bulmer, 1979; Hair et al., 2010; Huck, 2004). It can be seen that the data are slightly deviated from normality, as the values of skewness and kurtosis are a little above and below the recommended range of -1/+1 (Bulmer, 1979; Hair et al., 2010; Huck, 2004). For instance, according to the results of the skewness and kurtosis scores, one item is problematic, which is ATT1 under the Social Proof strategy. This has

a value of (1.133) which is out of the range -1.0 to +1.0. The normality data distribution test using the histogram is available in Appendix E.

5.3 Construct Reliability

In order to make the extent of measurement indicators feasible, researchers make use of construct reliability. Construct reliability can be defined as the consistency of a measure (Hair et al., 2014) and it assesses to what extent all items in the scale represent one underlying construct. The main disturbing factor of reliability is said to be the internal consistency of a construct (Cortina, 1993; Pallant, 2013).

The current research utilised consistency reliability, also known as Cronbach's alpha coefficient, which is considered a crucial reliability test in order to evaluate the measurement of internal consistency (Churchill, 1979; Cortina, 1993; Steenkamp and van Trijp, 1991). Cronbach's alpha offers various features such as clarity and accessibility, making it the most preferred reliability measurement method for researchers.

Cronbach's alpha offers a valid construct standard threshold of 0.7 or higher (Hair et al., 1998; Pallant, 2013). Bacon (2004), while accepting Hair et al.'s (2014) measurement range, added that a measure less than 0.7 is to be accepted for large-sample-size data. However, a Cronbach's alpha value lower than 0.6 illustrates inconsistency in the data and should be reconsidered (Malhotra, 2004). George and Mallery (2003) provided the following range for Cronbach's alpha: if the value is greater than or equal to .9 the Cronbach's Alpha is considered excellent, for values greater than or equal to .8, it is good, for values greater than or equal to .7 it is acceptable, for values greater than or equal to .6 the Cronbach's alpha is questionable, for values greater than or equal to .5 the Cronbach's Alpha is considered poor, and for values less than or equal to .5 it is unacceptable.

Cronbach's alpha was used in the current study for verifying the reliability of the factors. For basic research reliability, a minimum Cronbach's alpha of 0.7 is suggested (Hair et al., 1998; Nunally, 1978). Table 17 shows the Cronbach's alpha results for the TPB factors under SEPS.

Table 17 : Cronbach's Alpha Results for TPB Factors under SEPS

TPB factor under SEPS	Cronbach's Alpha	Number of Items
Attitude	.831	9
Subjective Norms	.852	6
Perceived Behavioural Control	.791	9
Intention	.833	6

The Cronbach's alpha values were above 0.7, which means the data were reliable. To sum up, the internal consistencies in this study for the factors were in agreement with the proposed threshold of values greater than 0.7 (Hair et al., 1998; Nunally, 1978; Pallant, 2013; Tabachnick and Fidell, 2007).

5.4 Construct Validity: Discriminant Validity

Discriminant validity is the extent to which factors are distinct and uncorrelated (Hair et al., 2006). A good instrument should show good discriminant validity where the factor is able to account for more variance in the observed variables rather than other constructs within the conceptual framework. The factor correlation matrix can be used to assess the discriminant validity, and the correlations between factors should be below 0.7 (Gaskin, 2016). Table 18 presents the outcomes of the discriminant validity for the TPB factors under SEPS.

Table 18 : Discriminant Validity Results for TPB Factors under SEPS

	ATT	SN	PBC	IN
ATT	1.000	.437	.026	-.180
SN	.437	1.000	.439	.117
PBC	.026	.439	1.000	.343
IN	.180	.117	.343	1.000

It can be seen from Table 18 that there is no correlation that is above the value of 0.7, which means the discriminant validity is achieved.

5.5 Data Analysis Techniques Results

5.5.1 Multiple Linear Regression Analysis (MLRA)

The MLRA explains the unique variance of the dependent factor (e.g., IN) by each independent factor (e.g., ATT, SN, and PBC) (Pallant, 2005). Additionally, it is a widely used multivariate statistical technique to test hypotheses and predict dependent variable values. As this study uses TPB, to analyse the user behavioural intention when responding to phishing emails, the MLRA establishes how independent variables (ATT, SN, and PBC) explain the unique variance of the dependent variable (IN).

To analyse the data, IBM SPSS software version 28 was used, and the data was loaded to test the hypothesis for MLRA. As it best aligns with the study's research question, the 'Enter' method (Mertler and Reinhart, 2017; Nathans et al., 2012) was used. To analyse and interpret the information, model summary, ANOVA, and coefficients tables were utilised. The model summary consisted of R, R squared (R2), and R squared adjusted (R2adj) values. The variance measurement values predicted the combination of how well the independent factors predicted the dependent

factor (Nathans et al., 2012). R2 values, as per Lowry and Gaskin (2014), should be high, with the following ranges: substantial .75, moderate .50, and weak .25 (Hair et al., 2016; Sarstedt et al., 2014).

In the current study, MLRA was used to answer the first and second research questions, which were:

RQ1. To what extent ATT, SN, and PBC impact the behavioural intention of Saudi Arabian undergraduate students when responding to phishing emails under SEPS?

RQ2. What factors of TPB have the strongest influence in explaining the behavioural intention of Saudi Arabian undergraduate students when faced with phishing emails under SEPS?

Firstly, MLRA was performed to assess the impact of the TPB independent factors (ATT, SN, and PBC) on the dependent factor (IN), in the context of responding to phishing emails under the Authority strategy. This was followed by MLRA assessing the impact of ATT, SN, and PBC on IN in the context of responding to phishing emails under the Social Proof strategy. Lastly, MLRA was performed to assess the impact of ATT, SN, and PBC on IN in the context of responding to phishing emails under the Scarcity strategy.

5.5.1.1 Assessment of the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Authority Strategy

In order to assess the impact of ATT, SN, and PBC on IN in the context of responding to phishing emails under Authority strategy, MLRA was performed. MLRA was executed using the "Enter" method to determine how much the independent factors of the TPB explain the behavioural intention (IN) to respond to phishing emails. All of the independent factors under the authority strategy has been entered as shown in Table (19). Regression results show that the TPB model significantly predicts intended behaviour to respond to phishing emails under Authority strategy ($R2 = .538$, $p < .001$). The three main independent constructs of the TPB (ATT, SN, and PBC) explained 53.8% of the variance in behavioural intention to respond to phishing emails under Authority. This means that under the Authority strategy, 53.8% variance in behavioural intention to respond to phishing emails can be predicted by ATT, SN, and PBC.

In addition, the coefficient (Table 22) evaluated each of the TPB independent factors individually with regard to IN (the dependent factor). The coefficient values for ATT are significant, showing that ATT significantly impacts behavioural intention in the context of

responding to phishing emails under Authority, (β =.468, p < 0.01). Moreover, the beta coefficients value tell us that ATT had the strongest influence independent factor of TPB in explaining the behavioural intention to respond to phishing emails under the Authority strategy. In addition to this, the coefficient values for SN are significant, showing that SN significantly impacts behavioural intention to respond to phishing emails under the Authority strategy (β = .259, p < 0.01). The coefficient values for PBC are significant, showing that PBC significantly impacts behavioural intention to respond to phishing emails under the Authority strategy, where β = .109, and p value = .009, which is less than 0.05. In addition to this, Table (23) shows that among the three demographic factors used in this study (Gender, Age, and Field of Study), the gender was significantly impacts behavioural intention to respond to phishing emails under Authority strategy (Sig = .002). The following tables (20, 21, 22, and 23) provide analysis statistics of multiple linear regression results for the TPB factors under the Authority strategy (Appendix D).

Table 19 : Variables Entered under Authority strategy

Model	Variables Entered	Variables Removed	Method
1	ATT, SN, PBC	.	Enter

Table 20 : Model Summary results of TPB factors under Authority strategy

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.734	.538	.536	.562

Table 21 : ANOVA results of TPB factors under Authority strategy

Model		Sum of Squares	df	Mean Squares	F	Sig.
1	Regression	183.393157.195	3	61.131	193.277	<.001
	Residual	340.587	497	.316		
	Total		500			

Table 22 : Coefficients results of TPB factors under Authority strategy

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.529	.164		3.220	.001
	ATT	.519	.046	.468	11.386	< .001
	SN	.229	.036	.259	6.285	< .001
	PBC	.139	.053	.109	2.617	.009

Table 23 : Coefficients results of demographic and TPB factors under Authority strategy

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	3.509	.209		16.802	<.001
	Gender	.217	.070	.142	3.075	.002
	Age	.010	.051	.009	.188	.851
	Field of Study	-.003	.031	-.004	-.087	.931

5.5.1.2 Assessment of the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Social Proof Strategy

In order to assess the impact of ATT, SN, and PBC on IN in the context of responding to phishing emails under Social Proof strategy, MLRA was performed. Regression results show that the TPB model significantly predicts intended behaviour to respond to phishing emails under Social Proof strategy ($R2 = .518$, $p < .001$). The three main independent constructs of the TPB (ATT, SN, and PBC) explained 51.8% of the variance in behavioural intention to respond to phishing emails under Social Proof strategy. This means that under the Social Proof strategy, 51.8% variance in behavioural intention to respond to phishing emails can be predicted by ATT, SN, and PBC.

In addition, the coefficient (Table 27) evaluated every independent factors of the TPB individually with respect to IN (the dependent factor). The Coefficient values for attitude are significant, showing that ATT significantly impacts behavioural intention to respond to phishing emails under the Social Proof strategy, ($\beta = .431$, $p < 0.01$). Furthermore, the beta coefficients value tell us that ATT had the strongest influence independent factor of TPB in explaining the behavioural intention to respond to phishing emails under the Social Proof strategy. Additionally, the coefficient values for SN are significant, showing that SN significantly impacts behavioural intention to respond to phishing emails under the Social Proof strategy ($\beta = .285$, $p < 0.01$). However, the coefficient values for PBC revealed that PBC did not significantly impact behavioural intention to respond to phishing emails under the Social Proof strategy, with ($p = .123$), which is greater than 0.05. Table (28) displays that age was significantly impacts behavioural intention to respond to phishing emails under Social Proof strategy (Sig = .005) among the three demographic factors used in this study. The following tables, Table (25), Table (26),

Table (27), and Table (28) provide analysis statistics of multiple linear regression results for the TPB factors under the Social Proof strategy (Appendix D).

Table 24 : Variables Entered under Social Proof strategy

Model	Variables Entered	Variables Removed	Method
1	ATT, SN, PBC	.	Enter

Table 25 : Model Summary results of TPB factors under Social Proof strategy

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.719	.518	.515	.892

Table 26 : ANOVA results of TPB factors under Social Proof strategy

Model		Sum of Squares	df	Mean Squares	F	Sig.
1	Regression	424.418	3	141.473	177.714	<.001
	Residual	395.646	497	.796		
	Total	820.064	500			

Table 27 : Coefficients results of TPB factors under Social Proof strategy

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.054	.159		-.338	.735
	ATT	.581	.097	.431	5.982	< .001
	SN	.381	.095	.285	4.029	< .001
	PBC	.078	.050	.052	1.546	.123

Table 28 : Coefficients results of demographic and TPB factors under Social Proof strategy

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.077	.331		6.271	<.001
	Gender	.050	.112	.021	.444	.658
	Age	.227	.080	.135	2.828	.005
	Field of Study	-.094	.049	-.089	-1.914	.056

5.5.1.3 Assessment of the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Scarcity Strategy

In order to assess the impact of ATT, SN, and PBC on IN in the context of responding to phishing emails under Scarcity strategy, MLRA was executed. Regression results display that the TPB model significantly predicts intended behaviour to respond to phishing emails under Scarcity strategy ($R2 = .498$, $p < .001$). The three main independent constructs of the TPB (ATT, SN, and PBC) explained 49.8% of the variance in behavioural intention to respond to phishing emails under Scarcity strategy. This means that under the Scarcity strategy, 49.8% variance in behavioural intention to respond to phishing emails can be predicted by the three independent factors (ATT, SN, and PBC).

In addition, the coefficient (Table 32) evaluated each independent factors of the TPB individually with respect to IN (the dependent factor). The Coefficient values for attitude are significant, showing that ATT significantly impacts behavioural intention to respond to phishing emails under the Scarcity strategy, ($\beta = .235$, $p < 0.01$). Additionally, the coefficient values for SN are significant, showing that SN significantly impacts behavioural intention to respond to phishing emails under the Scarcity strategy ($\beta = .490$, $p < 0.01$). Moreover, the beta coefficients value tell us that SN had the strongest influence independent factor of TPB in explaining the behavioural intention to respond to phishing emails under the Scarcity strategy. The coefficient values for PBC revealed that PBC did not significantly impact behavioural intention to respond to phishing emails under the Scarcity strategy, with ($p = .718$), which is greater than 0.05. Table (33) shows that the demographic factors (age, gender, and field of study) did not significantly impact behavioural intention to respond to phishing emails under the Scarcity. The following tables, Table (30), Table (31), Table (32), and Table (33) provide analysis statistics of multiple linear regression results for the TPB factors under the Scarcity strategy (Appendix D).

Table 29 : Variables Entered under Scarcity strategy

Model	Variables Entered	Variables Removed	Method
1	ATT, SN, PBC	.	Enter

Table 30 : Model Summary results of TPB factors under Scarcity strategy

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.705	.498	.495	.927

Table 31 : ANOVA results of TPB factors under Scarcity strategy

Model		Sum of Squares	df	Mean Squares	F	Sig.
1	Regression	423.209	3	141.070	164.134	<.001
	Residual	427.161	497	.859		
	Total	850.370	500			

Table 32 : Coefficients results of TPB factors under Scarcity strategy

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.281	.188		1.493	.136
	ATT	.318	.080	.235	3.989	< .001
	SN	.599	.068	.490	8.742	< .001
	PBC	.024	.066	.015	.362	.718

Table 33 : Coefficients results of demographic and TPB factors under Scarcity strategy

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.426	.332		10.313	<.001
	Gender	-.094	.112	-.039	-.842	.400
	Age	.050	.081	.030	.622	.534
	Field of Study	-.076	.049	-.073	-1.551	.121

The current research has three main hypotheses (discussed in Chapter 3); from the results in the above tables, Hypothesis 1 (H1: Saudi Arabian undergraduate students' ATT factor impacts the behavioural intention to respond to phishing emails under SEPS) is supported, where ATT significantly impacts behavioural intention to respond to phishing emails, under all of the SEPS (Authority, Social Proof, and Scarcity) ($p < 0.01$). Additionally, Hypothesis 2 is supported (H2: Saudi Arabian undergraduate students' SN factor impacts the behavioural intention to respond to phishing emails under SEPS.), since the SN significantly impacts behavioural intention to respond to phishing emails under SEPS ($p < 0.01$). However, Hypothesis 3 (H3: Saudi Arabian undergraduate students' PBC factor impacts the behavioural intention to respond to phishing emails under SEPS.) is not supported, because the PBC did not impact behavioural intention to

respond to phishing emails, under either the Social Proof or the Scarcity strategies, where the p-value was greater than 0.05.

5.5.2 Factor Analysis (FA) Test Results

5.5.2.1 Kaiser-Meyer-Olkin (KMO) Test

The KMO test is a measure of sampling sufficiency. In addition, it is an index used to examine the suitability of FA – whether or not you have adequate samples to run your FA. In addition, the KMO value should be higher than 0.50; anything less than 0.50 indicates data might not be appropriate for running FA (Hair et al., 2010; Tabachnick and Fidell, 2007). (Appendix G)

5.5.2.2 Bartlett's Test of Sphericity

Bartlett's test of sphericity is a statistical test that is utilised in examining the hypothesis to determine if the factors are not correlated in a given population, because the lack of correlation might be illogical in analysing the factors. The factors should be correlated so they can be easily grouped. Bartlett's test of Sphericity value less than 0.05 indicates that the data might return an identity matrix, which means that the factors are correlated and there are significant relationships among variables (Hair et al., 2010; Costello and Osborne, 2005; Tabachnick and Fidell, 2007; Verbeke and Viaene, 2000).

Table 34 : KMO and Bartlett's Test of Sphericity Results

SEPS	TPB	KMO	Bartlett's Test
			Sig. Value
Authority	Attitude	.853	.000
	Subjective Norm		
	Perceived Behavioural Control		
	Intention		
Social Proof	Attitude	.840	.000
	Subjective Norm		
	Perceived Behavioural Control		
	Intention		
Scarcity	Attitude	.867	.000
	Subjective Norm		
	Perceived Behavioural Control		
	Intention		

Table 34 presents the KMO and Bartlett's test values. Hoelzle et al. (2013) and Lloret et al. (2017) recommended that a KMO value greater than or equal to .70 is desired. Child et al. (2006) suggested that a KMO value less than .50 is considered unacceptable. Further, the Barlett's test value should be less than 0.05. The KMO values for the current research are greater than .8

and the Barlett's test values are less than .05. Therefore, the data are appropriate for conducting FA. (Appendix G)

5.5.2.3 Communality Test

Communality is the amount of variance a factor shares with all the other factors. Ideally, if the communality value is less than 0.50, that variable should be removed (Hair et al., 2010; Tabachnick and Fidell, 2007). The following table shows the results of the communality test.

Table 35 : Communality Test Results

SEPS	TPB	Questions	Communalities
Authority	Attitude	Q1	.702
		Q2	.757
		Q3	.814
	Subjective Norms	Q1	.781
		Q2	.720
	Perceived Behavioural Control	Q1	.674
		Q2	.722
		Q3	.700
	Intention	Q1	.710
		Q2	.662
Social Proof	Attitude	Q1	.831
		Q2	.813
		Q3	.809
	Subjective Norms	Q1	.837
		Q2	.840
	Perceived Behavioural Control	Q1	.628
		Q2	.955
		Q3	.926
	Intention	Q1	.683
		Q2	.657
Scarcity	Attitude	Q1	.663
		Q2	.748
		Q3	.749
	Subjective Norms	Q1	.835
		Q2	.786
	Perceived Behavioural Control	Q1	.608
		Q2	.676
		Q3	.656
	Intention	Q1	.787
		Q2	.786

Table 35 shows the values of communalities for the TPB factors in all strategies. Authority, Social Proof, and Scarcity are all higher than the critical value of 0.50. (Appendix G)

5.5.3 Confirmatory Factor Analysis (CFA)

CFA is a part of the Structural Equation Modeling (SEM) technique that is used to examine the multidimensionality and factor validity of the theoretical framework's variables (Byrne, 2010). CFA is also used to examine the validity of a construct via model GOF indices (Tabachnick and Fidell, 2007). The relation between factors and their measured variables is established using the CFA technique. Therefore, CFA denotes a test of measurement model (Byrne, 2001).

CFA was used to assess the research model's validity by initiating acceptable levels of GOF measurement model, and any evidence specific to construct validity (Hair et al., 2006). Model fit indices were used to determine if the model used represented data. The model was said to be acceptable if the data fit indices returned adequate, which means, if a flawless fit exists between the theoretical model and the covariation data pattern (Alojail, 2013). If the data returned sufficient results, further data analysis was performed to re-arrange and re-estimate the model (Byrne, 2010). It has been stated by several researchers (Awang, 2015; Byrne, 2010; Hair et al., 2006) that model indices are classified in three categories: Absolute fit indices, Incremental fit indices, and Parsimony fit indices.

The above categories include a number of GOF criteria indices such as: Chi-Square ($\chi 2$) or CMIN; Degree of Freedom (Chi Square/df); RMSEA; NFI; TLI; Comparative Fit Index (CFI); Goodness of Fit Index (GFI); and Adjusted Goodness of Fit Index (AGFI). These determine the data's model fitness (Awang, 2015; Byrne 2010, Hair et al., 2006, 2010; Holmes-Smith, 2006; Joreskog and Sorbom, 2005; Kline 1998). Using all of the GOF criteria is not recommended (Kline, 1998). Most SEM researchers (Bentler and Wu, 2002; Hair et al., 1998; Kline 1998) suggested evaluating the models by observing more than one of the GOF indices. Kline (1998) recommended that four GOF measures is an acceptable number for assessment of the measurement models. The following section shows the results of the third research question: **What is the GOF for the TPB model applied to explain the behavioural intention of Saudi Arabian undergraduate students to respond to phishing emails under SEPS?**

Firstly, the results of assessment model GOF under the Authority strategy will be shown and discussed. Then, the results of assessment model GOF under the Social Proof strategy will be shown and discussed. After that, the results of assessment model GOF under the Scarcity strategy will be shown and discussed.

5.5.3.1 Assessment Model Goodness-of-Fit (GOF) under the Authority Strategy

Table 36 : GOF Results for the TPB Factors under the Authority strategy

Fit Index	GOF Result	Acceptable Range	Reference
Chi-Square ($\chi 2$) or (CMIN)	159.285	<3 is good, <5 is acceptable	(Wheaton et al., 1977; Garver and Mentzer, 1999; Hoe, 2008; Awang, 2015)
RMSEA	.126	<0.05 superior fit <0.08 good fit <0.1 acceptable fit	(Garson, 2006; Kenny,2010; Garver and Mentzer, 1999; Hoe, 2008; Awang, 2015; Byrne, 2010; Schumacker and Lomax, 2010).
GFI	.935	>0.90	(Joreskog and Sorbom, 1984; Baumgartner and Hombur, 1996; Awang, 2015)
CFI	.962	>0.95 is superior, >0.90 is good	(Bentler, 1990; Garver and Mentzer, 1999; Hoe, 2008; Awang, 2015; Byrne, 2010).
TLI	.925	>0.95 is superior, >0.90 is good	(Byrne, 2010; Awang, 2015).
NFI	.958	>0.9 is acceptable	(Awang, 2015; Bollen, 1989; Bentler and Bonett, 1980).
AGFI	.838	>0.90	(Awang, 2015; Tanaka and Huba, 1985; Baumgartner and Hombur, 1996)
CMIN/DF	8.849	<3.0 is acceptable	(Shah and Goldstein, 2006; Hair et al., 2010; Byrne, 2010).
p	.000	< 0.001	

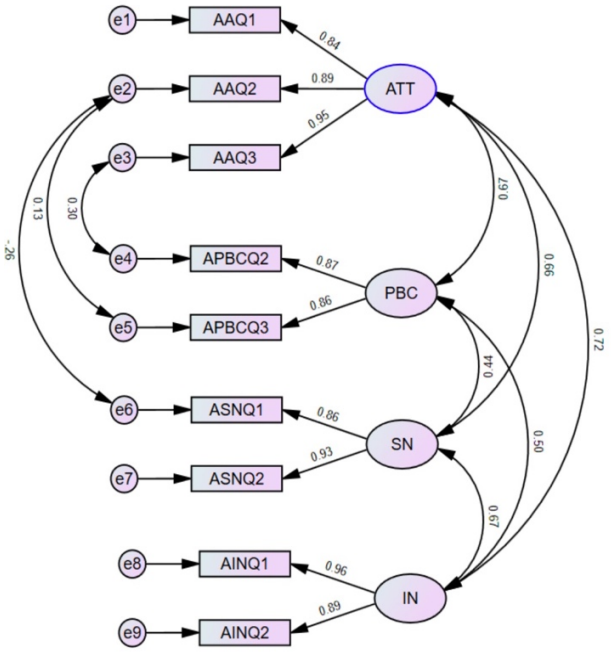


Figure 9 : CFA measurement model under the Authority strategy

5.5.3.2 Assessment Model Goodness-of-Fit (GOF) under the Social Proof Strategy

Table 37 : GOF Results for the TPB Factors under the Social Proof strategy

Fit Index	GOF Result	Acceptable Range	Reference
Chi-Square ($\chi 2$) or (CMIN)	117.164	<3 is good, <5 is acceptable	(Wheaton et al., 1977; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015)
RMSEA	.109	<0.05 superior fit <0.08 good fit <0.1 acceptable fit	(Garson, 2006; Kenny, 2010; Browne and Cudeck, 1993; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015; Hu and Bentler, 1999; Hooper et al., 2008; Byrne, 2010; Schumacker and Lomax, 2010).
GFI	.955	>0.90	(Joreskog and Sorbom, 1984; Baumgartner and Hombur, 1996; Awang, 2015)
CFI	.981	>0.95 is superior, >0.90 is good	(Bentler, 1990; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015; Tabachnick and Fidell 2007; Hooper et al., 2008; Byrne 2010).
TLI	.959	>0.95 is superior, >0.90 is good	(Byrne 2010; Awang,2015).
NFI	.978	>0.9 is acceptable	(Awang, 2015; Bollen, 1989; Bentler and Bonett, 1980).
AGFI	.881	>0.90	(Awang, 2015; Tanaka and Huba, 1985; Baumgartner and Hombur, 1996)
CMIN/DF	6.892	<3.0 is acceptable	Shah and Goldstein (2006), Hair et al. (2010), Byrne (2010).
p	.000	< 0.001	

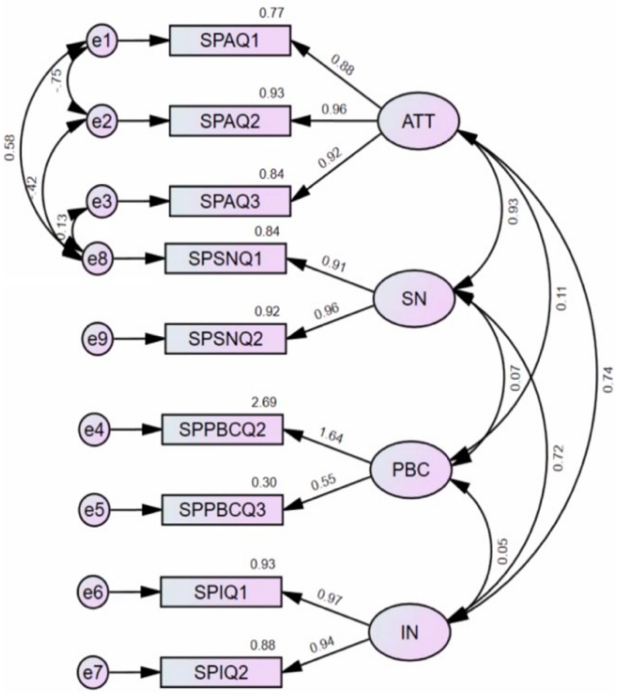


Figure 10 : CFA measurement model under the Social Proof strategy

5.5.3.3 Assessment Model Goodness-of-Fit (GOF) under the Scarcity Strategy

Table 38 : GOF Results for the TPB Factors under the Scarcity strategy

Fit Index	GOF Result	Acceptable Range	Reference
Chi-Square ($\chi 2$) or (CMIN)	161.784	<3 is good, <5 is acceptable	(Wheaton et al., 1977; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015)
RMSEA	.102	<0.05 superior fit <0.08 good fit <0.1 acceptable fit	(Garson, 2006; Kenny, 2010; Browne and Cudeck, 1993; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015; Hu and Bentler, 1999; Hooper et al., 2008; Byrne, 2010; Schumacker and Lomax, 2010).
GFI	.952	>0.90	(Joreskog and Sorbom, 1984; Baumgartner and Hombur, 1996; Awang, 2015)
CFI	.968	>0.95 is superior, >0.90 is good	(Bentler, 1990; Garver and Mentzer; 1999; Hoe, 2008; Awang, 2015; Tabachnick and Fidell 2007; Hooper et al., 2008; Byrne 2010).
TLI	.945	>0.95 is superior, >0.90 is good	(Bentler and Bonett, 1980; Hair et al., 2006; Byrne 2010; Awang, 2015).
NFI	.963	>0.9 is acceptable	(Awang, 2015; Bollen, 1989; Bentler and Bonett, 1980).
AGFI	.877	>0.90	(Awang, 2015; Tanaka and Huba, 1985; Baumgartner and Hombur, 1996)
CMIN/DF	6.221	<3.0 is acceptable	Shah and Goldstein (2006), Hair et al. (2010), Byrne (2010).
p	.000	< 0.001	

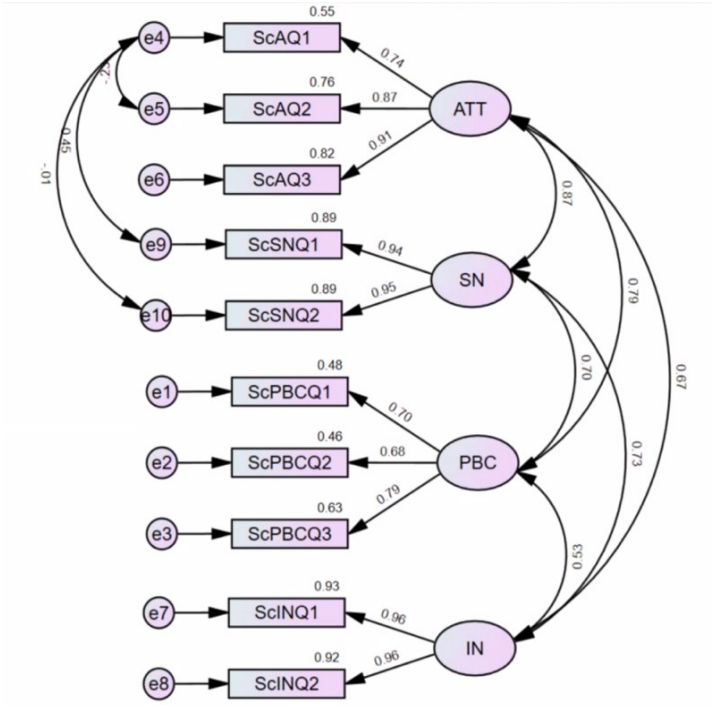


Figure 11 : CFA measurement model under the Scarcity strategy

The diagnostic analysis demonstrated a good fit of the data model, which would indicate the Theory of Planned Behaviour (TPB) model might work well when applied to the intention of responding to phishing emails under SEPS in the Saudi Arabian undergraduate students. Numerous common model-fit measures were used in measuring the model's overall GOF. Many researchers (Bentler and Wu, 2002; Hair et al., 1998; Kline, 1998) recommended evaluating the models by observing more than one of the GOF indices. Kline (1998) recommended that four GOF measures is an acceptable number for assessment of the measurement models. Consistent with recommendations by Kline (1998), four GOF indices were selected, which reflect good and acceptable values for the measurement model. The four GOF indices are NFI, TLI, CFI, and GFI. The next section discusses the assessment model GOF under each of the Social Engineering Persuading strategies.

The assessment model GOF under the Authority strategy demonstrates good model fit values. It can be seen from Table 36 that the four GOF indices (NFI, TLI, CFI, and GFI) demonstrate good model fit values. The NFI, TLI, CFI, and GFI values are .958, .925, .962, and .935 respectively, which are in the good fit range (above 0.90). Additionally, the assessment model GOF under Social Proof strategy shows good model fit values. It can be seen from Table 37 that the four GOF indices NFI, TLI, CFI, and GFI values are .978, .959, .981, and .955 respectively, which are in the good fit range (above 0.90). Furthermore, the assessment model GOF under the Scarcity strategy demonstrates good model fit values. It can be seen from Table 38 that the values of the four GOF indices NFI, TLI, CFI, and GFI are .963, .945, .968, and .952 respectively, which are in the good fit range which is greater than 0.90.

Additionally, it can be seen from the all above tables (36, 37, and 38) that there are some indices that did not achieve good model fit values, such as Chi-Square and RMSEA. The possible reason behind this could be because these indices are influenced by sample size. It has been stated by Sekaran (2003) that Chi-Square not meeting its recommended value might be due to the sample size, which exceeds the recommended maximum of 200. Awang (2015) mentioned that it is not applicable for a large sample size, i.e. greater than 200. Moreover, other researchers mentioned that indices such as Chi-Square and RMSEA are highly sensitive to sample size (Ainur et al., 2017; Awang, 2015; Iacobucci, 2010; Kenny, 2010).

Additionally, it can be seen from Figures 9 and 10 that one item, PBCQ1, was deleted from the model. According to Awang (2015), items can be removed from the measurement model if they do not fit in the measurement model, but the item removal should not be more than 20% of the mode's total items (Awang, 2015).

5.5.3.4 Construct Reliability (Composite Reliability)

Composite reliability is a measurement of internal consistency in scale items, much like Cronbach alpha (Netemeyer, 2003). Internal consistency refers to the test which ensures all the constructs in a certain instrument return a similar latent summary (Sekaran and Bougie, 2010). The internal consistency reliability limits are the upper and lower control limits of composite reliability and Cronbach alpha (Hair et al., 2017). The composite reliability values should be greater than 0.7, as they determine the data reliability (Hair et al., 2017). Table 39 illustrates the composite reliability values, which are in an acceptable range, greater than the set range of 0.7.

Table 39 : CFA Construct Reliability Results for the TPB Factors under SEPS

SEPS	TPB	Composite Reliability
Authority	Attitude	.922
	Subjective Norms	.890
	PBC	.849
	Intention	.925
Social Proof	Attitude	.942
	Subjective Norms	.934
	PBC	.821
	Intention	.952
Scarcity	Attitude	.871
	Subjective Norms	.942
	PBC	.766
	Intention	.961

5.5.3.5 Construct Validity

Validity denotes to how precisely an instrument measures what it is planned to measure. Construct validity, also known as dimension validity, is the common type of validity, and can be explained as the degree used to measure a test that requires measurement (Hair et al., 2006). This consists of two main aspects – convergent validity and discriminant validity.

5.5.3.5.1 Convergent Validity

Convergent validity measures if the factors are similar to the other variables, and displays the correlations among the variables (Kline, 1998). In addition, convergent validity is achieved when there is greater correlation between the items that share the same scenario (Sekaran and Bougie, 2010). Fornell and Larcker (1981) suggested the value of an AVE to be greater than 0.5.

Table 40 illustrates the AVE values, which are above the threshold of 0.5. Therefore, the convergent validity of the model was achieved.

Table 40 : CFA Convergent Validity Results for the TPB Factors under SEPS

SEPS	TPB	AVE
Authority	Attitude	.599
	Subjective Norms	.571
	Perceived Behavioural Control	.639
	Intention	.789
Social Proof	Attitude	.634
	Subjective Norms	.607
	Perceived Behavioural Control	.750
	Intention	.512
Scarcity	Attitude	.533
	Subjective Norms	.510
	Perceived Behavioural Control	.611
	Intention	.531

5.5.3.5.2 Discriminant Validity

Discriminant validity refers to the variables that are not similar to the other variables. There are different criteria to calculate the discriminant validity; however, the current research uses the Fornell-Larcker criterion, as it is widely used, with good reviews when compared to the relatively new criterion, Heterotrait Monotrait Ratio (HTMT) (Hamid et al., 2017).

5.5.3.5.2.1 Fornell-Larcker Criterion

This criterion compares the AVE square root value for each factor with the correlation of other variables (Hair et al., 2017). Discriminant validity is attained when the AVE square root value is greater than the other values from the construct's correlation. The current research achieved the Discriminant validity as the AVE square root values are higher than the other correlation variable values.

Table 41 : CFA Discriminant Validity Results for the TPB Factors under the Authority strategy

	ATT	SN	PBC	IN
ATT	**0.773**			
SN	0.657	**0.633**		
PBC	0.696	0.466	**0.607**	
IN	0.723	0.631	0.529	**0.656**

Table 42 : CFA Discriminant Validity Results for the TPB Factors under the Social Proof strategy

	ATT	SN	PBC	IN
ATT	**0.796**			
SN	0.298	**0.661**		
PBC	0.107	0.074	**0.866**	
IN	0.74	0.724	0.055	**0.707**

Table 43 : CFA Discriminant Validity Results for the TPB Factors under the Scarcity strategy

	ATT	SN	PBC	IN
ATT	**0.73**			
SN	0.688	**0.707**		
PBC	0.71	0.703	**0.626**	
IN	0.675	0.705	0.527	**0.707**

5.6 Chapter Summary

This chapter illustrated the data analysis results for the survey conducted on KFU undergraduate students. The data were analysed to explain and predict the participants' behavioural intentions when responding to phishing emails under different SEPS (Authority, Social Proof and Scarcity), via understanding TPB. This study found that only two of the factors of TPB (Attitude and Subjective Norms) have a statistically significant impact on undergraduate students' behavioural intention under the three persuading strategies (Authority, Social Proof and Scarcity) however the third factor of TPB which is Perceived Behavioural Control has a significant impact on undergraduate students' behavioural intentions only under the Authority strategy. The strongest predictor of undergraduate students behavioural intention under the Authority and Social Proof strategies was found to be attitude, while the Subjective Norm factor was found to be the strongest predictor under the Scarcity strategy. Additionally, the TPB model was found to have a good model fit when applied to intention to respond to phishing emails. The following chapter discusses the results in further detail.

CHAPTER 6. Discussion and Conclusion

6.1 Introduction

The purpose of the current research was to evaluate TPB to explain individual behavioural intention when responding to phishing emails under SEPS. The current study examined the impact of the TPB independent factors (ATT, SN, and PBC) on the dependent factor IN. Additionally, the current study examined the TPB model GOF to show if the TPB might or might not work with responding to phishing emails under SEPS.

Ajzen's (1988) TPB can be divided into three conceptually independent factors that determine the behavioural intention: ATT; SN; and PBC (Ajzen, 1991). Attitude toward the behaviour determines the level at which an individual has a positive or negative evaluation toward the behavioural performance. Subjective Norms denotes to an individual's belief based on the opinion of other crucial relations (e.g., friends, family or colleagues) in their lives, who determine if a behaviour should be performed, or what these individuals are doing themselves. The perceived views of these people around the individual assist in determining the response of the person performing the behaviour. PBC can be defined as individual's perceptions of whether or not they can execute that specific behaviour, and the ease with which it can be performed.

In this chapter, the results in Chapter 5 (Data Analysis chapter) will be compared with results from previous studies, and will be discussed. Whether the findings of the current study agree or diverge from the previous studies will be addressed, and possible reasons for these findings are debated. This chapter commences a discussion of the major findings and compares them with findings from previous studies (section 6.2). Then, sections 6.3 and section 6.4 focus, respectively, on the theoretical and practical implications of the current study. The following section (6.5) discusses the limitations of this thesis, followed by section 6.6, which discusses recommendations and future work. Lastly, section 6.7 provides a conclusion to this chapter.

6.2 Major Findings

This thesis aimed to investigate the TPB factors to explain individual behavioural intention when responding to phishing emails under SEPS. This research examined: (1) the impact of TPB independent factors on the dependent factor under SEPS; (2) the factors of TPB having strongest influence in explaining the intentions behind individuals' behaviours when faced with phishing emails under SPES; and (3) the goodness of fit for the model under SEPS.

6.2.1 Major Finding 1

The TPB's independent factors (ATT, SN, and PBC) were found to be significant predictors of intention to respond to phishing emails under SEPS (Authority, Social Proof, Scarcity). This was supported by several researchers in the literature. For example, it has been stated by Yousafzai et al. (2010) and Tolliver (2016) that TPB has been used in numerous studies, and has proved to be a strong predictor of behavioural intention, in several fields and geographic locations. Furthermore, numerous studies found strong support for TPB usage (Alajmi, 2010; Sadeghi and Farokhian, 2011; Tsai et al., 2010). According to Armitage and Conner (2001), the most widely used social psychological theory is TPB, as it explains and predicts user behaviour in any given scenario. Additionally, according to Dunn et al. (2011), the likelihood of predicting intention and behaviour is increased by the TPB model.

In the current study, the three main independent factors of the TPB explain 53.8% of the variance in behavioural intention under the authority strategy. This means that under the authority strategy, 53.8% variance in behavioural intention can be predicted to attitude, subjective norms, and PBC. Additionally, the three main independent factors of the TPB explain 51.8% of the variance in behavioural intention under the social proof strategy. This means that, under the social proof strategy, 51.8% variance in behavioural intention can be predicted to attitude, subjective norms, and perceived behavioural control. Moreover, the attitude, subjective norms, and perceived behavioural control explain 49.8% of the variance in behavioural intention under the Scarcity strategy. This means that, under the Scarcity strategy, 49.8% variance in behavioural intention can be predicted to attitude, subjective norms, and perceived behavioural control.

Table 44 : Summary of the Variance in Behavioural Intention under SEPS

SEPS	Variance in Behavioural Intention
Authority	53.8% (moderate)
Social Proof	51.8% (moderate)
Scarcity	49.8% (moderate)

It can be seen from Table 44 (Hair et al., 2011; Sarstedt et al., 2014) that the TPB explains high to moderate values of the variance in behavioural intention under the authority, social proof, or scarcity strategy, or all of these. This supports what is mentioned in the literature; meta-analyses of correlational studies have suggested that intentions are moderately to highly associated with behaviour (Cohen et al., 2003).

A meta-analysis of approximately 190 studies relating to TPB supported the predictive power of the model, and found that TPB accounted for about 27-39% of the behavioural intention (Armitage and Conner, 2001). Furthermore, other researchers have shown the predictive power of TPB constructs on intention, with a range 39% according to Armitage and Conner (2001), and 50% for intention according to Hagger et al. (2002). A systematic review illustrated that the model is almost as good at anticipating intentions and behaviour pertaining to information security studies (such as compliance to information security policies); about 40% of the difference in intentions has been clarified in the survey research (Sommestad and Hallberg, 2013)

6.2.2 Major Finding 2

The findings of this study shows that attitude (ATT) has a significant influence on behavioural intention to respond to phishing emails under SEPS, and this supports research hypothesis 1. Furthermore, the attitude factor under both authority and social proof strategies was the highest value of beta ($\beta = .468$, $p < 0.01$) ($\beta = .431$, $p < 0.01$) respectively, which means that the factor ATT has the strongest impact on participants' behavioural intention to respond to phishing emails under the Authority and Social Proof strategies.

Consider a scenario, where an individual receives an email that appears to be from a government's authoritative figure, such as the Ministry of Health, requesting a download of a certain attachment, to protect from an on-going virus or the break-out of a pandemic (COVID-19). Additionally, consider another scenario, where an individual receives an email informing about an illegitimate activity on their account, creating a sense of urgency where there are chances an individual's account might be closed if no immediate action is taken. Moreover, the email provides a URL that directs the user to the phished webpage. There is a chance that the individual might panic and click the link, thus falling prey to the phishing attack.

In the above-mentioned scenarios, attackers use the Authority strategy – email appears to come from an institution of authority – to persuade the individuals to respond to the emails. The attackers also might understand and exploit the cultural factors of their targets and accordingly use suitable techniques. According to Hofstede, the KSA is considered as a power-driven (or power distance) and collectivist culture. So the attackers might send an email that appears to be from powerful authoritative entities (e.g., the Ministry of Health) requesting the performance of a particular action. Here, the attacker exploits the power distance as a cultural factor and uses the authority strategy to persuade the targets to respond to the phishing email. Collectivism is another

cultural factor that can be exploited by the attackers. For example, the attackers create a fake group on a social media app such as Facebook, with a title more favourable in the targeted culture (such as volunteering or working collectively for a suitable cause, and/or contributing in a survey), and send an email requesting to join the group. There is a chance that the attackers might demonstrate a fake number of members who joined the group, or participated in a particular activity. In this scenario, the hacker exploits the collectivist cultural factor, and by using the Social Proof technique (the email encourages the participants to carry out a certain action due to the fact that other people have already taken this act) persuades the target to respond and/or carry out phishing attacks.

In another Social Proof scenario, when an individual receives an email from social networking sites (Facebook, Instagram, Twitter, Swarm), with phrases mentioning a certain number of friends showing interest, the hacker might receive a response with the requested information. The individual might respond based on their belief or attitude, without considering the consequences of their actions. However, the individual might consider questions like, are such emails important or unimportant, favourable or unfavourable, useful or not useful.

The findings of the current research align with other studies, which confirms that attitude is a significant factor influencing an individual's behavioural intention (Arpaci and Baloglu, 2016; Bulgurcu et al., 2010; Burns and Roberts, 2013; Dinev and Hu, 2007; Flores and Ekstedt, 2014; Ifinedo, 2012; Jafarkarimi et al., 2016; Kumar et al., 2008; Lebek, 2014; Lee and Kozar, 2008; Ng and Rahim, 2005; Safa et al., 2016; Sommestad et al., 2015; Yao and Linz, 2008; Zhang and McDowell, 2009). For example, the effect of attitude on information security policies compliance intention (Bulgurcu et al., 2010; Ifinedo, 2011; Pahnila et al., 2007; Sommestad et al., 2015). There has been an immense support between the attitude factor and anti-spyware adoption (Dinev and Hu, 2007; Lee and Kozar, 2008) with regard to online privacy protection approaches (Burns and Roberts, 2013; Yao and Linz, 2008), updating anti-virus (Ng and Rahim, 2005), and adopting firewalls (Kumar et al., 2008), as well as using strong secure passwords (Zhang and McDowell, 2009).

Other studies, such as Anderson and Agarwal (2010), have determined that the attitude factor is related to intention, as it conducts security-related behaviour to protect their own computer from cybercriminal activities. Based on the rich seam of studies supporting the influence of attitude on user intention, it seems to be a significant factor of information security behaviour. Moreover,

the results of this research are in alignment with TPB, which demonstrates that attitude is one of the main predictors of behavioural intention (Ajzen, 1991).

The findings of this study also show that SN has a significant on behavioural intention to respond to phishing emails under SEPS, and this supports research hypothesis 2. Additionally, the SN factor under the Scarcity strategy was the highest value of beta (β =.490, $p < 0.01$), which means that the SN factor has the strongest impact on participants' behavioural intention to respond to phishing emails under the Scarcity strategy. The influence on the participants of important people such as their family and friends may impact their decision- making process. For example, when a user receives an email from an entertainment website such as Netflix, or a food-delivery application such as Hunger Station (widely used in the KSA), with phrases emphasising a short-term sale, or a limited-time offer requiring an immediate action. In such scenarios, the user takes into account the views of the people important to them (friends and family) – did they receive such an email before, did they respond to it, how highly have they spoken about the organisation/company? Here, the individual takes into consideration the opinions and beliefs of family and friends, rather than making their own decisions (Ryan, 1982; Sheppard et al., 1988). So, the impact of the participants' SN on the behavioural intention to respond to phishing emails under the Scarcity strategy happens, as the participants are probable to follow the trend in taking up the offers presented by different organisations.

The study result is similar to the results from several previous studies that supported the influence of SN on behavioural intentions (Bulgurcu et al., 2010; Hamidreza et al., 2020; Ifinedo, 2012; Ng and Rahim, 2005; Pahnila et al., 2007; Safa et al., 2015; Siponen et al., 2010; Sommestad et al., 2015). So, subjective norms seems to be an important element of behavioural intentions. Moreover, the results of this research are in alignment with TPB, which demonstrates that SN is one of the main predictors of behavioural intention (Ajzen, 1991).

Furthermore, the current study found that the PBC factor of TPB only has a significant impact on behavioural intention when responding to phishing email under the Authority strategy, while under the Social Proof and Scarcity strategies the factor did not have any significant impact. A study carried out by Safa et al. (2015), aimed at changing individuals' behaviour to conscious care behaviour in the information security area, also found that PBC does not have an impact on individuals' behaviour. The reason for the lack of impact from PBC might be the pre-set notion, where a certain idea is embedded in an individual's mind. The respondents had a different opinion

with respect to the provided emails in the survey, and preferred the perception having no relation with intention; most of the participants opted for the pre-set notion rather than their intended behaviour. Saudi culture is a collectivist society, with deeply embedded traditions and beliefs. When analysing a situation, a Saudi individual might prefer the pre-set notion of responding to certain emails, rather than being affected by the email's content. The traditions and beliefs take precedence over the phishing email. So, in the current study, Hypothesis 3 was not supported.

6.2.3 Major Finding 3

As described in Chapter 5, the model in the current study achieved the goodness of fit, which would show that Theory of Planned Behaviour (TPB) model might work well when applied to the intention of responding to phishing emails under SEPS in Saudi Arabian undergraduate students. Four GOF indices (NFI, TLI, CFI, and GFI) provided a good model fit score. This aligns with other studies, such as Burns and Roberts (2013), applying TPB to predict online safety behaviour, which also found that the TPB model achieved a good model fit.

6.3 Theoretical Implication

The three independent factors of TPB (ATT, SN, and PBC) were found to be significant factors of individual behavioural intention in responding to phishing emails under SEPS (Authority, Social Proof, Scarcity). Furthermore, the findings of the current study had a fit data model, which would specify Ajzen's TPB model may perform well when applied to the behavioural intent of responding to phishing emails under SEPS. The three independent factors of the TPB predicted and explained the power of the theory. An interesting theoretical outcome was the robust relation between Attitude under Authority and Social Proof and Subjective Norm under Scarcity. This strong relation enables the prediction and explanation of variance among TPB factors towards cybercriminal activities such as phishing emails. Theoretically, this indicates Ajzen's TPB might function similarly for cybercriminal activities such as phishing emails. There is a possibility that other unknown factors might be influenced by intention when responding to phishing emails under SEPS.

This research was conducted on Saudi Arabian undergraduate students studying at KFU; this presents an opportunity for other researchers to further test these theoretical findings on other countries, and cultures. Perhaps other organisations might be used; or maybe graduate students. Future researchers using the TPB might incorporate a relationship between Attitude under

Authority and Social Proof and Subjective Norm under Scarcity, and explore different pathways with different perspectives.

The current research aimed to evaluate the TPB, as developed by Ajzen, under different SEPS, when responding to phishing emails. The other popular theories might provide more explanation on the role of the independent factors of TPB Attitude, Subjective Norms, and Perceived Behaviour Control, and how these factors impact behaviour. For instance, Cialdini (2001) provided an insight on a person's need for the adoption of social proof during uncertain times. Cialdini (2001) asserted that people normally look at others in similar situations to make a decision during unknown times, thus emphasising the social norm of decision-making criteria (Cialdini, 2001). Several organisations are providing training and encouraging their employees to detect phishing emails; however, there is uncertainty among the employees and many employees are still unaware of the criteria for detecting phishing emails. Cialdini (2001) recommended considering normative influences when faced with uncertain situations. Other similar research (Glynn and Huge, 2007) acknowledged that normative influences are based on an individual's behaviour and opinion, encouraging people to consider others' opinions when faced with unknown and uncertain situations.

Cialdini did not incorporate the uncertainties of TPB studies, and a limited number of researchers have included the risk and uncertainties in their studies. TPB was used as a theoretical model by Quintal et al. (2010), who found the perceived uncertainties were impacted by attitudes to their study 'visiting Australia' among Asian Ethnicities, which involved uncertainty influenced by PBC. While these results are fascinating, they are distinctive to the nations of origin, and might not be applied to other countries and cultures using the TPB framework. Therefore, there is still ambiguity in terms of TPB uncertainties.

Another interesting note is that TPB does not include demographic factors (e.g., age and gender) in predicting an individual's behaviour. The addition of demographic factors in Ajzen's (2006) TPB model might present different results when predicting an individual's behaviour. The results of the current study involved demographic factors such as age, gender, and field of study in the survey, to evaluate an individual's response to phishing emails under SEPS. These demographic factors demonstrated a significant relationship with TPB. This suggests the demographic factors play a crucial role in evaluating an individual's behaviour when responding to phishing emails under SEPS. In addirion, there are other demographic factors that might provide

better insight when explored. Venkatesh, Morris and Ackerman (2000) suggested an individual's income plays a vital role during the decision-making process. Within the context of responding to phishing emails, income as a demographic factor might play a role in decision-making, as the income might be considered before responding to phishing emails.

Ajzen's (2006) TPB did not include emotional determinants of behaviour when predicting individuals' behaviour. However, its predecessor, TRA (Fishbein and Ajzen, 1980) included emotional variables such as anxiety, fear, and threat. Scholars may need to include emotional variables in studying an individual's responses to phishing emails. For example, when a user receives a phishing email saying their password is compromised, the anxiety levels might increase, as most individuals are aware of how confidential information is exploited. This might not only affect an individual's emotions, but also stress the person to take unknown steps, like responding to a phishing email by changing their password.

In conclusion, the three main independent factors of TPB (ATT, SN, and PBC) are useful in various contexts, and the current research's survey supports it with a data fit model. The utility of this theory is based on the operationalisation and measurement of TPB factors. Therefore, it can be decided that the TPB factors play a major role in determining an individual's behavioural intention when responding to phishing emails under SEPS. As mentioned earlier, other factors that predict the individual's behaviour are still unknown. There is an immense opportunity to further explore the relationships between TPB factors under different cultures, countries, and demographic factors.

6.4 Practical Implications

There are innumerable practical implications linked with the current study. The research found that there are several criteria to be evaluated when an individual receives a phishing email, especially when the individual has to make a decision, which might have a social context such as looking for others' opinions, and the reactions of family, friends, and authoritative figures involved. The training provided by employers regarding phishing email requires careful consideration, as any follow-up test phishing email might have consequences. The findings with regard to the impact of subjective norms when faced with phishing emails (e.g., a test phishing email sent by the organisation) suggest that the employee might seek colleagues' opinions in order to reply to the email. The attitude in similar scenarios is determined by the level of authority sending the email. For instance, if the sender is a senior manager or director, the employee might

have a more concerned attitude out of fear or respect for the authoritative figure. The influence of PBC in the same scenario might be the preconceived notion provided during the phishing email training. The employee might refer to the notes or training material and respond accordingly. Although the significance and effectiveness of the phishing scenarios and solutions are deeply discussed, social engineers are still exploiting human weaknesses, therefore, there is a need to develop solutions that understand and protect the human vulnerabilities.

6.4.1 Recommendations for University Faculties, Students, and Management

A deeper level of understanding of the characteristics influencing cyberattacks will enable educational institutions to develop effective curricula, consisting of individual's behaviour, persuading strategies, and in-depth analysis of types of cybercriminal activities, such as phishing emails. This will benefit and educate the students during their preparatory years. The undergraduate students during their prime years might still be unaware enough of cybercriminal activities such as phishing attacks; this means they are vulnerable to phishing activities, and phishers target individuals in the age range 18-25. The chances of being attacked by phishers, for this age group, are quite high (Kumaraguru et al., 2010; Sheng et al, 2010).

There are instances where a student might share their confidential information with friends or faculty out of respect or trust. Here, the student should be educated about the vulnerabilities involved in sharing of private information. The curriculum should develop effective security and privacy courses to educate the students and protect their confidential information. The students should be encouraged to share their experience with other students, as it might protect them.

The faculty should conduct a survey to learn about student's awareness about cybercriminal activities, as this provides an insight on the mindset of the students towards phishing emails. Social engineering methods are altering frequently, and the phishers are improving the phishing scenarios, therefore periodically the cybercriminal curriculum should be re-assessed.

6.4.2 Recommendations for Training and Awareness Programmes

As mentioned earlier, an educational curriculum should be designed to educate the students. For organisations, the employers should provide adequate training to their employees and periodically assess their cybercriminal awareness skills. A questionnaire should be distributed to learn about employees' weak areas, and an awareness programme should be arranged accordingly. Employees should be encouraged to report any cybercriminal attacks they face, either

in their personal or professional life. The awareness programme should be more manageable, so the employees do not take it as a stressful or burdening activity.

Respected academic leaders and professors play a vital role in educating students regarding cybercriminal activities, especially phishing. During the education process, the risk and uncertainty of successfully detecting phishing email should be considered. Furthermore, the teaching curriculum should include real-time scenarios of phishing emails, and different ways to avoid being phished. The current research suggests that higher education should not only include cybercriminal activities such as phishing in the curriculum, but also provide emphasis and education on the affects that phishing email causes in an individual's life.

6.5 Limitations of Study

There are some limitations in the current study as in any research. One of them is with TPB, as it does not take demographic factors and emotions into consideration when predicting an individual's behaviour. Emotions such as fear, happiness or sadness sometimes determine the action taken by an individual. When faced with cybercriminal attacks such as phishing emails, the individual might go through technology anxiety or stress.

Another limitation is that the current research focuses on TPB to evaluate individual responses to phishing emails. There were only three independent factors, attitude, subjective norms, and perceived behavioural control, and one dependent factor, intention, involved to explain and predict the individual's behaviour when responding to phishing attacks. Future researchers can also consider other behavioural theories, such as Protection Motivational Theory (PMT) and the Elaboration Likelihood Model (ELM) to explain and predict individual responses and compare the results with the current research.

A further limitation of the current study is that it used a scenario-based questionnaire rather than conducting a real vulnerability study. This was unavoidable, as the ethical considerations had to be considered. However, the chosen scenarios were designed to resemble closely the actual cybercriminal phishing email attacks.

The current research was limited to the KSA, as it has a unique culture that is different from other countries (Albladi, 2018). The current research, due to time constraints, could not examine and compare the effects of other countries on the research model. Another limitation of the current research is simply that it focused on undergraduate students in the age group 18-25. This might be a limitation as the results do not reflect the responses of other Saudi nationals. The

undergraduate student context is crucial, as the cybercriminals targeted individuals in the age group 18-24; the phishers are aware that individuals are more vulnerable in this age group.

A further limitation is the focus on three demographic factors (age, gender, and field of study) in only one university – KFU. This university has been selected as it is one of the most popular universities in the KSA, with advanced technology; it aims to enrich and develop knowledge for future competitive human capabilities, and provide sustainability to business development (KFU, 2022). Additionally, in 2019, the KFU database was hacked by cybercriminals (Nabbout, 2019). Further, more demographic factors such as income and employment status should be taken into consideration when evaluating an individual's behaviour when responding to cybercriminal activities such as phishing email. Future studies can investigate the vulnerabilities to different cybercriminal activities in different universities and demographic factors, and compare the results with the current research.

6.6 Suggestions for Future Research

The researcher offers numerous recommendations for upcoming research. There is a need for extra testing to be carried out to realise if the Attitude factor under Authority and Social Proof strategies and Subjective Norm under Scarcity strategy continue to be the major predictor of responding to phishing emails. Therefore, it is suggested to use different behavioural theories to determine the responses of the individual when responding to phishing emails.

There is a need to include cybercriminal activities in academic preparatory years, as most of the students might be unaware of social engineering attacks, like phishing and its tricks, and the strategies used by phishers to persuade the victim to respond to the attack. In addition, early education might create awareness and reduce the phishing responses. Al-Qurashi and other researchers (2020) recommended incorporating social engineering awareness training in the education institute's curriculum in the KSA, so the students can intelligently handle social engineering attacks. These outcomes align with the findings of Al Janabi et al. (2016), that there is a necessity for information security awareness in several educational sectors in the Kingdom of Saudi Arabia, after carrying out a number of social awareness studies in the educational sector. Referring to these studies, it is crucial for educational institutes to involve information security awareness and training as an essential part of their curriculum, to minimise the danger of social engineering attacks.

The researcher provided a relation between independent and dependent TPB variables under SEPS; this information might be used to develop an app, using advanced coding languages, that not only educates individuals but also understands their intentional behaviours to respond to phishing attacks.

The current research used SEPS in phishing emails to persuade the victim to respond to the emails. Future research might use different strategies, in order to provide deeper insight into the comprehensive framework and model, to predict user responses when faced with phishing emails. The current research used an online survey to record user responses to phishing emails.

The survey consisted of different email types based on the most frequently visited websites in only one country, which is the KSA. Future research might use different data collection techniques, such as interviews or case studies, and build the questions based on frequently visited websites in different geographic locations (e.g., Canada, USA or European countries). In addition to this, the results might be analysed from collected information and compared with the results of the current research to determine the differences between two cultures in responding to phishing emails.

The current research is limited to the TPB independent factors, ATT, SN, and PBC. Future research might include more independent variables to determine the relation with the dependent variable, intention. This would expand the horizon to deeply study the individual's intention, and determine the correlation among different variables to determine user responses to phishing emails.

Another suggestion is to include the role of uncertainty in future research, and take technology into consideration. Cialdini (2001) studied the role of uncertainty and it was determined that subjective norms influence the attitude and intention during uncertain circumstances. The concept of uncertainty is integrated in technology adoption by different theories such as the Task-Technology Fit Model (D'Ambra and Wilson, 2004). To sum up, there is a need to study the role of uncertainty with relation to technology. There are studies that placed emphasis on the role of uncertainty through the decision-making process. The theory of uncertainty orientation, by Sorrentino and Roney (2000), showed that individuals have different ways to handle uncertain circumstances. The uncertainty role is very closely linked with culture (Hofstede-Insights, 2021), and the KSA has the highest level of uncertainty. Therefore, the role of uncertainty should be studied from the lens of the country's culture when analysing the responses to phishing emails.

Another factor to be considered is the use of scientific user-motivation studies. There are innumerable insights from research that focus on this element and determine the different factors in relation to an individual's susceptibility. Future researchers might determine what motivates an individual's responses when faced with phishing emails. Considering qualitative analysis is highly recommended to explore this factor. Correspondingly, it might be beneficial to take technology anxiety or related emotions into account to determine how the intentional factor is affected when responding to phishing emails.

Financial variables might be related to the PBC factor, as individuals might believe their responses are based on their income and other responsibilities. It might be useful to conduct research among different groups of people, like students and working professionals. This might provide a better insight on the PBC factor, to determine if an individual indeed faces the pressure of pre-set notions.

Future research might consider more demographic factors, such as an individual's financial situation, when evaluating the responses towards phishing emails. The results with more demographic factors can be compared with the current research, to see the difference in individual intention.

6.7 Conclusion

This thesis started by discussing social engineering and focusing mainly on phishing attacks. The implications of phishing attacks are not only dangerous but also damaging. For many years, phishing attacks have been part of cyberspace. Although many precautionary steps are taken to prevent phishing attacks, studies and statistics have shown an increase in the attack rate, rather than a decrease. Phishers use different persuading strategies to prey on people's vulnerabilities, thereby creating an opportunity to attempt to phish the victim. These strategies are called SEPS, and the ones discussed in this thesis are Authority, Social Proof, and Scarcity.

To study the motivations behind responding to phishing emails attacks, Theory of Planned Behaviour (TPB) was used in the current research. As mentioned in the literature review, the theory is one of the most powerful and popular theories for predicting and explaining human behaviour. In addition, it is effectively proven by previous researchers to predict and explain the user's behavioural intention in different domains. With respect to TPB, user behavioural intentions towards clicking on phishing emails are studied from the lens of the TPB factors: Attitude, Subjective Norms, and Perceived Behavioural Control.

The phishers may study the culture of the country, organisation or society and act accordingly. Previous studies have described Saudi culture as power-driven; therefore, the emotions are exploited through new ways, like making the content of the message more persuasive, or impersonating a higher authority. Additionally, as Saudi culture is more inclined towards socialising, the phishers send an email to individuals, quoting other family and friends who have taken the survey. Out of social pressure or trust the individuals fall prey to phishing.

Therefore, the current research aimed to evaluate the TPB factors (i.e. Attitudes, Subjective Norms, and Perceived Behavioural Control) in order to predict and explain behavioural intentions of Saudi Arabian undergraduate students when responding to phishing emails under SEPS. The current research studied the impact of TPB independent factors on the dependent factor under SEPS, and found that TPB's independent factors (Attitude, Subjective Norms, and Perceived Behavioural Control) were significant predictors of intention to respond to phishing email under SEPS (Authority, Social Proof, Scarcity). Additionally, the current research examined the factors of TPB that have the strongest influence in explaining the intentions behind individuals' behaviours when faced with phishing emails under SEPS; it found that the Attitude factor was the strongest influence in explaining the intentions behind individuals' behaviours when faced with phishing emails, under both Authority and Social Proof strategies, while the Subjective Norms factor was the strongest influence in explaining the intentions behind individuals' behaviours when faced with phishing emails under the Scarcity strategy. Furthermore, it was found that the TPB model has a good model fit when applied to intention to respond to phishing emails. This indicates that the TPB model might work well when applied to the behavioural intention of Saudi Arabian undergraduate students to respond to phishing emails under SEPS .

References

Abass, I. (2018) 'Social engineering threat and defence: A literature survey', *Journal of Information Security*, pp. 257-264.

Aburrous, M., Hossain, M., Dahal, K., Bradford, U. and Thabatah, F. (2010) 'Experimental case studies for investigating ebanking phishing intelligent techniques and attack strategies', *Journal of Cognitive Computation*, 2 (3), pp. 242-253. https://link.springer.com/article/10.1007/s12559-010-9042-7

Acton, C., Miller, R., Fullerton, D. and Maltby, J. (2009) *SPSS for social scientists*. New York: Palgrave Macmillan.

Adler, E. S. and Clark, R. (2010). *An invitation to social research: How it's done* (4th edn.).Mason, OH: Cengage Learning.

Ainur, K., Sayang, D., Jannoo, Z. and Yap, W. (2017) 'Sample size and non-normality effects on goodness of fit measures in structure equation model', *Pertanika Journal of Science and Technology*, 25 (2), pp. 575-586.

Airehrour, D., Vasudevan Nair, N. and Madanian, S. (2018) 'Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user reflective mitigationmodel', *Information*, 9 (5), p. 110.

Ajzen, I. (1985) 'From intentions on to actions: A theory of planned behaviour' in Kuhl, J. and Beckman, J. (eds.) *Action-control: From cognition to behaviour*. Heidelberg: Springer.

Ajzen, I. (1991) 'The theory of planned behaviour', *Organisational Behaviour and HumanDecision Processes*, 50 (2), pp. 179-211.

Ajzen, I. (2001) 'Nature and operation of attitudes', *Annual Review of Psychology*, 52, pp. 27-58.

Ajzen, I. (2002) 'Perceived behavioural control, self-efficacy, locus of control, and the theory of planned behaviour', *Journal of Applied Social Psychology*, 32, pp. 665-683.

Ajzen, I. (2012) 'Martin Fishbein's legacy: The reasoned action approach', *The ANNALS of the American Academy of Political and Social Science*, 640 (1), pp. 11-27.

Ajzen, I. and Driver, B. (1992) 'Application of the theory of planned behaviour to leisurechoice', *Journal of Leisure Research*, 24 (3), pp. 207-224.

Ajzen, I. and Fishbein, M. (1980) *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I. and Klobas, J. (2013) 'Fertility intentions: An approach based on the theory of planned behaviour', *Demographic Research*, 29 (8), pp. 203–232. https://www.demographic-research.org/volumes/vol29/8/29-8.pdf

Ajzen, I. and Sheikh, S. (2013) 'Action versus inaction: Anticipated affect in the theory ofplanned behaviour' *Journal of Applied Social Psychology*, 43 (1), pp. 155-162. http://doi.org/10.1111/j.1559-1816.2012.00989.x

Akbar, N. (2014) *Analysing persuasion principles in phishing emails*. Master's Thesis.University of Twente, Enschede, Netherlands.

Al-abdan, R. (2020) 'Phishing attacks survey: Types, vectors, and technical approaches', *MDPI Future Internet*, 12 (10), pp. 1-39.

Al-abdulatif, A. (2018) *Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia*. Published Master's Thesis. University of Houston.

Al-arifi, H. Tootell and Hyland, P. (2012) 'A study of information security awareness andpractices in Saudi Arabia', *International Conference on Communications and InformationTechnology.*

Al-Izki, F. (2018) *Exploring the Organisational, Social and Cultural Factors Influencing those Employee Attitudes and Behaviours That Impact the Implementation of an Information SecurityCulture within Omani Organisations*. PhD thesis. University of Strathclyde.

Al-Janabi, S. and Al-Shourbaji, I. (2016) 'A Study of Cyber Security Awareness in Educational Environment in the Middle East', *J. Inf. Knowl. Manag*. (15).

Al-Mukahal, H. M. and Alshare, K. (2015) 'An examination of factors that influence the numberof information security policy violations in Qatari organisations', *Information and Computer Security*, 23 (1), pp. 102-118. http://doi.org/10.1108/ICS-03- 2014-0018

Al-Rasheed, A. (2001) 'Features of traditional Arab management and organisation in the Jordan business environment', *Journal of Transnational Management Development*, 6 (2), pp. 27-53.

AL-Sharif, H. (2014) *The Impact of Saudi Arabia's Societal Culture on Human Resource Management Practices within The Public and Private Sectors: The Case of Saudi ArabianAirlines*. PhD thesis. School of Engineering and Design, Brunei University.

Al-Shehry, A., Rogerson, S., Fairweather, N. B, and Prior, M. (2006) 'The motivations forchange towards e-government adoption: Case studies from Saudi Arabia', *eGovernment Workshop 06 (eGOV06)*. Brunel University.

Al-Thakhri, R. and Rees, C. (2008) 'Organisational change strategies in the Arab region: A review of critical factors', *Journal of Business Economics and Management*, 9(2), pp. 123-132.

Alas, R. (2006) 'Ethics in countries with different cultural dimensions', *Journal of BusinessEthics*, 69 (3), pp. 237-247.

Alaskar, M., Vodanovich, S. and Shen, K. N. (2015) 'Evolvement of information securityresearch on employees' behavior: A systematic review and future direction', *48th Hawaii International Conference on System Sciences.* http://doi.org/10.1109/HICSS.2015.508

Albakry, S., Vaniea, K., and Wolters, M. K.(2020) 'What Is This URL's Destination? Empirical Evaluation of Users' URL Reading,' *Proceedings of the 2020 CHI Conference on Human Factors in Computing System*, pp. 1-12.

Albladi, S. M. and Weir, G. R. S. (2018) *A user-centric framework for addressing vulnerability to social engineering in social networks: A mixed method study of a Saudi academic community*.PhD thesis. University of Strathclyde.

Aldahaban, F. (2016) *Exploratory study of the adoption and use of the smartphone technology in emerging region: Case of Saudi Arabia*. PhD thesis. Portland State University.

Aldawood, H. and Skinner, G. (2018) 'Educating and raising awareness on cyber security social engineering: a literature review', *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*. IEEE, 4-7 December. Wollongong, NSW, Australia. https://doi.org/10.1109/TALE.2018.8615162

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs - pitfalls and ongoing issues', *Future Internet*, 11 (3), pp. 1-19. https://www.mdpi.com/1999-5903/11/3/73

AlGahtani, S. S., Hubona, G. S. and Wang, J. (2007) 'Information technology (IT) in Saudi Arabia: Culture and the acceptance and use of IT', *Information & Management*, 44 (8), pp. 681-691.

Algarni, A. (2019) 'What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk', *Information 2019*, 10,p. 211.

Algarni, A., Xu, Y. and Chan, T. (2017) 'An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook', *European Journal of InformationSystems*, 26 (6), pp. 661-687.

AlGhamdi, D. Flechais, I and Jirotka, M. (2015) 'Security practices for households bankcustomers in the Kingdom of Saudi Arabia', *Symposium of Usable Privacy and Security*.USENIX Association.

Alghazo, J. and Kazimi, Z. (2013) 'Social engineering in phishing attacks in the eastern province of Saudi Arabia, *Asian Journal of Information Technology*, 12 (3), pp. 91-98.

AlHamar, M. (2010) *Reducing the risk of email phishing in the State of Qatar through effective awareness framework*. PhD thesis. Loughborough University.

Ali, M., and Brooks, L. (2008) 'Culture and IS: National cultural dimensions within IS discipline', *Proceedings of the 13th annual conference of the UK academy for informationsystems*. Bournemouth.

Aljabri, S. (2021) 'Cybersecurity awareness In Saudi Arabia', *International Journal of Research Publication and Reviews*, 2 (2), pp. 320-330.

Aljasir, S., Woodcock, A. and Harrison, S. (2013) 'Facebook in Saudi Arabia: Some aspects of Facebook usage by Saudi university students', *International Journal of Engineering and Technology*, 5 (1), p. 80.

Aljniebi, A. (2020). *Human behaviour in cyber security*. MSc Dissertation. The BritishUniversity in Dubai.

Aljumah, Y. and Ahmed, S. (2021) 'A novel approach to get awareness in Saudi Arabia regarding phishing attacks', *Proceedings of the 3rd international conference on electrical, communication and computer engineering.* Kuala Lumpur, Malaysia.

Alkahtani, H. (2018). *Raising the information security awareness level in Saudi Arabian organisations through an effective culturally aware information security framework*. PhD thesis. Loughborough University.

Alkahtani, H. K., Dawson, R. and Lock, R. (2015) 'Communication and effective email usage in Saudi Arabia', *BCS software quality management conference 2015*. Loughborough University. https://hdl.handle.net/2134/18274

Alkhaiwani, A. and Almalki, G. (2021) 'Saudi human awareness needs. A survey in how human causes errors and mistakes leads to leak confidential data with proposed solutions in Saudi Arabia', *2021 National Computing Colleges Conference*. https://ieeexplore.ieee.org/document/9428790

Allam, S., Flowerday, S. V. and Flowerday, E. (2014) 'Smartphone information security awareness: A victim of operational pressures', *Computers & Security*, 42, pp. 55-65. http://doi.org/10.1016/j.cose.2014.01.005

Allan, P. and Barbara, P. (2002) *Why Men Don't Have a Clue and Women Always Need More Shoes*.

Almaghrabi, T. and Dennis, C. (2010) 'Driving online shopping: Spending and behavioural differences among women in Saudi Arabia', *International Journal of Business Science and Applied Management*, 5 (1), pp. 31-47.

AlMindeel, R. and Martins, J. T. (2020) 'Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia', *Inf. Technol. People*, 34, pp. 770-788.

Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2016) 'A survey of cyber-security awareness in Saudi Arabia', *11th International Conference for Internet Technology and Secured Transactions.* Barcelona.

Alotaibi, N. and Mukred, M. (2022) 'Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA', *Technology in Society*, 68.

Alqarni, A. (2015) 'Educational technology in Saudi Arabia: A historical overview', *International Journal of Education, Learning and Development*, 3, pp. 62-69.

AlQurashi, R. K., Alzain, M. A., Soh, B., Masud, M. and Al-Amri, J. (2020) 'Cyberattacks and impacts: A case study in Saudi Arabia', *Int. J. Adv. Trends Comput. Sci. Eng.*, 9, pp. 217-224.

Alsanad, A. (2018) *The Blackmail Crime*. Riyadh: Committee for the Promotion of Virtue andthe Prevention.

Alsayed, A. and Bilgrami, A. (2017) 'E-banking security: Internet hacking, phishing attacks, analysis, and prevention of fraudulent activities', *Int. J. Emerg. Technol. Adv. Eng.*, 7 (1), p.110.

Alseadoon, I. (2014) *The Impact of Users' Characteristics on Their Ability to Detect Phishing Emails*. PhD thesis. Queensland University of Technology, Brisbane, Australia.

Alsharnouby M., Alaca, F. and Chiasson, S. (2015) 'Why phishing still works: User strategiesfor combating phishing attacks', *International Journal of Human-Computer Studies*, 69-82.

Alshehri, O. (2021) *Examining The Existing Reality of Using Social Media as E-learning Tool at an Emerging University in Saudi Arabia from The Viewpoint of Tutors and Students*. PhD thesis.University of Glasgow.

Alshumaim, Y. and Alhuassan, R. (2010) 'Current availability and use of ICT among secondary EFL teachers in Saudi Arabia: Possibility and reality', *ACADEMIA*, 523-532, King Saud University, College of Education – Dept. of Curriculum and Instruction.

Alsulami, M., Alharbi, F., Almutairi, H., Almutairi, B., Alotaibi, M., Alanzi, M., Alotaibi, K. and Alharthi, S. (2021) *Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia*. https://www.mdpi.com/2078-2489/12/5/208

Alvesson, M. (2002) *Understanding Organisational Culture*. London: Sage.

Alzahrani, A. (2015) 'Cyberbullying among Saudi's higher-education students: Implications for educators and policymakers', *World J. Educ*. 5 (3), pp. 15-26.

Alzubaidi, A. (2021) 'Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia', *Heliyon journal*, 7 (1). https://doi.org/10.1016/j.heliyon.2021.e06016

Anastasi, A. and Urbina, S. (1997) *Psychological Testing*. Hoboken: Prentice Hall.

Anawar, S., Kunasegaran, D. L., Mas'ud, M. and Zakaria, N. A. (2019) 'Analysis of phishing susceptibility in a workplace: A big five personality perspectives', *Journal of Engineering Science and Technology*, 14 (5), pp. 2865-2882.

Anthony, B. (2019) *Social Engineering: The Human Element of Cybersecurity*. Master's thesis. Utica College. https://www.proquest.com/openview/de962d722378732c5e7e2cb9049cf9a1/1?pq-origsite=gscholar&cbl=18750&diss=y

Anti-Phishing Working Group (2014) *Phishing Activity Trends Report, 4th Quarter*. https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

Anti-Phishing Working Group (2016) *Phishing Activity Trends Report, 1st Quarter*. https://docs.apwg.org//reports/apwg_trends_report_q1_2016.pdf

Arab News (2019) *Saudi Arabia in the crosshairs as cyber-raids target Gulf*. https://www.arabnews.com/node/1452756/saudi-arabia

Arab News (2020a) *Cybercriminals target Saudis with vaccine data fraud*. https://www.arabnews.com/node/1787841/saudi-arabia

Arab News (2020b) *Saudi targeted in new wave of financial scams.* https://www.arabnews.com/node/1760281/saudi-arabia

Arana, M. (2017) *How much does a cyberattack cost companies?* https://opendatasecurity.co.uk/how-much-does-a-cyberattack-cost-companies/

Armitage, C. J. and Conner, M. (2001a) 'Efficacy of the theory of planned behaviour: A meta-analytic review', *British Journal of Social Psychology*, 40 (4), pp. 471-499. http://doi.org/10.1348/014466601164939

Armitage, C. J. and Conner, M. (2001b) 'The theory of planned behaviour: Assessment of predictive validity and "perceived control"', *British Journal of Social Psychology*, 38 (1), pp. 35-54.

Arpaci, I. and Baloglu, M. (2016) 'The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates', *Computers in Human Behavior*, 56, 65-71. http://doi.org/10.1016/j.chb.2015.11.031

Atkins, B. and Huang, W. (2013) 'A study of social engineering in online frauds', *Open J. Soc.Sci*., 1 (3), pp. 23-32.

Avast (2020) *What is cybercrime and how can you prevent it?* https://www.avast.com/c-cybercrime#topic-1

Ayatollahi, H., Bath, P. A., Goodacre, S., Lo, S. Y., Draegebo, M. and Khan, F. A. (2013) 'What factors influence emergency department staff attitudes towards using information technology?' *Emergency Medicine Journal*, 30 (4), pp. 303-307. http://doi.org/10.1136/emermed-2011-200446

Ayob, Z. and Weir, G. (2021) 'Is human behaviour the real challenge in combating phishing', in Joelianto, E., Turnip, A. and Widyotriatmo, A. (eds) *Cyber Physical, Computer and AutomationSystem, Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-981-33- 4062-6_3

Babbie, E. (1998) *Survey Research Methods* (2nd edn.). Belmont, CA: Wadsworth.Babbie, E. (2013) *The practice of social research*. London: Wadsworth.

Bacon, D. (2004) 'The contributions of reliability and pre-tests to effective assessment', *Practical Assessment, Research and Evaluation*, 9 (3), pp. 31-36.

Badewi, A. (2013) *MIS Research Methodology Course (2) Positivism V.S Interpretivism*. http://misresearchmethodologies.blogspot.com/2013/03/mis-research-methodology-course- 2.html

Bagozzi, R. P. and Yi, Y. (2012) 'Specification, evaluation, and interpretation of structuralequation models', *Journal of the Academy of Marketing Science*, 40 (1), pp. 8-34. http://doi.org/10.1007/s11747-011-0278-x

Bakhshi, T., Papadaki, M. and Furnell, S. (2008) 'A practical assessment of social engineering vulnerability', *Proceedings of the second International Symposium on Human Aspects of Information Security & Assurance (HAISA)*.

Bandi, S. (2016) *An empirical assessment of user online security behavior: Evidence from a university*. Master's Thesis. University of Maryland, College Park, United States of America.

Bandura, A. (1982) 'Self-efficacy mechanism in human agency', *American Psychologist*, 37 (2), pp. 122-147.

Barron, B. J. S., Schwartz, D. L., Vye, N. J., Moore, A., Petrosino, A., Zech, L. and Bransford J. D. (1998) 'Doing with understanding: Lessons from research on problem and project-basedlearning', *The Journal of the Learning Sciences*, 7 (3/4), pp. 271-311.

Baumgartner, H. and Hombur, C. (1996) 'Applications of structural equation modelling in marketing and consumer research: A review', *International Journal of Research in Marketing*,13, pp. 139-161.

BBC (2020) *Google blocking 18m coronavirus scam emails every day*. https://www.bbc.com/news/technology-52319093

Beck, B. E. F. and Moore, L. F. (1985) 'Linking the host culture to organisational variables', in Frost (ed.) *Organisational Culture.* Beverly Hills: Sage, pp. 335-354.

Beck, L. and Ajzen, I. (1991) 'Predicting dishonest actions using the theory of planned behaviour', *Journal of research in personality*, 25 (3), pp. 285-301.

Beduz, M. (2014) *The Role of Attitudes, Subjective Norms, Perceived Behavioural Control, And Context In Nurses' Behavioural Intentions*. PhD thesis. McMaster University.

Benenson, Z., Gassmann, F. and Landwirth, R. (2017) 'Unpacking spear phishing susceptibility', *International Conference on Financial Cryptography and Data Security*. https://link.springer.com/chapter/10.1007/978-3-319-70278-0_39

Bentler, P. M. and Bonett, D. G. (1980) 'Significance tests and goodness of fit in the analysis of covariance structures' *Psychological Bulletin*, 88, pp. 588-606. https://psycnet.apa.org/record/1981-06898-001

Beville, J. M., Umstattd Meyer, M. R., Usdan, S. L., Turner, L. W., Jackson, J. C. and Lian, B. E. (2014) 'Gender differences in college leisure time physical activity: Application of the theory of planned behavior and integrated behavioural model', *Journal of American College Health*, 62(3), pp. 173–184.

Bezuidenhout, M., Mouton, F. and Venter, H. (2010) Social Engineering Attack DetectionModel: SEADM. *IEEE.*

Bhattacherjee, A. and Sanford, C. C. (2006) 'Influence processes for information technology acceptance: An elaboration likelihood model', *MIS Quarterly*, 30 (4), pp. 805-825.

Bhusal, C. (2021) 'Systematic Review on Social Engineering: Hacking by Manipulating Humans', *Journal of Information Security*, pp. 104-114.

Bielski, L. (2004) 'Phishing phace-off', *ABA Banking Journal*, 96 (9), p. 46.

Bik, O. P. G. (2010) *The Behaviour of Assurance Professionals: A Cross-cultural Perspective*. Utrecht: Eburon Uitgeverij BV.

Blythe, J. (2015) *Information Security in the Workplace: A Mixed-Methods Approach to Understanding and Improving Security Behaviours*. PhD thesis. Northumbria University.

Blythe, M., Petrie, H. and Clark, J. A. (2011) 'F for fake: Four studies on how we fall for phish', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ACM.* Vancouver.

Bobek, D. D., Hatfield, R. C. and Wentzel, K. (2007) 'An investigation of why taxpayers prefer refunds: A theory of planned behaviour approach', *The Journal of the American Taxation Association*, 29 (1), pp. 93-111.

Bock, G.W. and Kim, Y.G. (2002) 'Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing', *Info. Resour. Manage. J*. 15 (2), pp. 14-21.

Bond, M. H. (1988) 'Finding universal dimensions of individual variation in multicultural studies of values: The Rokeach and Chinese value surveys', *Journal of Personality and SocialPsychology*, 55(6), p. 1009.

Boodaei, M. (2012) Mobile users' three times more vulnerable to phishing attacks.

Borges, J. A. R., Tauer, L. W., Lansink, A. G. J. M. (2016) 'Using the theory of planned behavior to identify key beliefs underlying Brazilian cattle farmers' intention to use improvednatural grassland: A MIMIC modelling approach', *L. Use Policy* 55, pp. (193-203).

Breda, F., Barbosa, H. and Morais, T. (2017) 'Social engineering and cyber security', *Proceedings of the International Conference on Technology, Education and Development.*Valencia.

Brown, J. S., Collins, A. and Duguid, P. (1989) 'Situated cognition and the culture of learning', *Educational Researcher,* 18 (1), pp. 32-42.

Bryant, F. B., Yarnold, P. R. and Michelson, E. A. (1999) 'Statistical methodology: VIII. Using confirmatory factor analysis (CFA) in emergency medicine research', *Academic Emergency Medicine*, 6 (1), pp. 54-66.

Bryman, A. (2012) *Social research methods*. 4th edn. Oxford: Oxford University Press.

Bryman, A. and Bell, E. (2007) *Business Research Methods*, 3rd edn. Oxford: Oxford University Press.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance:An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, 34 (3), pp. 523-548.

Bullée, J. M. (2017) 'On the anatomy of social engineering attacks - a literature-based dissectionof successful attacks', *Journal of Investigative Psychology and Offender Profiling*, 15 (1), pp. 20-25. https://doi.org/10.1002/jip.1482

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M. and Hartel, P. H. (2015) 'The persuasion and security awareness experiment: Reducing the success of social engineering attacks', *Journalof experimental criminology*, 11 (1), pp. 97-115.

Bulmer, M. (1979) *Principles of Statistics*. 3rd edn. Mineola, NY: Dover Publications.

Burns, N. and Grove, S. (2011) *Understanding Nursing Research Building an Evidence-Based Practice*. 5th edn. Maryland Heights, MO: Elsevier.

Burns, S. and Roberts, L. (2013) 'Applying the theory of planned behaviour to predicting online safety behaviour', *Crime Prevention and Community Safety*, 15 (1), 48-64. http://doi.org/10.1057/cpcs.2012.13

Butler, R. (2005) 'An investigation of phishing to develop guidelines to protect the Internet consumer's identity against attacks by phishers', *The South African Journal of InformationManagement*, 7 (3).

Butler, R. (2007) 'A framework of anti-phishing measures aimed at protecting the online consumer's identity', *Electronic Library* 25 (5), pp. 517-533.

Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. (2015) 'Breaching the human firewall: Social engineering in phishing and spear-phishing emails', *Australasian Conference on Information Systems*. https://arxiv.org/abs/1606.00887

Byrne, B. M. (2010) *Structural Equation Modelling with AMOS*. 2nd edn. Oxford: OxfordUniversity Press.

Cabrera-Nguyen, P. (2010) 'Author guidelines for reporting scale development and validation results', *Journal of the Society for Social Work and Research*, 1 (2), pp. 99-103.

Calder, B. J., Phillips, L. W. and Tybout, A. M. (1982) 'The concept of external validity', *Journal of Consumer Research,* 9, pp. 240-244.

Cameron, K. S. and Quinn, R. E. (1999) *Diagnosing and Changing Organisational Culture*. Reading: Addison-Wesley.

Campos, H. (2021) *A study of phishing emails and their ability to mislead recipients depending on age and education level*. KTH Royal Institute of Technology.

Casebeer, A. L. and Verhoef, M. J. (1997) 'Combining qualitative and quantitative research methods: Considering the possibilities for enhancing the study of chronic diseases', *ChronicDiseases and Injuries in Canada*, 18 (3), p. 130.

Castanier, C., Deroche, T. and Woodman, T. (2013) 'Theory of planned behaviour and road violations: The moderating influence of perceived behavioural control', *Transportation ResearchPart F: Traffic Psychology and Behaviour*, 18, pp. 148-158. https://doi.org/10.1016/j.trf.2012.12.014

Cavaye, A. (1996) 'Case study research: a multi-faceted approach for IS', *Information Systems Journal*, 6 (4), pp. 227-242.

Chang, J. H. and Lee, K. H. (2010). Voice phishing detection technique based on minimum classification error method incorporating codec parameters. *IET signal processing*, 4(5), 502-509.

Chan, L. and Bishop, B. (2013) 'A moral basis for recycling: Extending the theory of planned behaviour', *Journal of Environmental Psychology*, 36, pp. 96-102. http://doi.org/10.1016/j.jenvp.2013.07.010

Chanti, S and Chithralekha, T. (2020) 'Classification of Anti-phishing Solutions' , *Social Netw. Comput. Sci*., vol. 1, no. 1, p. 11, Jan. 2020.

Chao, H. P. (1998) *Relationship among Attitudes, Subjective Norms, Perceived Behavioral Control and Intention: An Example of Elementary School Students Participating RecreationSport Camp*. Master's dissertation. National College of Physical Education and Sports, Tao Yuen, Taiwan.

Chatterjee, S., Sarker, S. and Valacich, J. S. (2015). 'The behavioral roots of information systems security: Exploring key factors related to unethical IT use', *Journal of ManagementInformation Systems*, 31 (4), 49-87. http://doi.org/10.1080/07421222.2014.1001257

Chen, H. and Li, W. (2014) Understanding organisation employee's information security omission behavior: An integrated model of social norm and deterrence', *Pacific Asia Conferenceon Information Systems 2014 Proceedings*. Chengdu, China. http://aisel.aisnet.org/pacis2014/280

Chen, R., Gaia, J. and Rao, H. R. (2020) *An examination of the effect of recent phishing encounters on phishing susceptibility.* https://www.sciencedirect.com/science/article/pii/S0167923620300427?via%3Dihub

Chen, Y., Ramamurthy, K. and Wen, K. W. (2012) 'Organisations' information security policy compliance: Stick or carrot approach?', *Journal of Management Information Systems*, 29 (3), pp.157-188.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013) 'Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrencetheory', *Comput Secur* 39 (B), pp. 447-459. http://dx.doi.org/10.1016/j.cose.2013.09.009

Chowdhury, N., Adam, M. and Skinner, G. (2018) 'The impact of time pressure on human cybersecurity behaviour: An integrative framework', *6th International Conference on SystemsEngineering (ICSEng)*. https://ieeexplore.ieee.org/document/8638250

Churchill, G. A. (1979) 'A paradigm for developing better measures of marketing constructs', *Journal of Marketing Research*, 16 (February), pp. 64-73.

Cialdini, R. (2001) *Influence: Science and practice*. Boston: Pearson Education. Cialdini, R. (2007) *Influence: The Psychology of Persuasion*. New York: Harper Collins.

Cialdini, R., Kallgren, C. A. and Reno, R. R. (1991) 'A focus theory of normative conduct: A theoretical refinement and re-evaluation of the role of norms in human behaviour', in Zanna, M.(ed.) *M. P. Advances in Experimental Social Psychology*, *Vol. 24*. New York: Academic Press, pp. 201-234.

CISCO. (2021) *Think Before You Click.* https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Collis, J. and Hussey, R. (2003) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. 2nd edn. Basingstoke: Palgrave Macmillan.

Collis, J. and Hussey, R. (2009) *Business research: A Practical Guide for Undergraduate and Postgraduate students*. 3rd edn. New York: Palgrave Macmillan.

Conner, M. and Armitage, C. J. (1998) 'Extending the theory of planned behaviour: A reviewand avenues for further research', *Journal of Applied Social Psychology*, 28, pp. 1430-1464.

Conner, M. and Sparks, P. (2005) 'The theory of planned behaviour', in Conner, M. and Norman, P. (eds) *Predicting Health Behaviour: Research and Practice with Social CognitionModels.* Buckingham: Open University Press, pp. 121-162.

Connolly, L., Lang, M. and Tygar, D. (2014) 'Managing employee security behaviour in organisations: The role of cultural factors and individual values', *IFIP International federation for information processing conference.* https://link.springer.com/chapter/10.1007/978-3-642- 55415-5_35

Consumer Reports (2006). Don't bite at phishers' email bait.

Conteh, N. and Schmick, P. (2016) 'Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research*, 6 (23), pp. 31-38.

Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S. and Chen, F. (2017) 'A qualitative investigation of bank employee experiences of information security and phishing', *Thirteenth Symposium on Usable Privacy and Security.*

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J. and Rovira, E. (2012) 'The influences of social networks on phishing vulnerability', *45th Hawaii International Conferenceon System Sciences.* https://doi.org/10.1109/HICSS.2012.657

Cortina, J. (1993) 'What is coefficient alpha? An examination of theory and applications', *Journal of Applied Psychology*, 78 (1), pp. 98-104.

Costa, P., Terracciano, A. and McCrae, R. R. (2001) 'Gender differences in personality traits across cultures: Robust and surprising findings', *Journal of personality and social psychology*,81 (2), pp. 322-331. https://pubmed.ncbi.nlm.nih.gov/11519935/

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 2nd edn. London: Sage.

Creswell, J. W. (2014) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 4th edn. New York: Sage.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M. and Baskerville, R. (2013) 'Future directions for behavioural information security research', *Computers and Security*, 32, pp. 91- 101.

Crossley and Jansen (2021) *Saunders' Research Onion: Explained Simply*. https://gradcoach.com/saunders-research-onion/

Crotty, M. (1998) *The Foundations of Social Research: Meaning and Perspective in theResearch Process*. Sage.

Cyren. (2020). Cyren cyber threat report 2020.

Dadfar, A., Norberg, R., Helander, E., Schuster, S. and Zufferey, A. (2003) *Intercultural Aspects of Doing Business with Saudi Arabia*. http://docplayer.net/36084348-Intercultural-aspects-of-doing-business-with-saudi-arabia.html

Dadfar, H. (1990) *Industrial Buying Behaviour in the Middle East*. Linkoping: Linkoping University.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017) 'Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace', *Computers in Human Behavior*, 67, pp. 196-206. http://doi.org/10.1016/j.chb.2016.10.025

Darwish, A., El Zarka, A. and Aloul, F. (2012) 'Towards understanding phishing victims'profile', *Proceedings of International Conference on Computer Systems and Industrial Informatics*. Sharjah, United Arab Emirates.

Datareportal (2020) *Digital 2020: Saudi Arabia*. https://datareportadatel.com/reports/digital-2020-saudi-arabia

David Bisson, (2020) *6 Common Phishing Attacks and How to Protect Against Them.* https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

Dawn, M. Joanna, L. Corey, B and Mark, N. (2019) Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *SAGE Journal*.

Dawson, L., Mullan, B. and Sainsbury, K. (2014) 'Using the theory of planned behaviour tomeasure motivation for recovery in anorexia nervosa', Appetite (84) pp. 309-315. https://pubmed.ncbi.nlm.nih.gov/25450891/

Daxini, A. (2019) *An Examination of The Factors which Influence Farmers' Intentions Towards The Implementation of Nutrient Management Planning*. PhD thesis. University of Edinburgh.

De Leeuw, A., Valois, P., Ajzen, I. and Schmidt, P. (2015). 'Using the theory of planned behaviour to identify key beliefs underlying pro-environmental behavior in high-school students:Implications for educational interventions', *Journal of Environmental Psychology*, 42, pp. 128- 138. http://doi.org/10.1016/j.jenvp.2015.03.005

De Martino, B., Kumaran, D., Seymour, B. and Dolan, R. (2006) 'Frames, biases, and rational decision-making in the human brain', *Science*, 313 (5787), pp. 684-687.

DeLyser, D. and Sui, D. (2013) 'Crossing the qualitative-quantitative divide II: Inventive approaches to big data, mobile methods, and rhythm analysis', *Progress in Human Geography*,37(2), pp. 293-305. http://doi.org/10.1177/0309132512444063

Denno, J. (2016) *Attacking The Human – The Weakest Link In Cybersecurity*. Master's thesis.Utica College.

Denscombe, M. (2007) *The Good Research Guide*. 2nd ed. London: Open University Press and McGraw-Hill.

Denzin, N. K. (2000) 'Aesthetics and the practices of qualitative inquiry', *Qualitative Inquiry*, 6 (2), pp. 256-265.

Deutsch, M. and Gerard, H. B. (1955) 'A study of normative and informational social influences upon individual judgement', *Journal of Abnormal and Social Psychology*, 51 (3), pp. 629-636.

Dhamija, R., Tygar, J. D. and Hearst, M. A. (2006) 'Why phishing works', *Proceedings of theCHI Conference on Human Factors in Computing Systems*. Quebec, 24-27 April. New York: ACM Press. https://dl.acm.org/doi/10.1145/1124772.1124861

Dinev, T. and Hu, Q. (2007) 'The centrality of awareness in the formation of user behavioral intention toward protective information technologies', *Journal of the Association for InformationSystems*, 8(7), pp. 386-408. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1325&context=jais

Dodge, R., Coronges, K. and Rovira, E. (2012) 'Empirical benefits of training to phishing susceptibility', *IFIP International Information Security Conference*. https://www.researchgate.net/publication/266201895_Empirical_Benefits_of_Training_to_Phishing_Susceptibility

Donald, I. J., Cooper, S. R. and Conchie, S. M. (2014) 'An extended theory of planned behaviour model of the psychological factors affecting commuters' transport mode use', *Journal of Environmental Psychology*, 40, pp. 39-48.

Downs, J., Holbrook, M. and Cranor, L. (2006) 'Decision strategies and susceptibility to phishing', *Proceedings Second Symposium on Usable Privacy and Security*. 12-14 July. NewYork. Pittsburgh: ACM Press.

Dunn, K. Mohr, P. Wilson, C. and Wittert, G. (2011) 'Determinants of fast-food consumption.An application of the theory of planned behaviour', Appetite, 57 (2), pp. 349-357. http://doi.org/10.1016/j.appet.2014.10.028

Eagly, A. H. and Chaiken, S. (1993) *The Psychology of Attitudes*. Orlando, FL: Harcourt Brace Jovanovich College Publishers.

Easterby-Smith, M., Thorpe, R. and Lowe, A. (1991) *Management research: An Introduction*. London, Sage.

Easterby-Smith, M., Thorpe, R. and Jackson, P. R. (2012) *Management Research*. 4th edn.London: Sage.

Efrat, K. and Shoham, A. (2013) 'The theory of planned behavior, materialism, and aggressive driving', *Accident Analysis and Prevention*, 59, pp. 459-465.

Elnaim, B. and AlLami, H. (2017) 'The current state of phishing attacks against Saudi Arabia University students', *International Journal of Computer Applications Technology and Research*,6 (1), pp. 42-50.

Emigh, A. (2005) Online identity theft: phishing technology, chokepoints and countermeasures.

Epule, E., Peng, C., Lepage, L. and Chen, Z. (2011) 'Forest Loss Triggers in Cameroon: A Quantitative Assessment Using Multiple Linear Regression Approach', *Journal of Geography and Geology*, 3 (1), pp. 30-41.

Erb, K. (2018) *IRS warns on surge of new email phishing scams*. https://www.forbes.com/sites/kellyphillipserb/2018/12/04/irs-warns-on-surge-of-new-email-phishing scams/#3ae1aba14b24

F5 Labs (2017) *Lessons Learned from a Decade of Data Breaches.* https://www.f5.com/content/dam/f5/downloads/F5_Labs_Lessons_Learned_from_a_Decade_of_Data_Breaches_rev.pdf

Fagoyinbo, I. S., Akinbo, R. Y., Ajibode, I. A. and Dosunmu, A. O. (2011) 'Statistical analysison the awareness and safe guarding against social engineering', *Journal of Educational and Social Research*, 1 (2), pp. 115-120.

Fatima, S. and Naima, K. (2019) Social Engineering Attacks: A Survey. *Future internet*.

Felten, E. W., Balfanz, D., Dean, D. and Wallach, D. S. (1997) 'Web spoofing: An internet con game', *Proceedings of the Twentieth National Information Systems Security Conference*. Baltimore.

Ferguson, A. J. (2005) 'Cognitive reflection and decision making', *J. Econ. Perspect*., 16 (4), pp. 25-42.

Ferreira, A., Coventry, L. and Lenzini, G. (2015) 'Principles of persuasion in social engineering and their use in phishing', *International Conference on Human Aspects of Information Security,Privacy, and Trust*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-20376-8_4

Fishbein, M. and Ajzen, I. (1975) *Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research*. Boston: Addison-Wesley.

Fitzgerald, B. and Howcroft, D. (1998) 'Towards dissolution of the IS research debate: From polarisation to polarity', *Journal of Information Technology*, 13 (4), pp. 313-326.

Flores, W. R., Antonsen, E. and Ekstedt, M. (2014) 'Information security knowledge sharing in organisations: Investigating the effect of behavioral information security governance and national culture', *Computers & Security*, 43, pp. 90-110. http://doi.org/10.1016/j.cose.2014.03.004

Fornell, C. and Larcker, F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, 18(1), pp. 39-50.

Forte, D. (2009) 'Phishing in depth', *Network Security UK*, 2009 (5), pp. 19-20.

Fraenkel, J. R., Wallen, N. E. and Hyun, H. H. (1993) *How to design and evaluate research in education*. New York: McGraw-Hill.

Frauenstein, E. (2021) *A Personality-Based Behavioural Model: Susceptibility to Phishing on Social Networking Sites*. PhD thesis. Rhodes University.

Furnell, S. (2007) 'Phishing: can we spot the signs?', *Computer Fraud & Security*, 2007 (3), pp. 10-15.

Gabrilovich, E. and Gontmakher, A. (2002) 'The homograph attack', *Communications of theACM*, 45 (2), p.128.

Galliers, R. D. (1992) *Information Systems Research: Issues, Methods and Practical Guidelines*. Oxford: Blackwell.

Gartner (2002) *There Are No Secrets: Social Engineering and Privacy.*https://www.gartner.com/en/documents/345370

Garver, S. and Mentzer, T. (1999) 'Logistics research methods: Employing structural equation modelling to test for construct validity' *Journal of Business Logistics*, 20 (1), pp. 33-57.

Gaskin, J. (2021) *Gaskination's StatWiki.* http://statwiki.gaskination.com/index.php?title=Data_Prep#Outliers

George, D. and Mallery, P. (2003) *SPSS for Windows step-by-step: A simple guide andreferences*. 4th edn. Boston: Allyn and Bacon.

Gill, J. and Johnson, P. (2002) *Research Methods for Managers*. London: Sage.

Goertz, G. and Mahoney, J. (2013) 'Methodological Rorschach tests: Contrasting interpretationsin qualitative and quantitative research', *Comparative Political Studies*, 46 (2), pp. 236–251. http://doi.org/10.1177/0010414012466376

Gokhale, A. and Waghmare, V. (2016) 'The shoulder surfing resistant graphical password authentication technique', *7th International Conference on Communication, Computing and Virtualisation*.

Gorling, S. (2006) 'The myth of user education', *Proceedings 16th Virus Bulletin International Conference.*

Gorsuch, R. (1983) *Factor Analysis*., Hillsdale, NJ: Erlbaum.

Gosling, S. D., Vazire, S., Srivastava, S. and John, O. P. (2004) 'Should we trust web-based studies? A comparative analysis of six preconceptions about internet questionnaires', *American Psychologist*, 59 (2), pp. 93-104.

Granato, D., de Araújo Calado, V. M. and Jarvis, B. (2014) 'Observations on the use of statistical methods in food science and technology', *Food Research International*, *55* (October), pp. 137- 149. http://doi.org/10.1016/j.foodres.2013.10.024

Gray, D. E. (2014). *Doing research in the real world*. 2nd edn. London: Sage.

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), pp. 149-172. https://link.springer.com/article/10.1023/B:GRUP.0000021839.04093.5d

Greaves, M., Zibarras, L. D. and Stride, C. (2013) 'Using the theory of planned behavior toexplore environmental behavioural intentions in the workplace', *Journal of Environmental Psychology*, 34, pp. 109-120. http://doi.org/10.1016/j.jenvp.2013.02.003

Greenspan, S. (2008) 'Annals of Gullibility: Why We Get Duped and How to Avoid It.Westport, CT: Praeger.

Griffin, R. (2017) *Evaluating the impact of training and education to counteract socialengineering attacks in organisations*. Dublin: Dublin Institute of Technology.

Griffin, R. (2018) *A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks.* Masters dissertation. DIT University.

Grinnell, M. (2011) *Social Work Research and Evaluation: Quantitative and Qualitative Approaches*. New York: F. E. Peacock.

Guba, E. G. and Lincoln, Y. S. (1994) 'Competing Paradigms in Qualitative Research', *Handbook of Qualitative Research*, 2 (163-194), p. 105.

Guéguen, N. and Jacob, C. (2002) 'Solicitation by email and solicitor's status: A field study of social influence on the web', *CyberPsychology & Behaviour*, 5 (4), pp. 377-383.

Guin, T., Baker, R., Mechling, J. and Ruylea, E. (2012) 'Myths and realities of respondent engagement in online surveys', *International Journal of Market Research*, 54, pp. 1-21.

Gulati, R. (2003) *The Threat of Social Engineering and Your Defence Against It*. https://www.sans.org/white-papers/1232/

Gupta, B. B., Arachchilage, N. A. and Psannis, K. E. (2018) 'Defending against phishing attacks: Taxonomy of methods, current issues, and future directions', *Telecommunication Systems*, 67 (2), pp. 247-267.

Hadnagy, C. (2011) *Social Engineering: The Art of Human Hacking*. Wiley.

Hagger, M. S., Chatzisarantis, N. L. D. and Biddle, S. J. (2002) 'A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables', *Journal of Sport and Exercise Psychology*, 24 (1), pp. 3-32. http://psycnet.apa.org/psycinfo/2002-12499-001

Hair, J., Black, B., Babin, B., Anderson, R. and Tatham, R. (2006) *Multivariate Data Analysis*.6th edn. NJ: Pearson, Prentice Hall.

Hair, J., Black, W., Babin, B. and Anderson, R. (2010). *Multivariate Data Analysis: A Global Perspective*. 7th edn. NJ: Pearson, Prentice Hall.

Hair, J., Hult, G., Ringle, C. and Sarstedt, M. (2014) *A Primer on Partial Least SquaresStructural Equation Modelling (PLS-SEM)*. Los Angeles: Sage.

Hair, J., Hult, G., Ringle, C. and Sarstedt, M. (2017) *A Primer on Partial Least SquaresStructural Equation Modelling (PLS-SEM).* 2nd edn. Los Angeles: Sage.

Halevi, T., Memon, N. and Nov, O. (2015) *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy, and Vulnerability to Spear-Phishing Attacks*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742

Hamid, M. Sami, W. and Sidek, M. (2017) 'Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion', *Journal of Physics*.

Harding, T. S; Mayhew, M. J.; Finelli, C. J and Carpenter, D. D. (2007) 'The theory of planned behaviour as a model of academic dishonesty in engineering and humanities undergraduates', *Ethics & Behavior*, 17 (3), pp. 255-279.

Harl, G. (1997) *People Hacking - The Psychology of Social Engineering*. Text of Harl's Talk at Access All Areas III.

Harris, P., Middleton, W. and Joiner, R. (2000) 'The typical student as an in-group member: Eliminating optimistic bias by reducing social distance', *European Journal of Social Psychology*,30 (2), pp. 235-253. https://psycnet.apa.org/record/2000-08209-006

Hathaway, M., Spidalieri, F. and Alsowailm, F. (2017) *Kingdom of Saudi Arabia: CyberReadiness at a Glance*. Arlington, VA: Potomac Institute for Policy Studies.

Hesse-Biber, S. N. and Leavy, P. (2011) *The Practice of Qualitative Research*. 2nd edn.

Herzberg, A. and Jbara, A. (2004) *Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks*. https://dl.acm.org/doi/10.1145/1391949.1391950

Herzberg, A. (2009) 'Why Johnny can't surf (safely)? Attacks and defences for web users', *Computers & Security*, 28 (1-2), pp. 63-71.

Hill, C. E., Loch, K. D., Straub, D. W. and El-Sheshai, K. (1998) 'A qualitative assessment of Arab culture and information technology transfer' *Journal of Global Information Management*,6, pp. 29-38.

Hinz, O., Nofer, M., Schiereck, D. and Trillig, J. (2015) 'The influence of data theft on the share prices and systematic risk of consumer electronics companies', *Information & Management*, 52 (3), pp. 337-347. https://doi.org/10.1016/j.im.2014.12.006.

Ho, G., Sharma, A., Javed, M., Paxson, V. and Wagner, D. (2017) 'Detecting credential spear phishing in enterprise settings', *Proceedings of the 26th USENIX Security Symposium.*Vancouver.

Hoe, S. (2008) Issues and procedures in adopting structure equation modelling technique. *Journal of Applied Quantitative Methods*, 3(1), 76-83.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work-Related Values*. Thousand Oaks, CA: Sage.

Hofstede, G. (1984) *Culture's Consequences: International Differences in Work-Related Values*, Volume 5. Thousand Oaks, CA: Sage.

Hofstede, G. (1993) '*Cultural constraints in management theories*', The Executive, 7 (1), pp. 81-94.

Hofstede, G. (1998) *Masculinity and Femininity: The Taboo Dimension of National Cultures*. Thousand Oaks, CA: Sage.

Hofstede, G. (2001) *Culture's Consequences: Comparing Values, Behaviours, Institutions, and Organisations Across Nations*. London: Sage.

Hofstede, G. (2005) *Cultures and Organisations: Software of the Mind*. McGraw-Hill.

Hofstede, G., Hofstede, G. J. and Minkov, M. (2010) *Cultures and Organisations: Software ofThe Mind*. 3rd edn. New York: McGraw-Hill.

Hofstede-Insights (2021) *Country Comparison.* https://www.hofstede-insights.com/country-comparison/

Hong, J. (2012) 'The state of phishing attacks', *Commun ACM*, 55 (1), pp. 74-81.

Hooper, D., Coughlan, J. and Mullen, M. (2008) 'Structural equation modelling: Guidelines for determining model fit' *Journal of Business Research*, 6 (1), pp. 53-60.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) 'Managing employee compliance with information security policies: The critical role of top management and organisational culture', *AJournal of The Decision Sciences Institute*, 43 (4), pp. 615-659. http://doi.org/10.1111/j.1540- 5915.2012.00361.x

Huck, C. W. (2004) *Reading Statistics and Research*. Boston: Pearson. Hussey, J. and Hussey, R. (1997) *Business Research*. Basingstoke: Palgrave.

Hyland, J. J., Heanue, K., McKillop, J. and Micha, E., (2018). 'Factors underlying farmers' intentions to adopt best practices: The case of paddock based grazing systems', *Agric. Syst*. 162,pp. 97-106.

IBM (2020) *IBM X-Force Threat Intelligence Index 2020*. https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf

Ifinedo, P. (2012) 'Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory', *Computers& Security*, 31 (1), pp. 83–95. http://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014) 'Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition', *Information and Management*. 51 (1), pp. 69-79.

Infosec (2013) *Social engineering: A hacking story*. https://resources.infosecinstitute.com/topic/social-engineering-a-hacking-story/

Iuga, C., Nurse, J. R. and Erola, A. (2016) 'Baiting the hook: Factors impacting susceptibility to phishing attacks', *Human-Centric Computing and Information Sciences*, 6 (1), p. 8.

Jacob, J. (2013) *Security Behaviour of System Professionals on their Home Computer*. MSc Dissertation. University of Dublin.

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H. and Hee, J. M. (2016) 'Behavioral intention insocial networking sites ethical dilemmas: An extended model based on theory of planned behaviour', *Computers in Human Behavior*, 62, pp. 545-561. http://doi.org/10.1016/j.chb.2016.04.024

Jagatic, T., Johnson, N., Jakobsson, M. and Menczer, F. (2007) *Social Phishing.* https://www.researchgate.net/publication/220424040_Social_phishing

Jain, K. and Gupta, B. (2018) 'Two-level authentication approach to protect from phishing attacks in real time', *Journal of Ambient Intelligence and Humanised Computing*, 9 (6), pp.1783-1796.

Jayatilaka, A. and and Arachchilage, N. (2021) 'Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors', *Forty-Second International Conference on Information Systems, Austin 2021*.

Jakobsson, M. and Myers, S. (2006) *Phishing and Countermeasures: Understanding theIncreasing Problem of Electronic Identity Theft.* Hoboken, NJ: Wiley.

Jakobsson, M. (2007) 'The human factor in phishing', *Privacy & Security of ConsumerInformation* (7), pp. 1-19.

Jalali, M. Bruckes, M. Westmattelmann, D .and Schewe, G. (2020) 'Why Employees (Still)Click on Phishing Links: Investigation in Hospitals', *J Med Internet Res*, 22 (1): e16775.

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Alam, S. M. and Ashraf, R. (2018) 'MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook', *2018 IEEE International Conference on Big Data*. https://ieeexplore.ieee.org/document/8622505

Javadi, M., Kadkhodaee, M., Yaghoubi, M., Maroufi, M. and Shams, A. (2013) 'Applying theory of planned behavior in predicting of patient safety behaviors of nurses', *Materia Socio Medica*, 25, pp. 52-55.

Jiang, L., Zhang, J., Wang, H. H., Zhang, L., He, K. (2018) 'The impact of psychological factors on farmers' intentions to reuse agricultural biomass waste for carbon emission abatement', *Journal of Cleaner Production*, 189, pp. 797-804.

Johnson, D. (2017) *How Attitude Toward the Behaviour, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behaviour Intention*. PhD thesis. WaldenUniversity.

Johnson, P. and Clark, M. (2006) *Business and Management Research Methodologies.* London: Sage.

Johnson, R. B. and Christensen, L. B. (2004) *Educational research: Quantitative, Qualitative,and Mixed approaches*. Boston: Allyn and Bacon.

Johnston, A. C. and Warkentin, M. (2010) 'Fear appeals and information security behaviours: An empirical study', *MIS Quarterly*, 34 (3), pp. 549-566.

Jung, B. and Kim, S. (2014) 'A festival satisfaction evaluation method using multiple regression analysis', *International Journal of Software Engineering and Its Applications*, 8 (4), pp. 187- 196. http://doi.org/10.14257/ijseia.2014.8.4.20

Kabasakal, H. and Bodur, M. (2002) 'Arabic cluster: A bridge between East and West', *Journalof World Business*, 37 (1), pp. 40-54.

Kalnins, R., Purins, J., Alksnis, G. (2017) 'Security evaluation of wireless network accesspoints', *Appl. Comput. Syst*. 21, pp. 38-45.

Karakasiliotis, A., Furnell, M. S. and Papadaki, M. (2006) 'Assessing end-user awareness ofsocial engineering and phishing', *Proceedings of 7th Australian Information Warfare and Security Conference.*

Kasi, P. (2009) *Research: What, Why and How? A Treatise from Researchers to Researchers.* Bloomington: Author House.

Katadae, A. (2000) *Phenomenological Understanding of the Meaning in Lifeworld: Bridging Philosophy and Research Methodology.* Olive Kagawa University Information repository, pp. 11-19.https://kagawau.repo.nii.ac.jp/?action=repository_action_common_download&item_id=2001&item_no=1&attr ibute_id=22&file_no=1

KFU (2022) *King Faisal University*. https://www.kfu.edu.sa/ar/pages/home.aspx

Kim, D., and Kim, J. H. (2013) 'Understanding persuasive elements in phishing emails: a categorical content and semantic network analysis', *Online Information Review* , 37(6), 2-2.

Kleitman, S., Law, M. K., and Kay, J. (2018) 'It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLOS One*, *13*(10).

Klenke, K. (2008) *Qualitative Research in The Study of Leadership*. Bradford: Emerald Group Publishing.

Kline, R. B. (2010) *Principles and Practice of Structural Equation Modelling.* 3rd edn. New York, New York: Guilford Press.

Kline, R. B. (1998) *Principles and Practice of Structural Equation Modelling.* Guilford Press,New York.

Knox, K. (2004) *A Research's Dilemma-Philosophical and Methodological Pluralism*.Nottingham Business School, Trent University. Nottingham, UK.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015) 'Advanced Social Engineering Attacks', *Journal of Information Security and Applications*, 22, pp. 113-122. DOI: https://doi.org/10.1016/j.jisa.2014.09.005

Kumar, N., Mohan, K., and Holowczak, R. (2008) 'Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls', *Decision Support Systems*, 46(1), pp. 254–264. DOI: http://doi.org/10.1016/j.dss.2008.06.010

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, F., and Hong, J. (2007) 'Getting users' to pay attention to anti-phishing education: evaluation of retention and transfer',*Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, Pittsburgh, Pennsylvania.

Kwan, M. and Bryan, D. (2010) 'Affective response to exercise as a component of exercise motivation: Attitudes, norms, self-efficacy, and temporal stability of intentions', *Psychology ofSport and Exercise*, 11, pp. 71-79.

Lalani, B., Dorward, P., Holloway, G. and Wauters, E. (2016) 'Small holder farmers' motivations for using Conservation Agriculture and the roles of yield, labour and soil fertility in decision making' *Agric. Syst*. 146, pp. 80–90.

Lapple, D. and Kelley, H. (2013) 'Understanding the uptake of organic farming: Accounting for heterogeneities among Irish farmers', *Ecol. Econ*. 88, pp. 11– 19.

Larsson, R., and Risberg, A. (1998) 'Cultural Awareness and National versus Corporate Barriersto Acculturation', In *Gertsen, Söderberg & Torp Cultural Dimensions of International Mergers and Acquisitions*, 85, 39.

Lastdrager, E. (2014) 'Achieving a consensual definition of phishing based on a systematicreview of the literature', *Crime Science*, 3(1):9.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, H. (2014) 'Information security awareness and behavior: a theory-based literature review', *Management Research Review*, 37(12), pp. 1049–1092. DOI: http://doi.org/10.1108/MRR-04-2013-0085

Lee, Y. and Kozar, K. (2008) 'An empirical investigation of anti-spyware software adoption: A multitheoretical perspective', *Information & Management,* 45(2), pp. 109–119. DOI: http://doi.org/10.1016/j.im.2008.01.002

Lee, K. and Rao, R. (2007) 'Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government citizens online interactions in a turbulent environment', *Decision Support Systems*, 43(4), pp. 1431-1449.

Leedy, D. and Ormrod, E. (2015) *Practical Research: Planning and Design*. 11th edn. Pearson education.

Leonard, K., Cronan, P. and Kreie, J. (2004) 'What influences IT ethical behavior intentions planned behavior, reasoned action, perceived importance, or individual characteristics*?', InfManag*, 42(1).

Levine, R. (2003) *The Power of Persuasion. Hoboken*. NJ: John Wiley & Sons Inc.

Liang, H. and Xue, Y. (2010) 'Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective', *Journal of the Association for Information Systems*, 11(7), pp.394–413.

Lin, H. (2010) 'Applicability of the extended theory of planned behavior in predicting job seeker intentions to use job-search websites', *International Journal of Selection and Assessment*, 18, pp.64-74.

Lin, S., Chun, C. and Chua, F. (2011) 'Application of Theory of Planned Behavior on the Studyof Workplace Dishonesty', *IPEDR IAC S IT Press*, Manila. Philippines.

Lin, T., Capecci, E., Ellis, M., Rocha, A., Dommaraju, S., Oliveira, S. and Ebner, C. (2019) 'Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and EmailContent', *ACM Trans. Comput. Interact,* pp.26, 32.

Liping, J. and Watters, P. (2009). 'Establishing phishing provenance using orthographicfeatures', *NJ*, pp. 1-10.

Litan, A. (2004) *Phishing Attack Victims Likely Targets for Identity Theft*. Gartner

Lowry, B. and Gaskin, J. (2014). 'Partial least squares (PLS) structural equation modelling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it',*IEEE Transactions on Professional Communication*, 57(2), pp. 123–146. http://doi.org/10.1109/TPC.2014.2312452

Luenendonk, M. (2019) *Theory of Planned Behavior: Definition, Explained, Examples*. https://www.cleverism.com/theory-of-planned-behavior/

Lutz, S. (2011) 'The Theory of Planned Behaviour and the Impact of Past Behaviour', *The International Business & Economics Research Journal*, 10(1), pp. 91-110.

MacDonald, S. and Headlam, N. (2011) *Research Methods Handbook: Introductory Guide to Research Methods for Social Research*. CLES, Express Network. Manchester, UK.

Madden, J., Ellen, S. and Ajzen, I. (1992) 'A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action', *Personality and Social Psychology Bulletin*, 18(1), pp. 3-9.

Marett, K., Biros, D., and Knode, M. (2004) 'Self- efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training', *Lecture Notes in Computer Science*, 3073, pp. 187-200.

Martin, B. (2004) 'Telling lies for a better world?' *Social Anarchism*, 35, pp. 27-39.

McClelland, S. (1994) 'Training needs assessment data-gathering methods: Part 1, Survey questionnaires', *Journal of European Industrial Training, 18*, pp. 22–26.

McKerchar, M. (2003) 'The Impact of Complexity Upon Tax Compliance: A Study of Australian Personal Taxpayers', *Australian Tax Research Foundation*, 39, Sydney.

McLellan, H. (1996) *Situated learning perspectives, Educational Technology Publications*.

Meiriana, M., Suwena, K. and Indrayani, L. (2018) 'The Influence of Fraud Triangle and Theory of Planned Behavior on Students Academic Fraud in Bali', *3rd International Conference on Tourism, Economics, Accounting, Management, and Social Science (TEAMS 2018)*, PP 136-141.

MeanThat & Authentic Data Science. (2016) *1.3 Exploratory, Descriptive and ExplanatoryNature Of Research* [Video]. YouTube. https://www.youtube.com/watch?v=FlBFdEgrTBM

Mertler, A. and Reinhart, V. (2017) *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation.* 6th edn. New York, NY: Routledge.

Merwe, A., Loock, M. and Dabrowski, M. (2005) 'Characteristics and responsibilities involvedin a Phishing attack', *Proceedings ACM WISCT 05*, pp. 249-254.

Micha, E., Areal, J., Tranter, B. and Bailey, P. (2015) 'Uptake of agri-environmental schemes in the Less-Favoured Areas of Greece: The role of corruption and farmers' responses to the financial crisis', *L. Use Policy*. 48, pp. 144–157.

Michie, S., and West, R. (2013) 'Behaviour change theory and evidence: A Presentation to Government' *Health Psychology Review*, 7(1), pp. 1–22. http://doi.org/10.1080/17437199.2011.649445

Microsoft. (2020) *The psychology of social engineering – the 'soft' side of cybercrime*. https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/

Mika, Kontio. (2016) *Social engineering 101*. Bachelor's thesis. Turku University of Applied Sciences.

Miksza, P. and Elpus, K. (2018) *Design and Analysis for Quantitative Research in MusicEducation.* New York. Oxford University Press.

Miles, B. and Huberman, M. (1994) *Qualitative Data Analysis*. 2nd edn. Newbury Park, CA,Sage.

Milgram, S. (1974) *Obedience to Authority*. Harper.

Mimiso, M. (2018) *Threat-actor opportunism at peak during holiday season*. https://www.flashpoint-intel.com/blog/threat-actor-opportunism-at-peak-during holiday-season/

Mitchell, L. and Jolley, M. (2013) *Research Design Explained.* 8th edn. Belmont, CA:Wadsworth.

Mitnick, K. and Simon, W. (2003) *The Art of Deception: Controlling the Human Element in Security*. Wiley: Hoboken, NJ, USA, 2003; ISBN 978-0-471-23712-9.

Modic, D. and Lea, S. (2013) 'Scam Compliance and the Psychology of Persuasion', *SSRN Electronic Journal*, pp. 1-34, DOI: 10.2139/ssrn.2364464.

Mohamed, G., Mohideen, M. and Banu, S. (2014) 'Email Phishing – An open threat to everyone', *International Journal of Scientific and Research Publication*, Vol 4, Issue 2.

Mohammad, R., Thabtah, F. and McCluskey, L. (2015) 'Tutorial and critical analysis of phishing websites methods', *Computer Science Review* .17, pp. 1-24.

Mohammed, S. (2011) 'Internet usage and user preferences in Saudi Arabia', *Journal of KongSaud University – Engineering Sciences*, Vol 23, pp. 101-107.

Mohebzada, J., Zarka, A., Bhojani, H. and Darwish, A. (2012) 'Phishing in a university community: two large scale phishing experiments', In *International Conference on Innovations in Information Technology (IIT)*, pp. 249–254. https://doi.org/10.1109/ INNOVATIONS.2012.6207742

Morais, M., Borges, R. and Binotto, E. (2018) 'Using the reasoned action approach to understand Brazilian successors' intention to take over the farm', *Land use policy* 71, pp. 445–452.

Mouton, F., Malan, M., Leenen, L. and Venter, H. (2014) 'Social engineering attack framework', *Information Security for South Africa, IEEE*, pp. 1-9.

Mouton, F., Leenen, L. and Venter, H. (2016) 'Social engineering attack examples, templatesand scenarios', *Computer and Security*. 59, pp. 186–209.

Mullan, B., Allom, V., Sainsbury, K. and Monds, A. (2015) 'Examining the predictive utility ofan extended theory of planned behaviour model in the context of specific individual safe food-handling', *Appetite*, 90, pp. 91–98. http://doi.org/10.1016/j.appet.2015.02.033

Murnaghan, A., Blanchard, M., Rodgers, M., LaRosa, N., MacQuarrie, R.,MacLellan, L. and Gray, J. (2010) 'Predictors of physical activity, healthy eating and being smoke-free in teens: Atheory of planned behaviour approach', *Psychology and Health*, 25, pp. 925-941.

Muscanell, L., Guadagno, E. and Murphy, S. (2014) 'Weapons of influence misused: s social influence analysis of why people fall prey to internet scams', *Soc. Pers. Psychol. Compass* 8 (7),pp. 388–396. https://doi.org/10.1111/spc3.12115

Mwagwabi, F., McGill, T. and Dixon, M. (2014) 'Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines', In *Proceedings of the Annual Hawaii International Conference on System Sciences,* pp. 3188–3197. http://doi.org/10.1109/HICSS.2014.396

Myers, D. and Avison, D. (2002) *Qualitative Research in Information Systems: A Reader*. Sage.

Myers, D. (1997) 'Qualitative Research in Information Systems', *MIS Quarterly*, Vol. 21, No.2,pp. 241-242.

Nabbout, M. (2019) *Saudi hacker gives 19 students full grades, faces jail and millions in fine*. https://stepfeed.com/saudi-hacker-gives-19-students-full-grades-faces-jail-and-millions-in-fine-7234

Nabie, Y. and Paul, J. (2016). 'Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research*,Vol.6, pp. 23-31.

Naidu, S. (2004) 'Learning design as an indicator of quality in teacher education', In. *Rama, K. and Menon, M. Innovations in teacher education - International practices for quality assurance,* pp. 65-76, Bangalore, NAAC.

Nalin, A., Gamagedara, A., Steve, L. and Konstantin, B. (2016) 'Phishing threat avoidance behaviour: An empirical investigation', *Computers in Human Behavior*, Vol.60, pp. 185-197.

Nasir, A., Arshah, R. and Hamid, M. (2018) 'The Significance of Main Constructs of Theory of Planned Behavior in Recent Information Security Policy Compliance Behavior Study: A Comparison among Top Three Behavioral Theories', *International Journal of Engineering & Technology*, pp. 737-741.

Nathans, L., Oswald, F. and Nimon, K. (2012) 'Interpreting multiple linear regression: A guidebook of variable importance', *Practical Assessment Research & Evaluation*, *17*(9), 19. http://doi.org/10.3102/00346543074004525

Neill, J. (2008) *Writing up a factor analysis*.

Netemeyer, R., Bearden, W. and Sharma, S. (2003) *Scaling Procedures: Issues and Applications*. SAGE.

Neuman, W. L. (1997) *Social Research Methods: Qualitative and Quantitative Approaches*. 3rd edn. Boston: Allyn and Bacon.

Neuman, W. L. (2014) *Social Research Methods: Qualitative and Quantitative Approaches*. 7thedn. Boston: Allyn and Bacon.

Neville, C. (2007) *Effective Learning Service: Introduction to Research and Research Methods*. University of Bradford School of Management. UK.

Ng, Y. and Rahim, M. (2005) 'A socio-behavioral study of home computer users' intention to practice security'. In *PACIS 2005 Proceedings*, pp. 234–247.

Nick, K. (2019) *How Phishing Attacks Are Getting Creative (and What Data Pros Can Do About It)*.https://www.dataversity.net/how-phishing-attacks-are-getting-creative-and-what-data-pros-can-do-about-it/

Nimon, F. and Oswald, L. (2013) 'Understanding the results of multiple linear regression: Beyond standardized regression coefficients', *Organizational Research Methods*, *16*(4), 650– 674. http://doi.org/10.1177/1094428113493929

Norman, P. and Conner, M. (2006) 'The theory of planned behavior and binge drinking: Assessing the moderating role of past behavior within the theory of planned behavior', *Journalof Health Psychology*, 11, pp. 55-70.

Nudgify. (2021) *What is Social Proof? The Ultimate Guide*. https://www.nudgify.com/social-proof/.

Nunally, C. and Ira, B. (1978) *Psychometric Theory*. 2nd edn. New York: McGraw-Hill.

Okere, I. and Niekerk, J. (2012) 'Assessing Information Security Culture: A Critical Analysis of Current Approaches', *Information Security for South Africa 2012, IEEE* , pp. 1-8.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoklu, M., Weir, D., Soliman,A., Lin, T. and Ebner, N. (2017) 'Dissecting spear phishing emails for older vs young adults: Onthe inter play of weapons of influence and life domains in predicting susceptibility to phishing', In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Vol 2017, pp. 6412-6424.

Ollman, G. (2004) *The phishing guide: understanding and preventing phishing attacks*.

Oluwatayo, A. (2012) 'Validity and reliability issues in educational research', *Journal of Educational and Social Research,* 2(2), pp. 39-400.

Onumo, A., Cullen, A. and Ullah-Awan, I. (2017) 'An Empirical Study of Cultural Dimensionand Cybersecurity Development', *IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 70-76.

Orgill, G., Romney, G., Bailey, M. and Orgill, P. (2004) 'The Urgency for Effective UserPrivacy-education to Counter Social Engineering Attacks on Secure', *Computer Systems, Proceedings of SIGITE'04*, Salt Lake City, UT.

Orlikowski, J. and Baroudi, J. (1991) 'Studying Information Technology in Organizations: Research Approaches and Assumptions', *Information Systems Research* ,Vol. 2, No.1, pp. 1-28

Orman, H. (2013) 'The complete story of phish', *IEEE Internet Computing,* 17(1), pp. 87-91. Oxford business group. (2020) *Saudi Arabia works to enhance cybersecurity.* https://oxfordbusinessgroup.com/analysis/secure-access-authorities-work-enhance-cybersecurity-and resilience-face-evolving-online-threats, 2020

Pahnila, S., Siponen, M. and Mahmood, A. (2007) 'Employees' behavior towards is securitypolicy compliance', In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. DOI: http://doi.org/10.1109/HICSS.2007.206

Pallant, J. (2001) *SPSS Survival Manual: A Step By Step Guide to Data Analysis*. Buckingham: Open University Press.

Pallant, J. (2013) *SPSS Survival Manual: A Step By Step Guide to Data Analysis*. 5th edn. Open University Press, New York.

Parker, D., Manstead, S. and Stradling, G. (1995) 'Extending the Theory of Planned Behaviour: The Role of Personal Norm', *British Journal of Social Psychology*, 34(2), pp. 127-138.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D. and Jerram, C. (2015) 'Do Users' Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?', *Australasian Conference on Information Systems*.

Parsons, K., Butavicius, M., Pattinson, M. and McCormac, A. (2014) 'Using actions and intentions to evaluate categorical responses to phishing and genuine emails', In *Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2014).* Plymouth, UK.

Pather, S. and Remenyi, D. (2004) 'Some of the philosophical issues underpinning research in information systems: from positivism to critical realism', In *Proceedings Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries 2004*, pp. 141-146. Stellenbosch, South Africa.

Patil, P and Devale, P. (2016) 'A literature survey of phishing attack technique', *Int. J. Adv. Res. Comput. Commun. Eng*, pp. 198-200.

Pavlou, P and Chai, L. (2002) 'What Drives Electronic Commerce Across Cultures? A Cross-Cultural Empirical Investigation of The Theory of Planned Behavior', *Journal of Electronic Commerce Research*, Vol (3), No (4).

Pett, M., and Lackey, N. and Sullivan, J. (2003) *Making Sense of Factor Analysis: The Use ofFactor Analysis for Instrument Development in Health Care Research*. California, Sage Publications Inc.

Petty, R. E., and Cacioppo, J. T. (1986) 'The elaboration likelihood model of persuasion', *Advances in experimental social psychology*, 19(1), pp. 123-205.

Pizam, A. (1993) *Managing Cross-Cultural Hospitality Enterprises. The International Hospitality Industry: Organisational and Operational Issues*. John Wiley, New York, NY.

Pokrovskaia, N. (2017) 'Social engineering and digital technologies for the security of the social capital' development', In *Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg*, pp. 16-19.

Polit, D., Beck, C. and Hungler, B. (2001) *Essentials of Nursing Research: Methods, Appraisal, and Utilization*. 5th edn. Philadelphia: Lippincott.

Prapavessis, H., Gaston, A. and DeJesus, S. (2015) 'The Theory of Planned Behavior as a model for understanding sedentary behavior', *Psychology of Sport and Exercise*, 19, pp. 23–32. http://doi.org/10.1016/j.psychsport.2015.02.001

Prashant, K. (2016) 'Prashant's algorithm for password management system', *InternationalJournal of Engineering Science*, pp. 2424-2426.

PWC. (2016) *Turnaround and transformation in cybersecurity: key findings from The GlobalState of Information Security Survey 2016*.

Puneeth, M., Farha, S., Yamini, M. and Sandhya, N. (2015) 'Social Engineering on Social Networking Sites', *International Journal of Advanced Engineering Research and Science*, 2, pp.57-60.

Pure Cloud. (2021) *The Difference Between Mass Phishing and Spear Phishing*. https://www.purecloudsolutions.co.uk/the-difference-between-mass-phishing-spear-phishing/

Qi, M., Nevill, D. and Mousoli, R., (2009) 'Spam and Social Effects', *Symposia and Workshopson Ubiquitous, Autonomic and Trusted Computing, UIC-ATC*, pp. 498-501. http://doi.10.1109/UIC-ATC.2009.89.

Ramona, S. E. (2011) 'Advantages and Disadvantages of Quantitative and QualitativeInformation Risk Approaches', *Chinese Business Review*, pp. 1106-1110.

Randall, D. M., and Gibson, A. M. (1991) 'Ethical decision making in the medical profession:An application of the theory of planned behavior', *Journal of Business Ethics,* 10(2), pp. 111– 122. http://doi.org/10.1007/BF00383614

Rekouche, K. (2011) 'Early phishing', *arXiv preprint arXiv,* pp.1106.4692.

Retruster. (2019) *Phishing Statistics and Fraud Statistics*. https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

Rezaei, R., Mianaji, S. and Ganjloo, A., (2018) 'Factors affecting farmers' intention to engage in on-farm food safety practices in Iran: Extending the theory of planned behavior', *J. Rural Stud.* 60, pp. 152–166.

Rise, J., Kovac, V., Kraft, P. and Moan, I. (2008) 'Predicting the intention to quit smoking and quitting behaviour: Extending the theory of planned behaviour', *British Journal of Health Psychology*, Volume 13, Issue 2, pp 291-310.

Robila, A., James, J. and Ragucci, W. (2006) 'Don't be a phish: steps in user education', Proceedings *11th annual SIGCSE conference on Innovation and technology in computer scienceeducation. ITICSE '06*, pp. 237-241. New York, NY, USA.

Robson, C. (1993) *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*. 2nd edn. Blackwell Publishing: Oxford, UK.

Roscoe, J. T. (1975) *Fundamental Research Statistics for The Behavioural Sciences* .2nd edn.New York, NY: Holt, Rinehart and Winston.

Ryan, M.J. (1982) 'Behavioral intention formation: the interdependency of attitudinal and social influence variables', *Journal of Consumer Research*, Vol. 9 No. 3, pp. 263-278.

Ryu, S. Ho, S. and Han, I. (2003) 'Knowledge sharing behavior of physicians in hospitals', *Expert Systems with Applications*, Vol 25, Issue 1, pp. 113-122.

Sadeghi, T. and Farokhian, S. (2011) 'The Role of Behavioral Adoption Theories in OnlineBanking Services', *Middle-East Journal of Scientific Research*, Vol 7, No 3, pp. 374-380.

Safa, N. S., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organizations', *Computers & Security*, 56, pp. 1-13. DOI: http://doi.org/10.1016/j.cose.2015.10.006

Said, A. R., Abdullah, H., Uli, J., and Mohamed, Z. A. (2014) 'Relationship between organizational characteristics and information security knowledge management implementation',*Procedia-Social and Behavioral Sciences*, *123*, pp. 433–443. DOI: http://doi.org/10.1016/j.sbspro.2014.01.1442

Sapsford, R. (2006) *Survey Research*. 2nd edn. London: Sage Publications.

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R. and Hair, J. F. (2014) 'Partial least squares structural equation modelling (PLS-SEM): A useful tool for family business researchers', *Journal of Family Business Strategy*, *5*(1), pp. 105–115. DOI: http://doi.org/10.1016/j.jfbs.2014.01.002

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research Methods For Business Students*. London: Pearson.

Saunders, M., Lewis, P. and Thornhill, A. (1997) *Research Methods For Business Students*.Pitman, London, United Kingdom.

Schein, E. (1992) *Organisational Culture and Leadership*. 2nd edn. San Francisco, CA.

Schifter, D. and Ajzen, I. (1985) 'Intention, Perceived Control, and Weight Loss: An Application of the Theory of Planned Behavior', *Journal of Personality and Social Psychology*, Vol 49, Issue 3, pp. 843-851.

Sebescen, N. and Vitak, J. (2017) 'Securing the human: Employee security vulnerability risk in organizational settings', *Journal of the Association for Information Science and Technology*, 68(9), pp. 2237-2247.

Security through education. (2020) *Social Engineering Defined*. https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Segovia, L., Torres, F., Rosillo, M., Tapia, E., Albarado, F. and Saltos, D. (2017) 'Social engineering as an attack vector for ransomware', In *Proceedings of the Conference on Electrical Engineering and Information Communication Technology*, Pucon, Chile, pp. 1-6.

Sekaran, U. (2003). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.

Sekaran, U. and Bougie, R. (2016) *Research Methods For Business: A Skill Building Approach*.7th edn. United Kingdom: John Wiley & Sons Ltd.

Senger, I., Borges, J. R., Machado, J. D., (2017) 'Using the theory of planned behavior to understand the intention of small farmers in diversifying their agricultural production', *J. RuralStud.* 49, pp. 32-40.

Shahbaznezhad, H., Kolini, F. and Rashidirad, M. (2020) 'Employees' Behaviour in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?', *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2020.1812134.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. and Downs, J. (2010) 'Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions', *Proceedings of the*

28th International Conference on Human Factors in Computing Systems - CHI, pp. 373–382. DOI: https://doi.org/10.1145/1753326.1753383

Sheppard, B.H., Hartwick, J. and Warshaw, P.R. (1988) 'The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research', *Journal of Consumer Research,* Vol. 15 No. 3, pp. 325-343.

Silic, M. and Back, A. (2016) 'The dark side of social networking sites: Understanding phishing risks', *Computers in Human Behavior,* 60, pp. 35-43. DOI: http://10.1016/j.chb.2016.02.050

Silverman, D (2013) *Doing Qualitative Research: A practical handbook*. SAGE Publications Limited.

Simon, D. and Yaras, D. (2000) *Lagom svenskt*. Stockholm: Bilda forlag.

Simons, H.W., (1976) *Persuasion: Understanding, Practice, and Analysis*. Reading, Mass: Addison-Wesley Pub Co.

Singer, P. and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs toKnow*. Oxford University Press.

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*, 51(2), pp. 217-224.DOI: http://doi.org/10.1016/j.im.2013.08.006

Smart, M. (2012) *The Application of The Theory of Planned Behaviour and Structural Equation Modelling in Tax Compliance Behaviour: A New Zealand Study*.

Smith, A. (2015) *Attitude, Subjective Norm, and Perceived Behavioral Control as Indicators for Nurse Educators' Intention to Use Critical Thinking Teaching Strategies: a Structure Equation Model Analysis.* PhD Dissertations. 1576. https://digitalcommons.andrews.edu/dissertations/1576

Snyder, C. (2015) *Handling human hacking: Creating a comprehensive defensive strategyagainst modern social engineering*. Liberty University.

Sommestad T, Hallberg J, Lundholm K, Bengtsson J. (2013) 'Variables influencing information security policy compliance: a systematic review of quantitative studies', *Information Management Computer Security*. Emerald Group Publishing Limited; 2013 Nov 19;22(1):3.

Sommestad, T. and Hallberg, J. (2013) 'A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance', *Security and Privacy Protection in Information Processing Systems*, vol. 405, pp. 257–271.

Sommestad, T. and Karlzén, H. (2019) 'A meta-analysis of field experiments on phishing susceptibility', In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, pp.1-14.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015) 'The sufficiency of the theory of planned behavior for explaining information security policy compliance', *Information and Computer Security*, 23(2), pp. 200–217. DOI: http://doi.org/10.1108/ics-04-2014-0025

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management*,36(2), pp. 215–225. DOI: http://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stahl, B.C. (2005) 'A critical view of the ethical nature of interpretive research: Paul Ricoeur and the other', *Proceedings 13th European Conference on Information Systems*, Regensburg, Germany.

Stajano, F. and Wilson, P. (2011) 'Understanding Scam Victims: Seven Principles for Systems Security', *Commun. ACM*, Vol. 54, No. 3, pp. 70-75.

Statista. (2021) *Number of Internet users' in Saudi Arabia from 2015 to 2023 (in millions)*, https://www .statista .com /statistics /462959 /internet -users' -saudi-arabia/.

Steenkamp, J. E. M. and van Trijp, H. C. M. (1991) 'The use of LISREL in validating marketing constructs', *International Journal of Research in Marketing*, 8, pp. 283–299.

Stern A. (2014) *Social Networkers Beware: Facebook is a Major Phishing Portal, KasperskyLab, 23 June 2014,* https://blog.kaspersky.com/1-in5-phishing-attacks-targets-facebook/5180/

Stone, Thomas H., Jawahar, I. and M.Kisamore, Jennifer L. (2010) 'Predicting Academic Misconduct Intention and Behavior Using the Theory of Planned Behavior', Psychology Press,pp. 35-45, DOI: http://10.1080/01973530903539895.

Straub, D. W., Loch, K. D., and Hill, C. E. (2001) 'Transfer of information technology to the Arab world: a test of cultural influence modelling', *Journal of Global Information Management*,9(4), pp. 1-60.

Sürücü, L. and Maslakçı, A. (2020) 'Validity And Reliability In Quantitative Research', *BMIJ*,8(3).

Swisher, L. and Beckstead, W. (2004) 'Factor Analysis as a Tool for Survey Analysis Using a Professional Role Orientation Inventory as an Example', *Physical Therapy*. 84(9), pp. 784-799.

Symantec .(2006). *Internet Security Threat Report – Trends for January 2006*, vol.10.

Tabachnick, B. G. and L. S. Fidell (2001) *Using Multivariate Statistics. Needham Heights*. MA, Allyn & Bacon.

Tabachnick, B.G. and L.S. Fidell, (2007) *Using Multivariate Statistics*. 5th edn. New York: Allyn and Bacon. Pearson Education.

Taib, R., Yu, K., Berkovsky, S., Wiggins, M. and Smith, P. (2019) 'Social Engineering and Organisational Dependencies in Phishing Attacks', IFIP *Conference on Human-Computer Interaction* (pp. 564-584).

Tally. G., Sames, D., Chen, T., Colleran, C., Jevans, D., Omiliak, K. and Rasmussen, R. (2006) 'The Phisherman Project: Creating a Comprehensive Data Collection to Combat Phishing Attacks', *Journal of Digital Forensic Practice*, July 2006, Vol. 1, Iss. 2, pp. 115 – 129.

Tally, G. (2009) *Phisherman: a phishing data repository*. Piscataway, NJ, Washington, DC.

Tashakkori, A. and Teddlie, C. (1998) 'Mixed Methodology: Combining Qualitative and Quantitative Approaches*', Applied Social Research Methods Series*, Vol. 46, Thousand Oaks,CA: Sage.

Tavakol, M. and Sandars, J. (2014a) 'Quantitative and Qualitative Methods in Medical Education Research', *AMEE Guide*, No 90: Part I. Medical Teacher, 36(90), pp. 746-756. DOI: http://doi.org/10.3109/0142159X.2014.915298

Tavakol, M., and Sandars, J. (2014b) 'Quantitative and Qualitative Methods in Medical Education research'*; AMEE Guide*, No 90: Part II. Medical Teacher, 36(90), pp. 838-848. DOI: http://doi.org/10.3109/0142159X.2014.915297.

Team, C. I. T. (2014) *Unintentional insider threats: Social engineering*. Software Engineering Institute.

Teijlingen, R. and Hundley, V. (2001) *The importance of pilot studies*. Social Research.Guildford: University of surrey.

Telstra Corporation. (2104) *Telstra Cyber Security Report 2014*. http://www.telstra.com.au/business- enterprise/download/document/telstra-cyber-security-report-2014.pdf

Telstra Corporation. (2017) *Telstra cyber security report 2017*.

Teodor, S., Henrik, K. and Jonas, H (2017) 'The Theory of Planned Behavior and Information Security Policy Compliance', *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2017.1368421

Themistocleous, M. (2002) *Enterprise Application Integration*. Brunel University.

Thompson, B. (2004) *Exploratory and confirmatory factor analysis: understanding concepts and applications*. Washington, DC, American Psychological Association.

Thompson, K. (2015) *Positivism and Interpretivism in Social Research*. https://revisesociology.com/2015/05/18/positivism-interpretivism-sociology/

Tipton, J. A. (2014) 'Using the theory of planned behavior to understand caregivers' intention to serve sugar-sweetened beverages to non-hispanic black pre-schoolers', *Journal of Paediatric Nursing*, *29*(6), pp. 564-575. DOI: http://doi.org/10.1016/j.pedn.2014.07.006

Titchen, A. and Hobson, D. (2005) 'Research Methods in the Social Science', pp 121-130. New Delhi: Sage.

Tiwari, P. (2020) *Exploring Phishing Susceptibility Attributable To Authority, Urgency, Risk Perception And Human Factors*. Purdue University.

Tolliver, M. (2016) *Using the theory of Planned Behavior to Predict Executives' Intentions toHire Psychologists in Federally Quailed Health Centres*.

Tout, H. and Hafner, W. (2009) 'Phishpin: an identity-based anti-phishing approach', *International Conference on Computational Science and Engineering*, Vol.3, pp. 347-52. DOI: http://10.1109/cse16093.2009

Triandis, H. C. (1994) 'Theoretical and methodological approaches to the study of collectivismand individualism', *In U. Kim, H. C. Triandis, C. Kagitcibasi, S. C. Choi, & G. Yoon (Eds.), Individualism and collectivism: Theory, method, and applications*, pp. 41-51. Thousand Oaks, CA: Sage.

Trompenaars, F. and Hampden-Turner, C. (1998) *Riding The Waves of Culture: Understanding Cultural Diversity in Global Business*. New York, NY: McGraw-Hill.

Tsai, C. (2010) 'Applying the theory of planned behaviour to explore the independent travellers' behaviour', *African Journal of Business Management*, Vol (4), Issue (2), pp. 221-234.

Turner, J. C. (1991) *Social Influences. Milton Keynes*. Open University Press.

Turner, T. L., Balmer, D. F. and Coverdale, J. H. (2013). 'Methodologies and study designs relevant to medical education research', *International Review of Psychiatry*, 25(3), 301-310. DOI: http://doi.org/10.3109/09540261.2013.790310.

Uchill. (2019) *Typo led to podesta email hack: report* https://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack

Ullman JB. (1996) 'Structural equation modelling', In: *Tabachnick BG, Fidell LS (ed). Using Multivariate Statistics.* 5th edn. Boston, MA: Pearson Education Inc, pp. 676-780.

Upadhyay, I. (2020) *Top 10 Challenges of Cyber Security Faced in 2020* https://www.iigsawacademv.com/blogs/cvber-securitv/challenges-of-cvber-securitv/

Van Deursen, A. J. and Van Dijk, J. A. (2013) 'The digital divide shifts to differences in usage', *New Media & Society*, *16*(3), pp. 507-526. DOI: http://doi.org/10.1177/1461444813487959

Varshney, G. Misra, M and Atrey K. (2016). 'A survey and classification of web phishing detection schemes', *Security and Communication Networks*, Vol (9), Issue (8), pp. 6266-6284.

Vaus, D. (2002) *Surveys in social research*. 5th edn. London, UK: Routledge.

Verizon Enterprise. (2013) *Data breach investigations report 2013*. http://www.frank-cs.org/cms/pdfs/Verizon/VERIZON_Cyber_EXECSUM_23.4.13.pdf.

Vreede, G.J.D. (1995) *Facilitating Organisational Change: The Participative Application of Dynamic Modelling.* Delft University of Technology.

Walsham G. (1995) 'The emergence of interpretivism in IS research', *Information Systems Research*, Vol. 6, No. 4, pp. 376-394.

Walsham, G. (1993). *Interpreting Information Systems in Organizations*. Chichester, Wiley.

Wang, J., Chen, R., Herath, T. and Rao, H. R. (2009) 'An Exploration of the Design Features of Phishing Attacks', *Information Assurance, Security and Privacy Services*, 4, 29.

Wardman, B., Shukla, G. and Warner, G. (2009) 'Identifying vulnerable Websites by analysis of common strings in phishing URLs', *Piscataway, NJ,* USA, 13 pp. 1-13.

Webber, R. (2004) 'The rhetoric of positivism versus interpretivism', *MIS Quarterly*, vol. 28,no.1.

Weinstein, N.D. (1980) ‘Unrealistic optimism about future life events’, *Journal of personalityand social psychology*, 39(5), 806. DOI: doi:10.1037/0022-3514.39.5.806.

Weirich, D. and M.A. Sasse. (2001) ‘Pretty good persuasion: a first step towards effective password security in the real world’, in *Proceedings of the 2001 workshop on New securityparadigms. 2001*. Cloudcroft, New Mexico: ACM.

Whiston, S. C. (2012) *Principles and Applications of Assessment in Counselling*. Cengage Learning. USA.

Whiteman, J. (2017) Social Engineering: Humans are the prominent reason for the continuanceof these types of attacks.

Whitten, A. and Tygar, D. (1999) ‘Why Johnny can't encrypt: A usability evaluation of PGP 5.0’, In *Proceedings 8th USENIX Security Symposium*, Washington, D.C., August 1999, vol. 8,pp. 169-183.

Whitty, M.T.(2013) ‘The Scammers Persuasive Techniques Model Development of a Stage Model to Explain the Online Dating Romance Scam’, *British Journal of Criminology*, 53(4), pp.665-684.

Williams, B., T. Brown, et al. (2010) ‘Exploratory factor analysis: A five-step guide for novices’, *Australasian Journal of Paramedicine* 8(3).

Wilson, A. (2012) *Marketing Research: An Integrated Approach*. Harlow: Pearson Education Limited.

Winder, D. (2009) ‘Stupid security attacks’, *PC Pro UK*, No.180.

Wong, C and Mullen, B .(2009). ‘Predicting breakfast consumption: An application of the theory of planned behaviour and the investigation of past behaviour and executive function’, *British journal of Health Psychology*, pp. 489-504.

Wright, K. B. (2005). ‘Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey Services’, *Journal of Computer-Mediated Communication, 10* (3).

Wu, M., Miller, R. C. and Garfinkel, S. L. (2006) 'Do security toolbars actually prevent phishing attacks?', Proceedings *SIGCHI Conference on Human Factors in Computing Systems*, Montréal,Québec, Canada, pp. 22-27 April.

Wynn, D. and Williams, C. K. (2012) 'Principles for Conducting Critical Realist Case Study Research in Information Systems', *Management Information Systems Quarterly*, 36(3): pp. 787-810.

Wyse, E. (2011) *What is the Difference between Qualitative research and Quantitative Research?* https://dokumen.tips/documents/what-is-the-difference-between-qualitative-research- and-quantitative-research.html

Xiangyu, L., Qiuyang, L. and Chandel, S. (2017) 'Social engineering and Insider threats', In *Proceedings of the International Conference on Cyber-Enabled Distributed Computing andKnowledge Discovery*, 12–14 October; pp. 25–34. Nanjing, China.

Xin, L. and Qinyu, L. (2007) 'Awareness education as the key to ransomware prevention', *Information Systems Security USA*, Vol.16, No.4, pp. 195-202.

Yami, A. (2015) *Using The Theory of Planned Behaviour to Explore The Intentions of a Multicultural Nursing Workforce to Comply With Policies and Procedures in The Prince SultanMilitary Medical City (PSMMC).* PhD thesis.

Yao, M. Z. and Linz, D. G. (2008) 'Predicting self-protections of online privacy', *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality onBehavior and Society*, 11(5). DOI: http://doi.org/10.1089/cpb.2007.0208

Yazdanmehr, A., and Wang, J. (2015) 'Employees' information security policy compliance: Anorm activation perspective', *Decision Support Systems*, 92, pp. 36–46. http://doi.org/10.1016/j.dss.2016.09.009

Ye, Z.T., Smith, S. and Anthony, D. (2005) 'Trusted paths for browsers', *ACM Transactions on Information and System Security (TISSEC)*, Vol. 8, No. 2, pp. 153-186.

Yilmaz, K. (2013) 'Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences', *European Journal of Education,*48(2), pp. 311–325. http://doi.org/doi:10.1111/ejed.12014.

Yin, R.K. (1994) *Case Study Research: Design and Methods*. 2nd edn. Newbury Park, Sage.

Yoon, C. and Kim, H. (2013) 'Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms', *Information Technology & People*, 26(4), pp.401-419. http://doi.org/10.1108/ITP-12-2012-0147

Yousafzai, S., Foxall, G. and Pallister, J. (2010) 'Explaining Internet Banking Behavior: Theoryof Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model?', *Journalof Applied Social Psychology*, vol. 40, no. 5, pp. 1172-1202.

Zaki, T., Uddin, M., Hasan, M. and Islam, N. (2017) 'Security threats for big data: A study onEnron email dataset', *Proceedings of the 5th International Conference on Research and Innovation in Information Systems (ICRIIS)*. Langkawi, Malaysia, pp. 1-6.

Zanna, P. and Rempel, K. (1988) 'Attitudes: A New Look at an Old Concept', In *D. B.Tal & A.W. Kruglanski (Eds.), The Social Psychology of Knowledge* , pp. 315-334. Cambridge:University Press.

Zemore, S. E., and Ajzen, I. (2014) 'Predicting substance abuse treatment completion using anew scale based on the theory of planned behavior', *Journal of Substance Abuse Treatment, 46(2),* pp.174–182. http://doi.org/10.1016/j.jsat.2013.06.011

Zeng, Z. and Cleon, B. (2018) 'Factors affecting the adoption of a land information system: An empirical analysis in Liberia', *Land use policy* 73, pp. 353–362.

Zeweld, W., Van Huylenbroeck, G., Tesfay, G. and Speelman, S. (2017) 'Smallholder farmers' behavioural intentions towards sustainable agricultural practices', *J. Environ. Manag*. 187, pp. 71–81.

Zhang, L., and McDowell, W. C. (2009) 'Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords', *Journal of Internet Commerce*, 8(3-4), pp. 180–197. http://doi.org/10.1080/15332860903467508

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E. and Mayhorn, C. B. (2014) 'One Phish, Two Phish, How to Avoid the Internet Phish Analysis of Training Strategies to Detect Phishing Emails', *In Proceedings of the Human Factors and Ergonomics Society AnnualMeeting*, Vol. 58, No. 1, pp. 1466-1470. SAGE Publications.

Zielinska, O., Welk, A., Mayhorn, C., and Murphy-Hill, E. (2016). 'The Persuasive Phish: Examining the Social Psychological Principles Hidden in Phishing Emails', Proceedings of the Symposium and Bootcamp on the Science of Security, pp.126-126. http://dx.doi.org/10.1145/2898375.2898382

Appendix A : Emails Respondents Survey

In this survey, you are asked to provide the information requested in the first section before proceeding to the subsequent sections. You will then be required to consider nine separate emails and answer the associated questions for each.

Each of the emails in this survey have been selected based on the most popular websites and social media applications used. Should you be unfamiliar with any of the organisations mentioned in the email, please do still take the time to consider the content of the email and answer the questions in each section fully.

Section 1 :

Q1.What is your gender?

- ○ Male
- ○ Female

Q2.Which age group do you belong to?

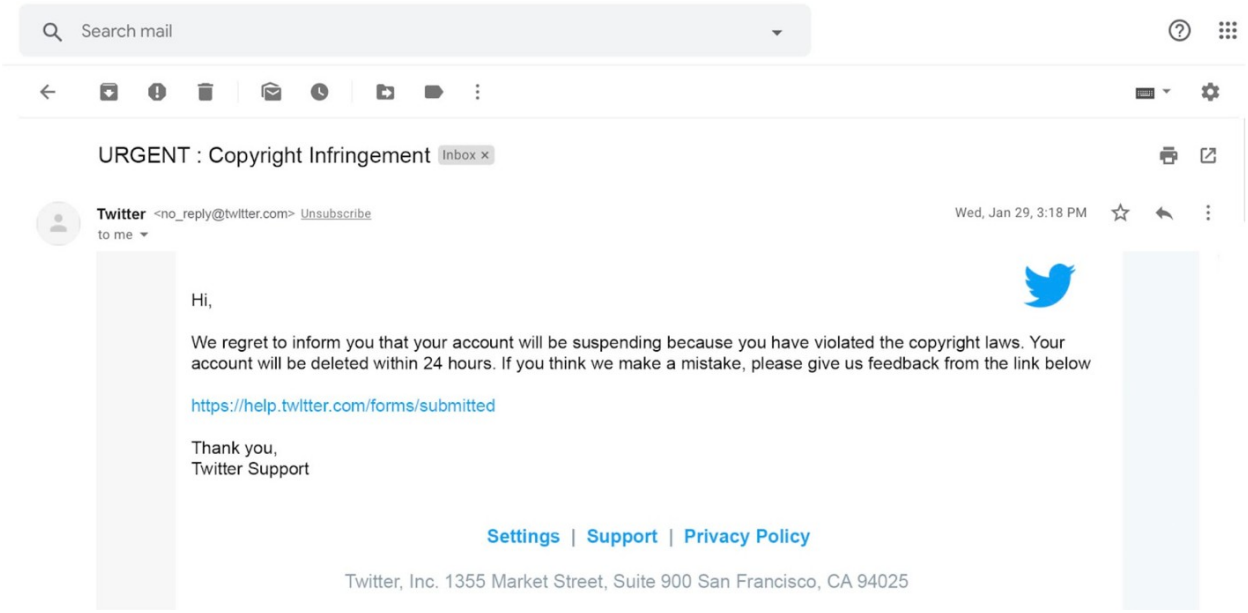
- ○ Less than 18
- ○ 18 - 21
- ○ 22 - 24
- ○ 25 and older

Q3.In which college are you studying?

- ○ Computer Sciences and Information Technology
- ○ Engineering
- ○ Medicine
- ○ Business Administration

Section 2 :

Email (1)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

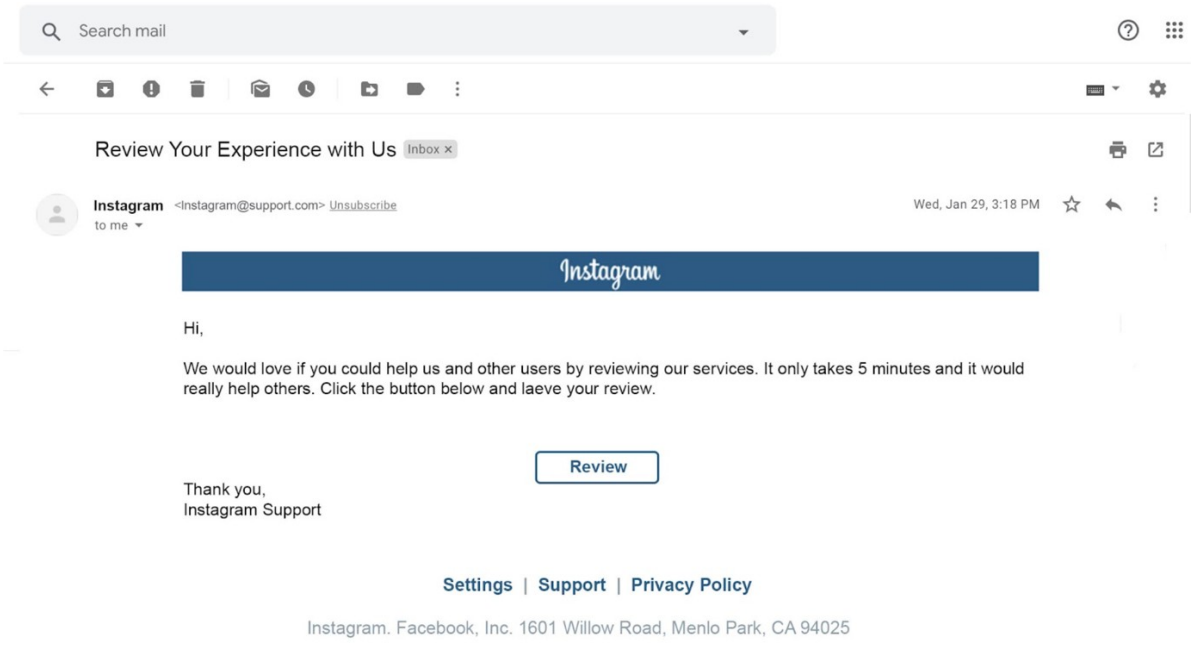
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (2)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behavior (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

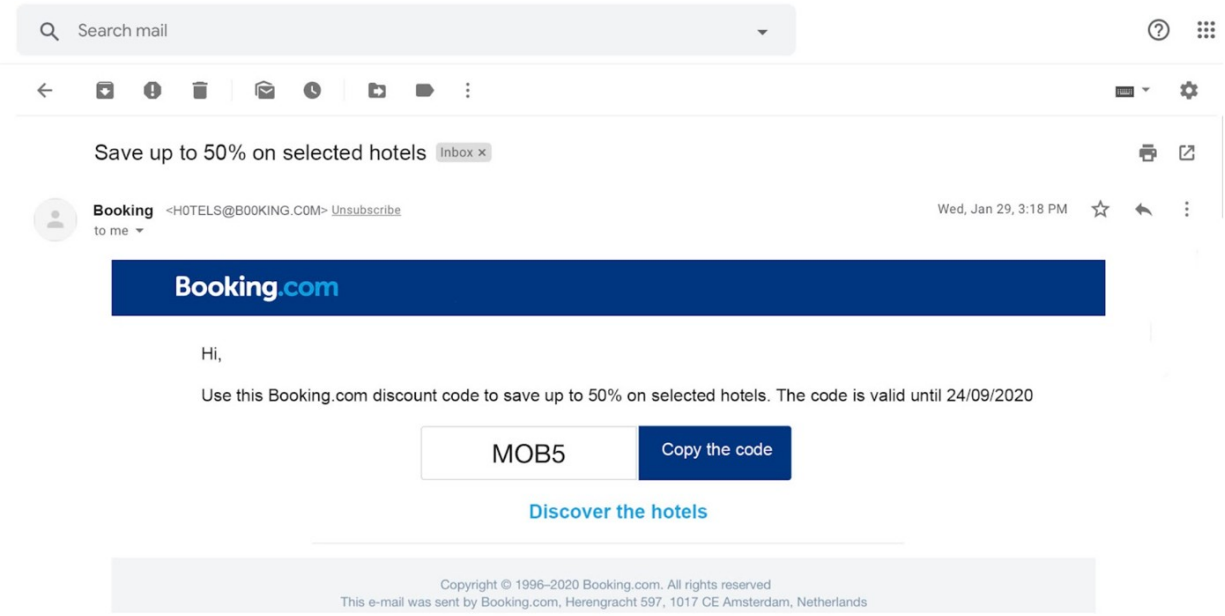
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (3)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

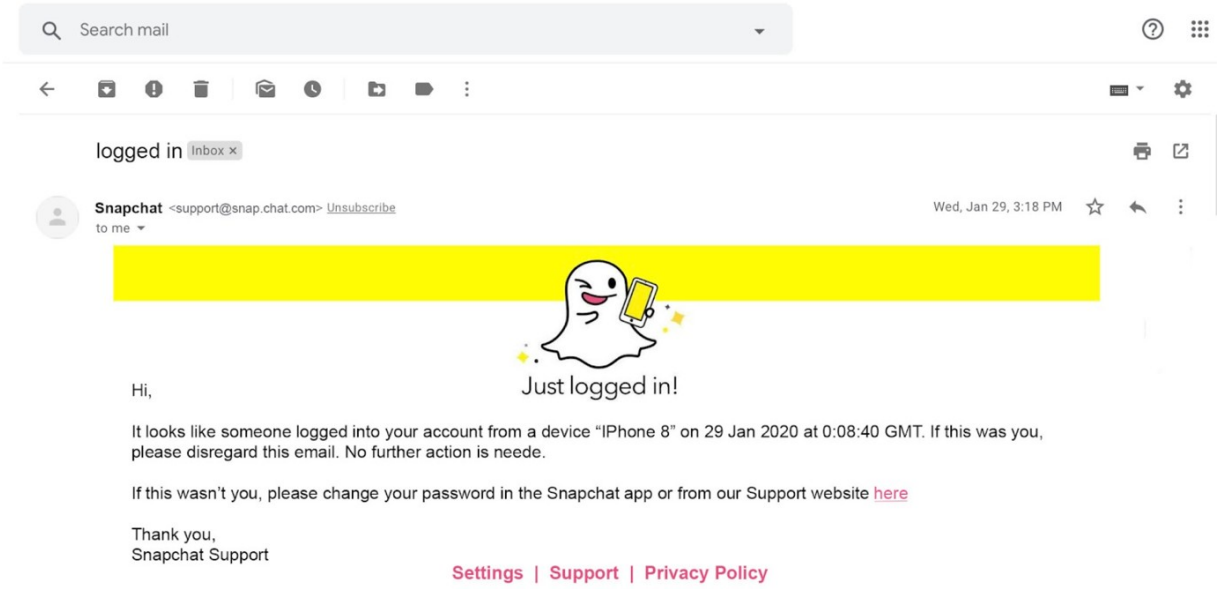
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (4)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

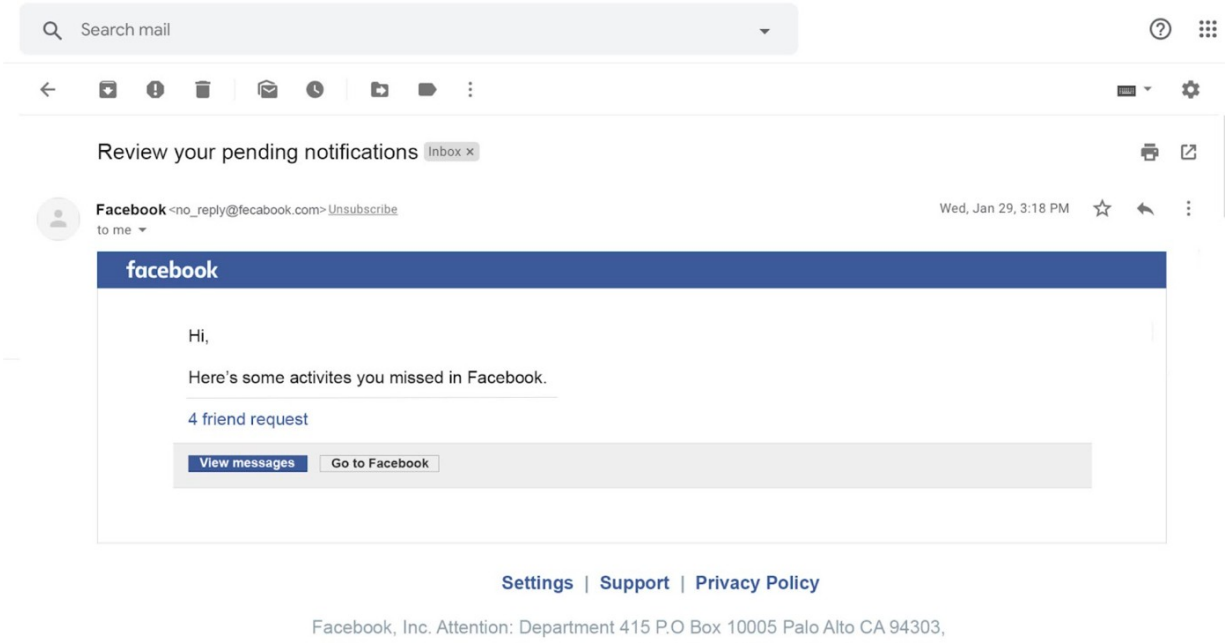
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (5)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

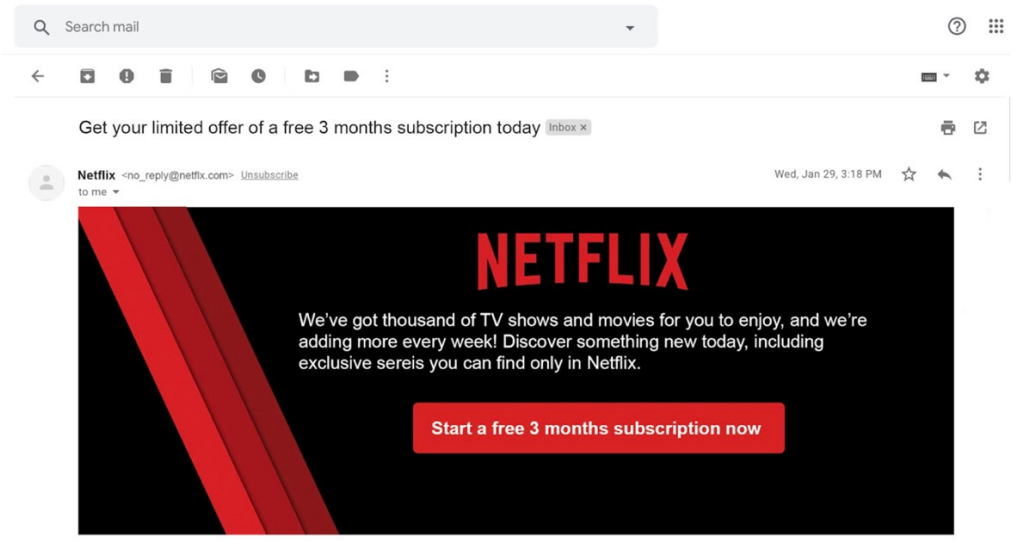
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (6)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

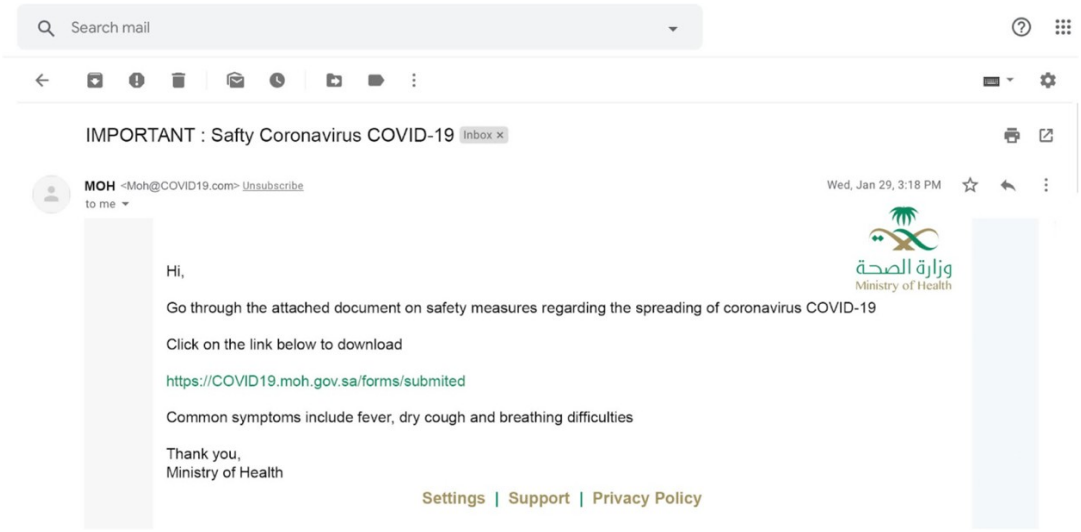
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (7)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

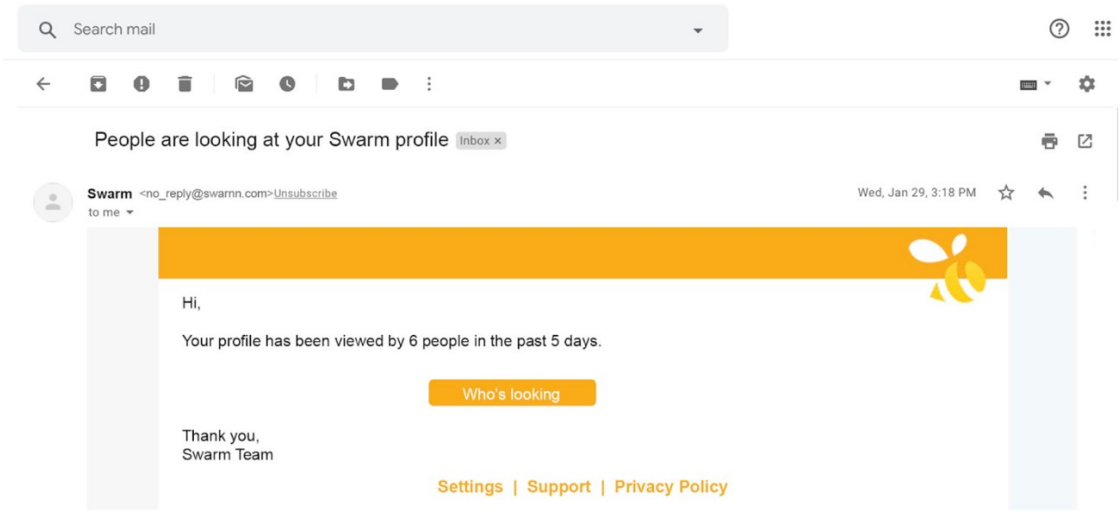
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (8)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

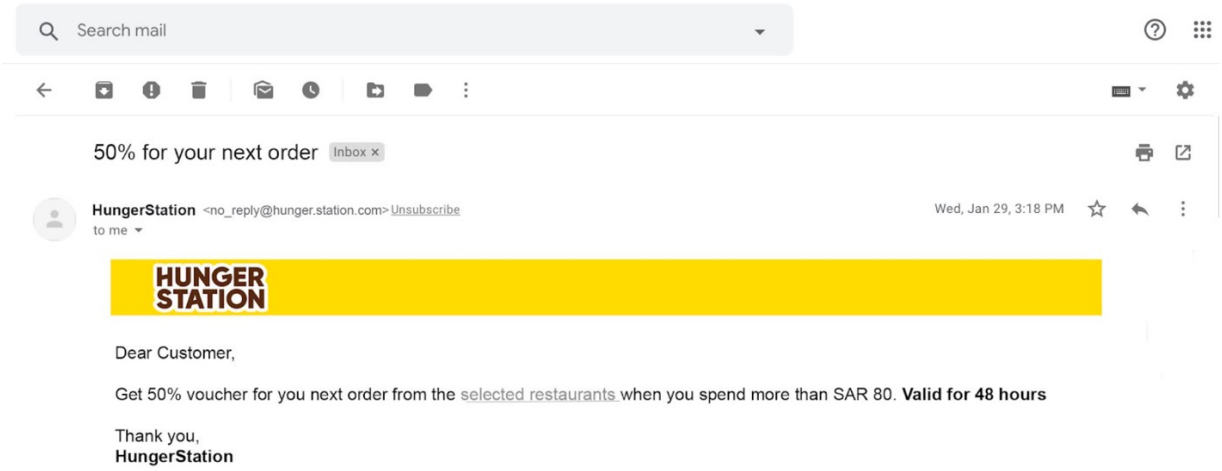
Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Email (9)



Q1. I believe responding to these types of emails is good for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q2. I believe responding to these types of emails is useful for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q3. I believe responding to these types of emails is important for me

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q4. People who influence my behaviour (e.g., my family and/or my friends) think that I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q5. People who are important to me or close to me (e.g., my family and/or my friends) have spoken highly about this organization and think I should respond to these types of emails

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q6. If I wanted to, I could seek the advice of people

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q7. For me, the decision to respond or take action is my own

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q8. For me, the decision to respond or take action is easy

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q9. I would respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Q10. I intend to respond to the email

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Appendix B : Consent Form for PhD Research Study

Consent Form for PhD Research Study

Name of department: Computer Science
Title of the study: An investigation of factors that contribute to the behavioural motivations of individuals when faced with social engineering attacks.

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.
- I consent to being audio recorded as part of the project.

(PRINT NAME)	
Signature of Participant:	Date:

Appendix C : Descriptive Statistics : Frequency Tables and Bar Charts for the Demographic Factors

Gender

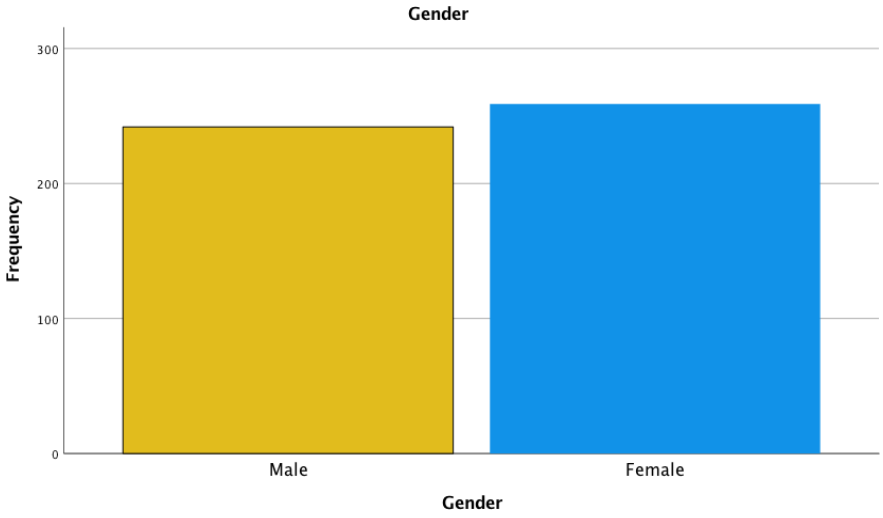
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	242	48.3	48.3	48.3
	Female	259	51.7	51.7	100.0
	Total	501	100.0	100.0	

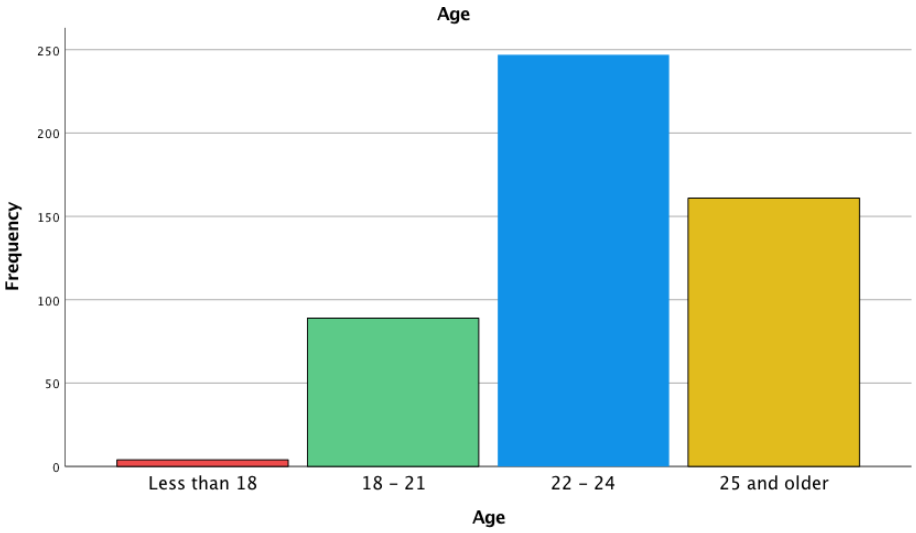
Age

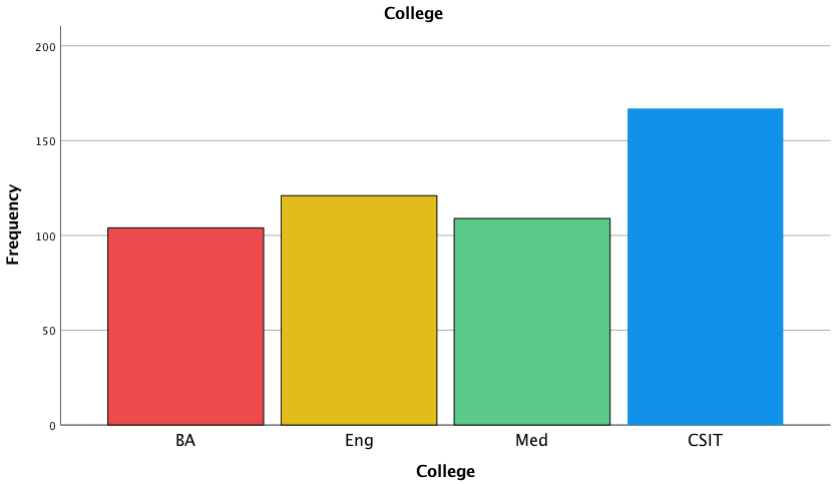
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 18	4	.8	.8	.8
	18 - 21	89	17.8	17.8	18.6
	22 - 24	247	49.3	49.3	67.9
	25 and older	161	32.1	32.1	100.0
	Total	501	100.0	100.0	

College

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	BA	104	20.8	20.8	20.8
	Eng	121	24.2	24.2	44.9
	Med	109	21.8	21.8	66.7
	CSIT	167	33.3	33.3	100.0
	Total	501	100.0	100.0	


Gender
300
200
100
0
Frequency
Male
Female
Gender


Age
250
200
150
100
50
0
Frequency
Less than 18
18 – 21
22 – 24
25 and older
Age


College
200
150
100
50
0
Frequency
BA
Eng
Med
CSIT
College

Appendix D : Multi Linear Regression Analysis Results

1. Assessment the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Authority strategy.

Model	Variables Entered	Variables Removed	Method
1	Authority (PBC), Authority (ATT), Authority (SN)[b]	.	Enter

a. Dependent Variable: Authority (IN)

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.734[a]	.538	.536	.562

a. Predictors: (Constant), Authority (PBC), Authority (ATT), Authority (SN)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	183.393	3	61.131	193.277	<.001[b]
	Residual	157.195	497	.316		
	Total	340.587	500			

a. Dependent Variable: Authority (IN)

b. Predictors: (Constant), Authority (PBC), Authority (ATT), Authority (SN)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	.529	.164		3.220	.001
	Authority (ATT)	.519	.046	.468	11.386	<.001
	Authority (SN)	.229	.036	.259	6.285	<.001
	Authority (PBC)	.139	.053	.109	2.617	.009

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	3.509	.209		16.802	<.001
	Gender	.217	.070	.142	3.075	.002
	Age	.010	.051	.009	.188	.851
	College	-.003	.031	-.004	-.087	.931

a. Dependent Variable: ATotal

2. Assessment the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Social Proof strategy.

Model	Entered	Removed	Method
1	Social Proof (PBC), Social Proof (SN), Social Proof (ATT)[b]	.	Enter

a. Dependent Variable: Social Proof (IN)

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.719[a]	.518	.515	.892

a. Predictors: (Constant), Social Proof (PBC), Social Proof (SN), Social Proof (ATT)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	424.418	3	141.473	177.714	<.001[b]
	Residual	395.646	497	.796		
	Total	820.064	500			

a. Dependent Variable: Social Proof (IN)

b. Predictors: (Constant), Social Proof (PBC), Social Proof (SN), Social Proof (ATT)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	-.054	.159		-.338	.735
	Social Proof (ATT)	.581	.097	.431	5.982	<.001
	Social Proof (SN)	.381	.095	.285	4.029	<.001
	Social Proof (PBC)	.078	.050	.052	1.546	.123

a. Dependent Variable: Social Proof (IN)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	2.077	.331		6.271	<.001
	Gender	.050	.112	.021	.444	.658
	Age	.227	.080	.135	2.828	.005
	College	-.094	.049	-.089	-1.914	.056

a. Dependent Variable: SPTotal

3. Assessment the impact of (ATT, SN and PBC) on (IN) to respond to phishing emails under Scarcity strategy

Model	Entered	Removed	Method
1	Scarcity (PBC), Scarcity (SN), Scarcity (ATT)[b]	.	Enter

a. Dependent Variable: Scarcity (IN)

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.705[a]	.498	.495	.927

a. Predictors: (Constant), Scarcity (PBC), Scarcity (SN), Scarcity (ATT)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	423.209	3	141.070	164.134	<.001[b]
	Residual	427.161	497	.859		
	Total	850.370	500			

a. Dependent Variable: Scarcity (IN)

b. Predictors: (Constant), Scarcity (PBC), Scarcity (SN), Scarcity (ATT)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.281	.188		1.493	.136
	Scarcity (ATT)	.318	.080	.235	3.989	<.001
	Scarcity (SN)	.599	.068	.490	8.742	<.001
	Scarcity (PBC)	.024	.066	.015	.362	.718

a. Dependent Variable: Scarcity (IN)

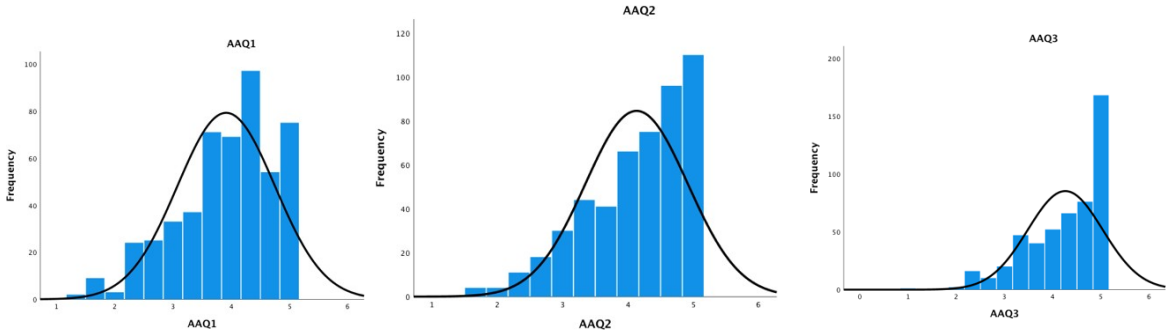
Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.426	.332		10.313	<.001
	Gender	-.094	.112	-.039	-.842	.400
	Age	.050	.081	.030	.622	.534
	College	-.076	.049	-.073	-1.551	.121

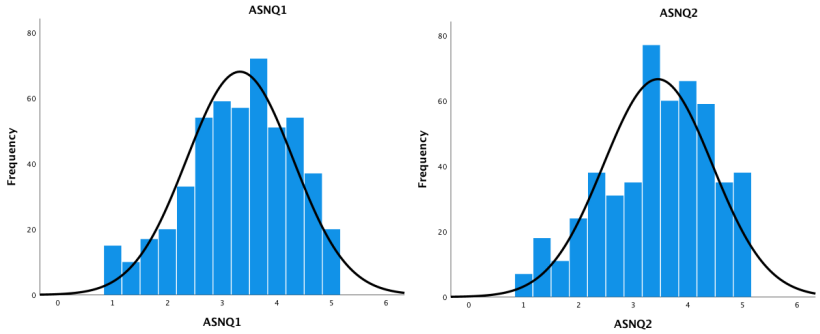
a. Dependent Variable: ScTotal

Appendix E : Data Normality Distribution (Histogram)

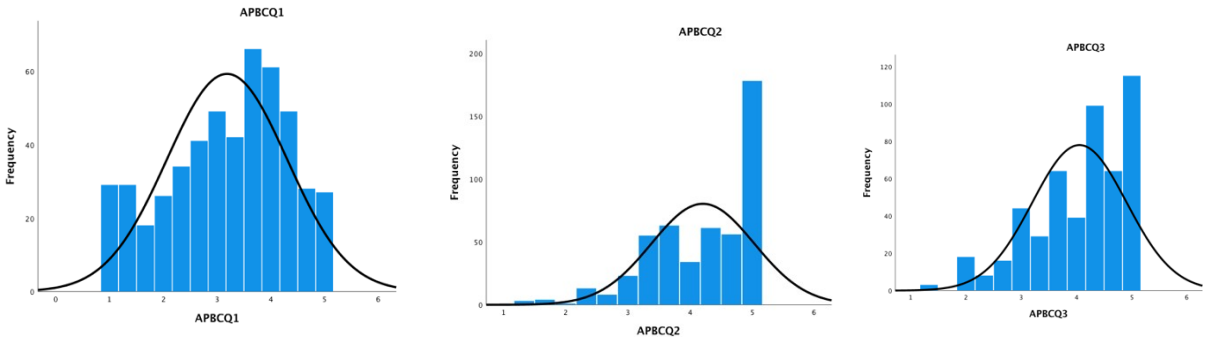
Attitude (ATT) Questions under the Authority strategy:



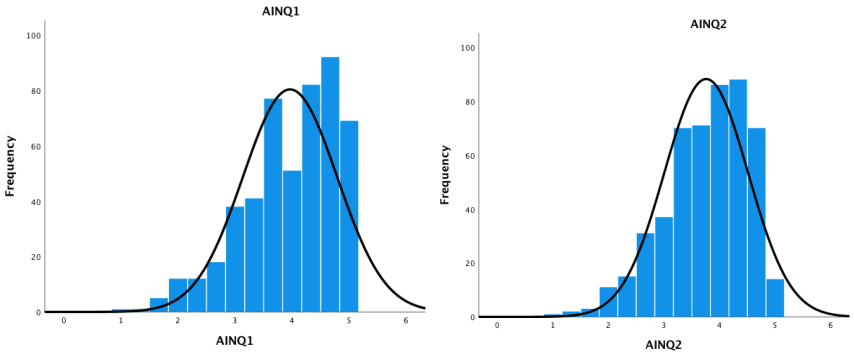
Subjective Norms (SN) Questions under the Authority strategy:



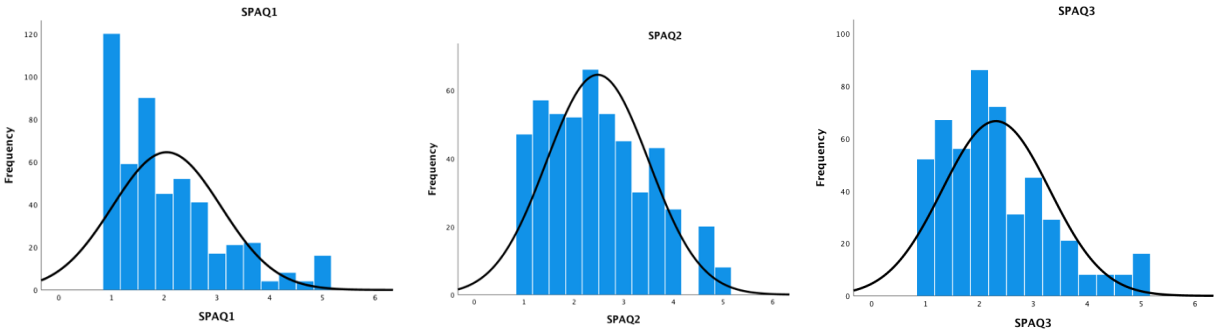
Perceived Behavioural Control (PBC) Questions under the Authority strategy:



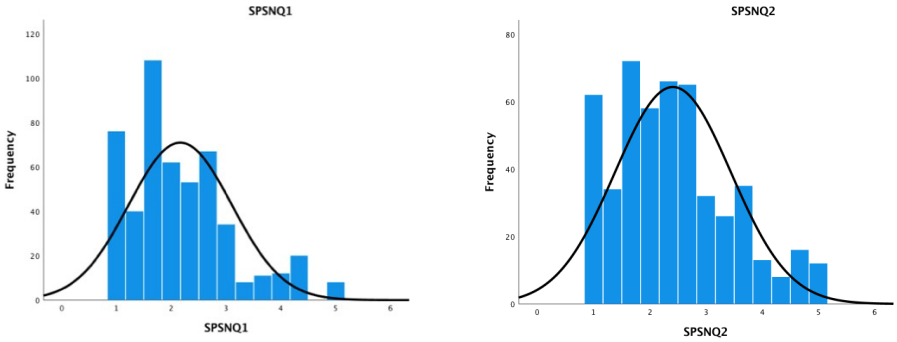
Intention (IN) Questions under the Authority strategy:



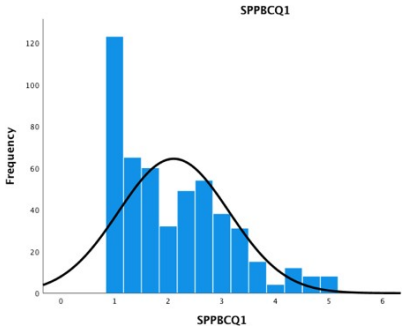
Attitude (ATT) Questions under the Social Proof strategy:

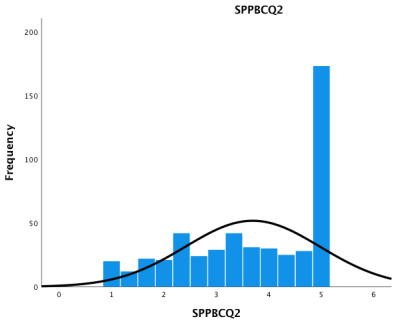


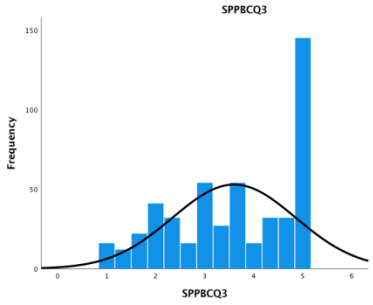
Subjective Norms (SN) Questions under the Social Proof strategy:



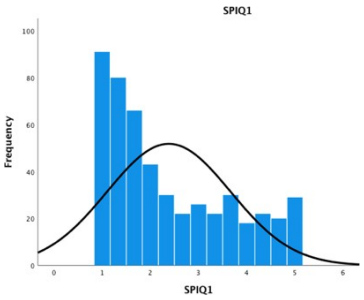
Perceived Behavioural Control (PBC) Questions under the Social Proof strategy:

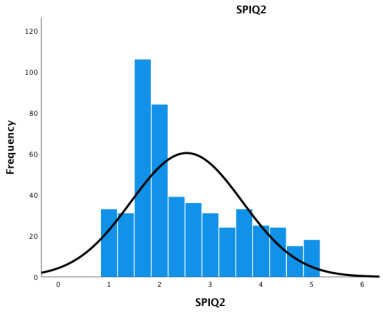




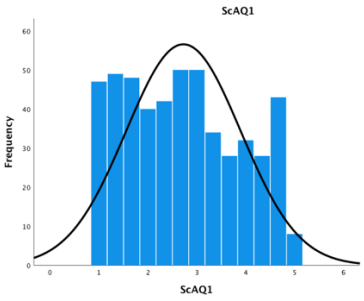


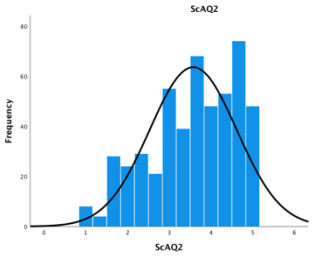
Intention (IN) Questions under the Social Proof strategy:

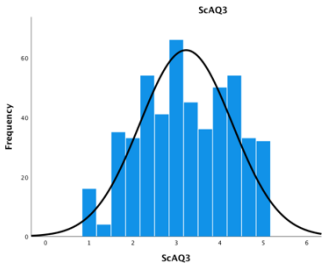




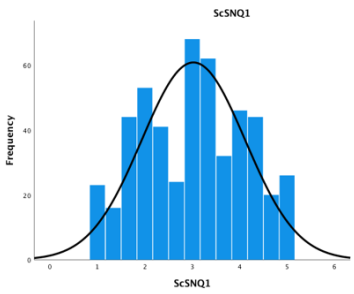
Attitude (ATT) Questions under the Scarcity strategy:

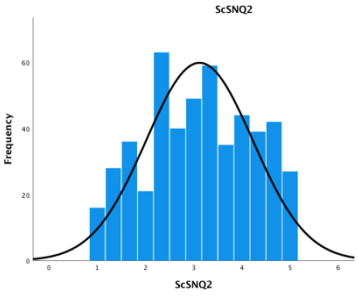




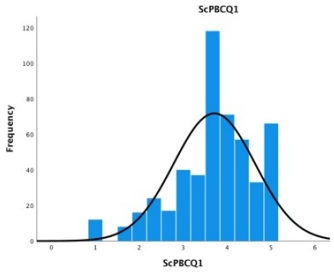


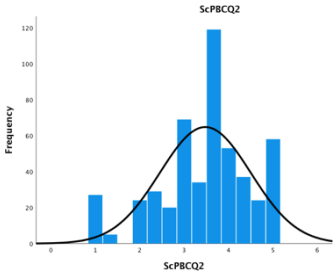
Subjective Norms (SN) Questions under the Scarcity strategy:

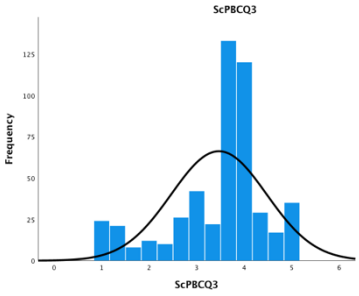




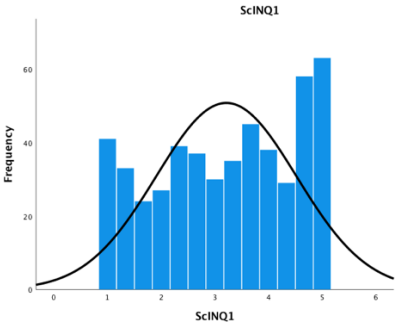
Perceived Behavioural Control (PBC) Questions under the Scarcity strategy:

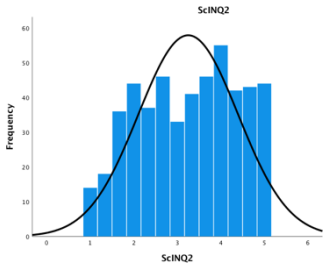






Intention (IN) Questions under the Scarcity strategy:





Appendix F : Scenarios/Emails under Social Engineering Persuading Strategies (SEPS)

1. Scenarios under the Authority strategy :

Scenario 1: An email from Twitter

The participant is presented with an email from twitter about deleting their account. It further presents a time constraint along with a link to feedback if a mistake was made. The content of this phishing email has a grammatical error. Besides, the sender email address is incorrect and the usage of word 'Urgent' in the subject of the email, inculcates fear and need for immediate action.

Scenario 2: An email from Snapchat

The participant is presented with an email from Snapchat providing information of last login from a device. It further requests for password change action in case it was not the user. The content of this phishing email has a spelling mistake. This scenario presents the participant with an incorrect sender's email address.

Scenario 3: An email from Minister of Health

The participant is presented with an email from the Government of Saudi Arabia (Ministry of Health) providing a link as well as an attachment for coronavirus safety measures. The content of Phishing email includes misspelled ('submitted') and redundant words along with unprofessional language. Here, although the sender email is incorrect, the participants are presented with a misspelled word, COVID, not with the letter 'I' but with lowercase letter 'l' (Uppercase – 'L') in the URL

2. Scenarios under the Social Proof strategy :

Scenario 4: A email from Instagram

The participant is presented with an email from Instagram requesting feedback. It provides a link to the review form for the user to leave reviews that will help other users' or improve the functionality. The content of this phishing email has unprofessional language along with peculiar verbiage. The sender email is incorrect and the word 'leave' is spelled as 'leave'.

Scenario 5: An email from Facebook

The participant is presented with an email from Facebook about pending notifications. It gives an option to the user to view the friend request notification by either clicking on the 'go to Facebook' link or 'view friend request'. The content of this phishing email has unprofessional language. The sender email is incorrect along with misspelled words and grammatical errors in the verbiage of the email.

Scenario 6: An email from swarm

The participant is presented with an email from Swarm about who all are viewing the account. It gives an option to the user to view other users' via a link. The content of this phishing email has unprofessional language. This scenario had an incorrect sender.

3. Scenarios under the Scarcity strategy :

Scenario 7: An email from Booking.com

The participant is presented with an email from booking.com with a 50% off offer when reserving hotels. The offer can be availed by copying the discount code, besides, it provides a link to explore the hotels. The content of this phishing email is missing punctuation marks. This scenario had an incorrect sender.

Scenario 8: An email from Netflix

The participant is presented with an email from Netflix with a limited time offering a 3-month subscription. The offer can be availed by clicking on the provided link. The content of this phishing email has unprofessional verbiage and the font does not match the original Netflix font. The sender email is incorrect along with misspelled words and grammatical errors in the verbiage of the email.

Scenario 9: An email from Hunger station

The participant is presented with an email from Hunger Station (Food delivery application) with 50% off on the next order. Here, the user is required to spend SAR 80 to receive 50% off on the order. The content of this phishing email has unprofessional verbiage, the subject of the email has a grammatical error, the words in the content were misspelled and the sender details were incorrect.

Appendix G : Factor Analysis tests results

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.842
Bartlett's Test of Sphericity	Approx. Chi-Square	3753.702
	df	36
	Sig.	.000

Communalities

	Initial	Extraction
AAQ1	1.000	.866
AAQ2	1.000	.879
AAQ3	1.000	.911
ASNQ1	1.000	.918
ASNQ2	1.000	.908
APBCQ2	1.000	.877
APBCQ3	1.000	.870
AINQ1	1.000	.927
AINQ2	1.000	.936

Extraction Method: Principal Component Analysis.