

# **MARA AND PUBLIC USER CHARACTERISTICS IN RESPONSE TO PHISHING EMAILS**

*Zalina Binti Ayob*

This dissertation is submitted for the degree of  
Doctor of Philosophy

School of Computer Science  
University Of Strathclyde  
United Kingdom

2020

## **Statement of Original Authorship**

The thesis is 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 degree.

The copyright of the thesis belongs to the author under the terms of the United Kingdom Copyright Acts as qualified by University Of Strathclyde Regulation 3.50. Due acknowledgement must always be made of the use of material contained in, or derived from, this thesis.

Signed:

A handwritten signature in black ink, appearing to read 'John'.

Date: 15 May 2020

# Acknowledgements

First, I am grateful to Allah for giving me the endurance to finish my PhD studies despite the many difficulties along the way. I am also grateful to my family. I thank my husband, kids, sisters, and my mother for their great support throughout my studies. I thank Allah every day for this great privilege for having them with me.

Second, I like to express my deepest gratitude to my principal supervisor, Dr. George R S Weir. Thank you for believing in me, for your tremendous support, encouragement, and patience, and for providing the invaluable insight necessary to fulfil the research objectives. Your helpful advice, support and continuous feedback were invaluable, for which I am incredibly grateful. Throughout this journey, you have been a great source of inspiration and strength to me.

With immense gratitude, I acknowledge my financial support, Majlis Amanah Rakyat (MARA), which also my employer for sponsoring my study. Finally, great appreciation goes to my friends, who always lend me their support and encouragement.

# Abstract

“Social Engineering” refers to the attacks that deceive, persuade and influence an individual to provide information or perform an action that will benefit the attackers. Fraudulent and deceptive individuals use social engineering traps and tactics through Social Networking Sites (SNSs) and electronic communication forms to trick users into obeying them, accepting threats, falling victims to various silent crimes such as phishing, clickjacking, malware installation, sexual abuse, financial abuse, identity theft and physical crime. Although computers can enhance our work activities, e.g., through greater efficiency in document production and ease of communication., the reliance on its benefits has reduced with the introduction of social engineering threats.

Phishing email results in significant losses, estimated at billions of dollars, to organisations and individual users every year. According to the 2019 statistics report from retruster.com, the average financial cost of a data breach is 3.8 million dollars, with 90% of it coming from phishing attacks on user accounts.

To reduce users’ vulnerability to phishing emails, we need first to understand the users’ detection behaviour. Many research studies focus only on whether participants respond to phishing or not. A widely held view that we endorse is that this continuing challenge of email is not wholly technical in nature and thereby cannot be entirely resolved through technical measures. Instead, we have here a socio-technical problem whose resolution requires attention to both technical issues

and end-users' specific attitudes and behavioural characteristics. Using a sequential exploratory mixed method approach, qualitative grounded theory is used to explore and generate an in-depth understanding of what and why the phishing characteristics influence email users to judge the attacker as credible. Quantitative experiments are used to relate participants' characteristics with their behaviour. The study was carefully designed to ensure that valid data could be collected without harm to participants, and with University Ethics Committee approval.

The research output is a new model to explain the impact of users' characteristics on their detection behaviour. The model was tested through two study groups, namely Public and MARA . In addition, the final model was tested using structural equation modelling (SEM). This showed that the proposed model explains 17% and 39%, respectively, for the variance in Public and MARA participants' tendency to respond to phishing emails. The results also explained which, and to what extent, phishing characteristics influence users' judgement of sender credibility.

## Table of Contents

Abstract.....	iv
Chapter 1	Introduction..... 1
1.1	Background..... 1
1.2	Research Motivation..... 8
1.3	Research focus..... 9
1.4	Research Question..... 14
1.5	Research Significance and Contribution..... 16
1.6	Study Design and Limitation..... 18
Chapter 2	Literature Review.....20
2.1	The Evolution of Phishing Attacks.....22
2.2	Types of Attack.....23
2.2.1	Social engineering attacks..... 24
2.3	Influence of spam/ phishing attacks..... 26
2.4	Email.....27
2.4.1	Phishing Email features..... 28
2.4.2	Persuasion techniques.....31
2.5	Decision Making.....34
2.5.1	The model of detecting deception (MDD) 34
2.5.2	The Decision-Making Model.....38
2.5.3	The Elaboration Likelihood Model (ELM)..... 39
2.6	Detector and Victim Cognitive Process.....40
2.7	Current Countermeasure.....41
2.7.1	Spam Detection.....42
2.7.2	Detecting Computer Operated Accounts..... 43
2.7.3	Detecting Cloned Profiles.....44
2.7.4	Owners' Profiling Classification..... 45
2.7.5	Detecting user susceptibility to Social Engineering Victimization 46
2.8	Gaps in Users' Detection Behaviour studies..... 48
2.9	Variables used in User Detection..... 50
2.9.1	Cultural..... 51
2.9.2	Personality..... 52
2.10	Other Related Variables in Phishing Email Study.....53
2.10.1	Age.....53

2.10.2	Gender.....	53
2.10.3	Education Level.....	54
2.10.4	Internet Experience.....	54
2.10.5	Email Experience.....	55
2.11	Study Group Background.....	56
2.11.1	The Role and Function Of MARA.....	56
2.11.2	MARA as the Studied Agency for This Research Study.....	57
2.11.3	Public Group.....	58
Chapter 3	Research Model.....	60
3.1	Model Selection.....	60
3.1.1	Theory of Deception.....	61
3.1.2	Unified Theories of Acceptance and Use of Technology Model (UTAUT)	63
3.1.3	The Big Five Personality Model.....	64
3.2	Research Hypothesis.....	66
3.2.1	Trust.....	66
3.2.2	Usage.....	67
3.2.3	Manage.....	67
3.2.4	Big Five Personality dimensions.....	68
3.2.5	Experience.....	69
3.2.6	Susceptibility.....	69
3.2.7	Demographic characteristics.....	70
3.2.8	Response.....	71
Chapter 4	Research Methodology.....	74
4.1	Methodology/model choice.....	74
4.2	Participant Selection.....	75
4.3	Data Collection Method.....	79
4.3.1	Study One ( Survey ).....	79
4.3.2	Study Two (Experiment).....	92
4.3.3	Development Of Email Experiment.....	97
4.3.4	Content Of Experimental Email And Victims Identification.....	98
4.3.5	Study Three (Interview).....	99
4.3.6	Difference Between Mara and Public Group Studies.....	102
Chapter 5	Quantitative Results.....	104
5.1	Overview.....	104
5.2	Quantitative Analysis.....	104
5.2.1	Data Preparation.....	105
5.2.2	Demographic items.....	105

5.2.3	Age and Gender.....	106
5.2.4	Internet Activities.....	110
5.2.5	Demographic Analysis.....	116
5.3	Instrument Validity.....	125
5.3.1	Reliability.....	125
5.3.2	Variable validity.....	126
5.4	Hypothesis Testing.....	131
5.4.1	The need for regression for hypothesis testing.....	132
5.4.2	Structural equation modelling (SEM).....	143
5.5	Summary.....	146
Chapter 6	Qualitative Analysis.....	148
6.1	Reliability and Validity.....	148
6.2	Analytic Procedure.....	150
6.2.1	Data reduction.....	150
6.2.2	Data display.....	151
6.2.3	Data interpretation.....	151
6.3	Results.....	152
6.3.1	Detectors' behaviour.....	152
6.3.2	Victims behaviour.....	153
6.3.3	Awareness of phishing email cues.....	157
6.4	Summary.....	158
Chapter 7	Discussion.....	160
7.1	Summary of Findings.....	160
7.2	Comparison of results from MARA and Public groups.....	163
7.2.1	Response Rate.....	164
7.2.2	Users' Characteristics.....	165
7.3	The implication of findings for defensive strategies.....	168
7.3.1	Focus on email content tricks.....	168
7.3.2	Inability to detect cues.....	170
7.3.3	Inefficiency in dealing with emails.....	170
7.4	Recommendations.....	171
7.4.1	Victims.....	172
7.4.2	Security aid designer.....	173
7.4.3	Organisation responsibility.....	173
7.5	Summary.....	175
Chapter 8	Conclusion.....	176
8.1	Academic Contributions.....	177
8.2	Contribution to Practice.....	177



8.2.1	Susceptibility.....	177
8.2.2	Response.....	182
8.3	Types of Victims.....	183
8.4	Propose Strategies and Techniques.....	185
8.4.1	Training.....	186
8.4.2	Reward.....	189
8.4.3	Disciplinary Measures.....	190
8.5	Limitations of Study.....	191
	References.....	193
	Appendices.....	215

## LIST OF FIGURES

FIGURE 1: 10 RISKIEST COUNTRIES TO MALWARE ATTACKS (SOURCE: SOPHOSLAB)....	5
FIGURE 2: TRUST PATH ON PHISHING ATTACK (LI & WU, 2003).....	9
FIGURE 3: EMAIL-BASED PHISHING ATTACK (JAMPEN, GÜR, SUTTER, & TELLENBACH, 2020).....	21
FIGURE 4: CLASSIFICATION OF PHISHING ATTACKS BASED ON TYPES OF FRAUD (B. B. GUPTA, ARACHCHILAGE, & PSANNIS, 2017).....	24
FIGURE 5(A), (B): EXAMPLES OF MALAYSIAN NATIONAL BANK PHISHING EMAILS.....	29
FIGURE 6: QUALITY MEASUREMENT FRAMEWORK (WANG ET AL., 2009).....	33
FIGURE 7: MODEL OF DETECTING DECEPTION BY (GRAZIOLI, 2004).....	35
FIGURE 8: MDD MODEL BY (WRIGHT, CHAKRABORTY, BASOGLU, & MARETT, 2010B)	37
FIGURE 9: DIFFERENCES BETWEEN DETECTORS AND VICTIMS (GRAZIOLI, 2004).....	38
FIGURE 10: PROPOSED SOLUTIONS IN THE LITERATURE.....	42
FIGURE 11: UTAUT MODEL [178].....	64
FIGURE 12: COGNITIVE AND BEHAVIOUR IN DETECTION PROCESS.....	65
FIGURE 13: RESEARCH MODEL WITH THE HYPOTHESIS.....	66
FIGURE 14: PROPOSED RESEARCH DESIGN.....	78
FIGURE 15: EMAIL EXPERIMENT 1.....	94
FIGURE 16: EMAIL EXPERIMENT 2.....	94
FIGURE 17: EMAIL EXPERIMENT 3.....	95
FIGURE 18: MARA GROUP METHOD.....	103
FIGURE 19: PUBLIC GROUP METHOD.....	103
FIGURE 20: RESPONDENT DISTRIBUTION.....	107
FIGURE 21: INTERNET ACTIVITY (PUBLIC).....	111
FIGURE 22: INTERNET ACTIVITY (MARA).....	111
FIGURE 23: MARA RESPONDENTS AGE FREQUENCY CHART.....	118
FIGURE 24: PUBLIC RESPONDENTS AGE FREQUENCY CHART.....	119
FIGURE 25: FREQUENCIES CHART GENDER (MARA).....	121
FIGURE 26: FREQUENCIES CHART GENDER (PUBLIC).....	121

FIGURE 27: REGRESSION SCATTER PLOT (PUBLIC).....	136
FIGURE 28: REGRESSION SCATTER PLOT (MARA).....	137
FIGURE 29: STRUCTURAL MODEL FOR PUBLIC GROUP.....	144
FIGURE 30: STRUCTURAL MODEL FOR MARA GROUP.....	145
FIGURE 31: USERS' ACTION WHEN DEALING WITH PHISHING EMAILS.....	154
FIGURE 32: IMPACT OF USERS' CHARACTERISTICS ON RESPONSE TO THE PHISHING EMAIL.....	161

## LIST OF TABLES

TABLE 1: KEY DESIGN FEATURES.....	30
TABLE 2: MESSAGE STRUCTURE (SHARMA, 2010).....	33
TABLE 3: DIFFERENCES BETWEEN DETECTORS AND VICTIMS.....	40
TABLE 4: FACET AND DOMAIN OF THE NEO PI-R INVENTORY (P T COSTA & MCCRAE, 1992).....	65
TABLE 5: SUMMARY OF CONSTRUCTS.....	71
TABLE 6: RESEARCH HYPOTHESES.....	72
TABLE 7: CODE ITEMS FOR TRUST.....	85
TABLE 8: CODE ITEMS FOR USAGE.....	85
TABLE 9: CODE ITEMS FOR MANAGE.....	86
TABLE 10: CHARACTERISTICS OF PHISHING EMAILS.....	89
TABLE 11: EXPERIENCE AND GENDER ITEMS.....	89
TABLE 12: CHARACTERISTICS OF EMAIL.....	95
TABLE 13: AGE AND GENDER (MARA).....	106
TABLE 14: AGE AND GENDER (PUBLIC).....	106
TABLE 15: DESCRIPTIVE STATISTICS FOR EMAIL USAGE.....	109
TABLE 16: TRUST RESULTS FOR MARA AND PUBLIC.....	112
TABLE 17: USAGE MEAN FOR MARA AND PUBLIC.....	112
TABLE 18: MANAGE MEAN FOR MARA AND PUBLIC.....	113
TABLE 19: SUSCEPTIBILITY MEAN FOR MARA AND PUBLIC.....	113
TABLE 20: BIG FIVE PERSONALITY DIMENSION MEAN FOR MARA AND PUBLIC.....	114
TABLE 21: FIVE DIMENSION MEAN FOR MARA AND PUBLIC.....	115
TABLE 22: FREQUENCY AGE - MARA.....	117
TABLE 23: CHI-SQUARED TEST AGE - MARA.....	117
TABLE 24: FREQUENCY AGE - PUBLIC.....	118
TABLE 25: CHI-SQUARED TEST AGE - PUBLIC.....	118
TABLE 26: FREQUENCY GENDER - MARA.....	120
TABLE 27: CHI-SQUARED TEST - GENDER MARA.....	120
TABLE 28: FREQUENCY GENDER - PUBLIC.....	120

TABLE 29: CHI-SQUARED TEST - GENDER MARA.....	120
TABLE 30: SPEARMAN'S RHO TEST ON EMAIL USAGE IN MARA.....	123
TABLE 31: RELIABILITY MEASURES.....	125
TABLE 32: MARA GROUP EXPLORATORY FACTOR ANALYSIS (EFA).....	127
TABLE 33: PUBLIC GROUP EXPLORATORY FACTOR ANALYSIS (EFA).....	128
TABLE 34: FACTOR LOADING MARA.....	130
TABLE 35: DISCRIMINATE VALIDITY (MARA).....	130
TABLE 36: COMPOSITE RELIABILITY (MARA).....	130
TABLE 37: FACTOR LOADING (PUBLIC).....	131
TABLE 38: DISCRIMINANT VALIDITY (PUBLIC).....	131
TABLE 39: COMPOSITE RELIABILITY (PUBLIC).....	131
TABLE 40: LINEAR REGRESSION WITH SUSCEPTIBILITY AS A DEPENDENT VARIABLE FOR MARA.....	134
TABLE 41: LOGISTIC REGRESSION WITH RESPONSE AS DEPENDENT VARIABLE FOR MARA.....	134
TABLE 42: LINEAR REGRESSION WITH SUSCEPTIBILITY AS A DEPENDENT VARIABLE FOR PUBLIC.....	135
TABLE 43: LOGISTIC REGRESSION WITH RESPONSE AS A DEPENDENT VARIABLE FOR PUBLIC.....	135
TABLE 44: COLLINEARITY STATISTICS.....	138
TABLE 45: LINEAR REGRESSION RESULT - SUSCEPTIBILITY (PUBLIC).....	138
TABLE 46: MODEL SUMMARY - SUSCEPTIBILITY (PUBLIC).....	138
TABLE 47: LINEAR REGRESSION RESULT - SUSCEPTIBILITY (MARA).....	139
TABLE 48: MODEL SUMMARY – SUSCEPTIBILITY (MARA).....	139
TABLE 49: PUBLIC LOGISTIC REGRESSION WITH A RESPONSE AS AN OUTCOME.....	140
TABLE 50: MODEL SUMMARY – RESPONSE (PUBLIC).....	140
TABLE 51: FINAL MARA LOGISTIC REGRESSION ON RESPONSE RESULT.....	141
TABLE 52: MODEL SUMMARY – RESPONSE (MARA).....	142
TABLE 53: LIST OF SUPPORTED HYPOTHESES.....	142
TABLE 54: R SOFTWARE RESULTS - PUBLIC.....	144
TABLE 55: R SQUARE VALUE - PUBLIC.....	145

TABLE 56: R SOFTWARE RESULTS - MARA..... 145

TABLE 57: R SQUARE VALUES - MARA..... 146

TABLE 58: INTER-CODER RELIABILITY..... 149

TABLE 59: CODEBOOK FOR ANALYSIS OF THE INTERVIEWS..... 151

TABLE 60: DETECTORS RESPONSE..... 153

TABLE 61: NAÏVE VICTIMS RESPONSE..... 154

TABLE 62: DOUBTFUL VICTIM RESPONSE..... 155

TABLE 63: RISK-TAKER VICTIMS' RESPONSE..... 156

TABLE 64: AWARENESS OF PHISHING EMAILS..... 158

## List Of Abbreviation

MDD	Model of Detection deception
Trust	Users' disposition to trust
Openness	Users' disposition to openness
Public	Users' who access email using free email account.
Activity	The type of activity on the Internet (Surfing,Social, transaction)
Detector	A user who manages to open and ignore the phishing email
Victim	A user who responds to phishing email

## Refereed Conference Paper

Ayob Z., Weir G.R.S. (2021) Is Human Behavior the Real Challenge in Combating Phishing. Cyber Physical, Computer and Automation System. Advances in Intelligent Systems and Computing, vol 1291. Springer, Singapore. [https://doi.org/10.1007/978-981-33-4062-6\\_3](https://doi.org/10.1007/978-981-33-4062-6_3)



# **Chapter 1 Introduction**

## **1.1 Background**

Since it was established in the 1960s by the U.S Department of Défense (Schneider, Evans, & Pinard, 2009), the Internet has become the most important and rapidly growing technology worldwide. It also offers continual improvement with a wide range of forms of communication. Email, cloud computing, data management and transfer, social networks like blogs and Facebook, and text messaging systems such as Twitter and SMS are information technology based on the Internet.

Due to the wide range of uses, the Internet is now cheaper and accessible for twenty-four hours and seven days a week. This reason supports the statistics done by InternetWorldStats.com where the number of population using the Internet from 2000 to 2018 dramatically growth from 28.7% up to 1,066% worldwide.

The Internet has provided a business opportunity for growth through the inception of online services. The most widely used applications on the Internet nowadays are Social Networking Sites (SNSs). The first recognizable SNSs was in 1997 with “SixDegrees.com” (Boyd & Ellison, 2010). Since then people have been attracted to SNSs that enable them to connect and communicate with each other depending on the nature of SNSs. This SNSs offer a wide range of technical features that enable people, companies, organizations or government agencies to perform a

variety of advanced services (boyd & Ellison, 2007)(Kizgin et al., 2020)(Shen, Chiou, Hsiao, Wang, & Li, 2016).

Business see the Internet as a core and the backbone of their daily business and SNSs as an opportunity for business. This can be seen with the growing number of services offered in the business using SNSs starting from promoting and marketing to dealing with customers online.

Ensuring the success of online services requires a high level of security, especially when it involves money and confidential data transactions such as online banking and shopping. These online services require access to sensitive and individual information and therefore, a similar degree of security by their traditional counterparts are involved. For example, customers are encouraged to use their personal identification number (PIN) at the auto teller machine (ATM) to guarantee safe transactions. The same concept needs to apply in online banking, where users are encouraged to employ an online PIN. Furthermore, additional identification verification through users' mobile number is added, such as One Time Password (OTP) and Type Allocation Code (TAC) to protect users' information. Unfortunately, some users still fail to satisfy these requirements, leading them to become victims of criminal activities (Camp, 2007).

Therefore, in online banking, customers are always advised to check the website's legitimacy and be aware of 'where' they made the transaction. They are also advised to not disclose personal information such as passwords by writing it in their phone or paper. However, not all users are willing to take this as security advice to prevent them from being vulnerable to attackers' requests (Mannan & van Oorschot, 2008).

Genius hackers will see SNSs such as Facebook, Twitter, Blog and many more as an opportunity to prey on their victims. They might get information about users' daily activities, lifestyle, employment status and attitude. This information can easily be found through users' comments and updates and even their friends network. In the current advanced and modern generation, the desire for information technology that pairs with the lifestyle in the sense of effectiveness and ease for societies are most in demand. This is proven when SNSs no longer require a computer but optionally, users can just use a smartphone or any latest mobile device such as a smart watch and tablet as long as they can access Internet connectivity.

However, the simplicity and advancement of technology can be a double-edged sword. While technology-based threats have been well discussed and directed in many studies, the issue of human threats seem less interesting to researchers in the information technology area, perhaps because of the complexity to understand and predict human behaviours associated with user's susceptibility to social engineering attacks.

(Schneier, 2000) defines social engineering as an action that involves persuading and manipulating legitimate user(s) of the information system to give or share the information that will allow the attacker to access the system. When the connection is successful, attackers become covetous by creating many new social engineering (SEs) attacks, such as phishing, scams, ransomware, and cyberbullying, creating a computer network as a victim to the attacks and threats (S. Gupta, Singhal, & Kapoor, 2017)

Email is not popular like other SNSs in terms of its functionality in support of social network development due to its one-way communication service. However, it

is still prevalent in a different way of use. One of them is in the verification procedure for online registration, such as creating an online banking account, social media, and other registration requirements that are needed for verification. The importance of email makes it no longer safe, and the information is constantly under threat where it can be intercepted, modified and exposed without users' knowledge. Moreover, facilities that are set up to monitor such attacks are also constantly under attack (Q. Zhang, Cheng, & Boutaba, 2010).

Email allows users to communicate very efficiently and has become an integral part of life for almost all daily activities, from working to socializing with family and friends. The impact of email in terms of popularity is more than memos or bulletin boards within organisations, and this can be seen from the growing number of email accounts worldwide, which expected will increase from 3.9 billion accounts in 2013 to over 4.9 billion accounts at the end of 2017 (Sara Radicati, Analyst, & Levenstein, 2013).

Email is still growing and remains the first choice of communication medium. However, as highlighted, email remains an effective medium for cybercriminals. Many attacks with clever designs, tricks and skills make expert users with advanced knowledge no exception of being susceptible to attackers (Aburrous, Hossain, Dahal, & Thabtah, 2010b).

In Malaysia, cybercrime is considered as a 'Ticking Bomb' by the Police Department and is a severe issues (Bernama, 2013) due to a loss of billions of Ringgit Malaysia (RM) every year. In addition, Malaysia was ranked at number five out of the ten riskiest and most vulnerable countries to cybercrime worldwide, as shown in Figure 1.

## MALAYSIA IS SIXTH MOST VULNERABLE TO CYBER CRIME



Figure 1: 10 Riskiest countries to Malware attacks (Source: SophosLab)

One of the primary forms of contribution to cybercriminal activity is users' attitude towards computer security and etiquette. They often take for granted the capability of computer systems which later opens a window of opportunity to an attacker. Phishing attacks are known for exploiting human characters (Karakasiliotis, Furnell, and Papadaki 2006) see this as an opportunity to deceive users and leverage attacks through phishing emails.

Moreover, phishing is a social engineering attack that no longer uses the state-of-the-art objective as before, by stealing data and spreading viruses; it is now simulating data breach and ransomware events. Many possible motivators drive phishing attacks, including illicit corporate espionage, political and financial benefits. Furthermore, (Cyveillance, 2015) claim the number of victims from phishing emails per day could reach 80,000 and involves a financial loss over millions and maybe up to billions of dollars. The actual figures cannot be identified due to unreported cases.

Unprepared users cannot defend themselves against phishing emails and are usually victims to attackers' baits (Downs, Holbrook, & Cranor, 2007). They are willing to give private information and comply to the contents in phishing emails. Many years ago, the motive of identity theft focused on establishing a trust connection between the attacker and users.

Previous research on email-borne threats focused on technical solutions and developing tools and software to prevent these threats from deceiving users (Purkait, 2012) (Tembe, Hong, Murphy-Hill, Mayhorn, & Kelley, 2013) (Yang, Xiong, Chen, Proctor, & Li, 2017). However, we forget that hackers are also human. Humans will always look for simple and easy ways to succeed. So, why would they need to bother with sophisticated ways to fight against complicated systems if they can simply trick users into giving up their information?. Moreover, the risk of attacks is associated with difficulty making judgment by users in a virtual environment. Research by (Zinoviev & Duong, 2009) suggests a significant difference between human behaviour in real life and their actions in a virtual environment. Nevertheless, persuasion research shows that people are more likely to obey, believe and accept the message when the presentation of the message appears to be credible and from a known sender (Hovland, Janis, & Kelly, 1953).

The problem of phishing emails becomes more complex when it targets every user who owns an email account regardless of their background. This will bring us to the question of which type of users are more vulnerable? Does a user's background play an important role in the users' vulnerability level?

Therefore, our study intends to investigate the impact of user behaviour on users' susceptibility to Social Engineering victimisation or the so-called phishing

email. Our research focused on two different target users; users who work in the same organisation and public users (different culture and background). In other words, this research aims to investigate how email users determine whether they encounter phishing or legitimate emails based on the experiment done. In addition, we developed a model that explains the characteristics in users that influence them to become susceptible to phishing. Finally, this research investigated the influence of each characteristic on users' susceptibility to phishing based on their demographics, such as gender, age, educational background, and frequency of email usage.

Therefore, as a resolution, we required both technical and specific human attitude as a solution. This combination of technical and human attitude towards email is a central issue to this research. Most researchers focused on the technical solutions while user attitude and behaviour perceived in emails receive less attention, and there are ongoing debates about the appropriateness of affirmation as a solution to combat threats.

Previous attention to technical perspective only should not be limited by demonstrating interest in understanding users' perceptions and behaviour. This is especially when most attacks today uses a method known as 'bait and hook' where users are deceived by its objective (Emm, 2006). Therefore, computer systems and networks should be reinforced to defy threats that are constantly looking for opportunities to intrude.

Phishing relies typically on social engineering to obtain credential access, where unaware users often provide ways to theft by leaving their information unsecured or unprotected. Furthermore, when an identity is used persuasively, this

type of behaviour leads to a social direction that requires a socio-technical solution instead of a technical solution only.

## **1.2 Research Motivation**

Since 2005, the risk of social engineering has become more popular and received serious attention, according to the Institute of Management and Administration findings. The report says they identified that social engineering was the top security threat in that year and will continue as a challenge in cybersecurity (S. Thompson, 2013).

Employees' behaviour causes around 70% of information security incidents and around 3% of an organisation's profit is lost due to those incidents (McIlwraith, 2006). Even though many organisations agree on the importance of predicting and controlling social engineering, many still fail to reach that goal (Brody, Brizzee, & Cano, 2012). In addition, research on SNSs security showed that most social engineering threats, such as spamming, social bots, and identity clones, mostly rely on the masquerade (fake identity) technique (Fire, Goldschmidt, & Elovici, 2014a).

A report from the "Information Security Breaches Survey 2015" stated, "Despite the increase in staff awareness training, people are as likely to cause a breach as viruses and other types of malicious software. It is fairly straightforward that people are the fundamental element of security and human error is the root cause of most security breaches.

It is strongly supported by experts, such as (Shaw, Chen, Harris, & Huang, 2009)(Lance Spitzner, 2010) (Nicholas Ismail, 2018), that the weakest link in



information security for an organisation comes from insiders. Regardless of their level or position, they can still be victims and businesses are still under risk from attacks such as fraud, money laundering, bribery, corruption and cybercrime, which has not shown a decrease of cases from year to year.

### 1.3 Research focus

User is the focus of this study since they are also the focus of phishing email attacks. Users are the target because they are known as the weakest link compared to the other two elements in the Internet security chain, namely servers and transit channels (Herzberg, 2009)(Bissell K, LaSalle RM, 2019). Figure 2 shows the path that comprises these three elements.

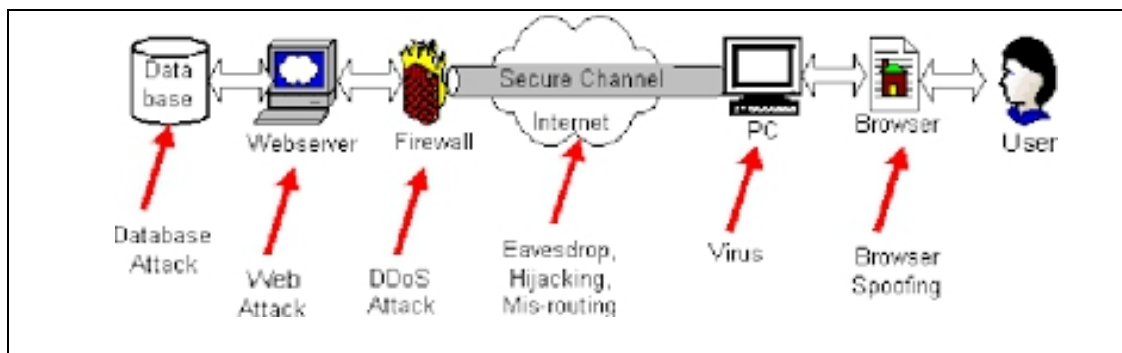


Figure 2: Trust path on phishing attack (Li & Wu, 2003)

When an email is sent to an addressee, some receivers may view it as public, whereas the sender thinks that every email sent is private. Therefore, the responsibility now depends on these three elements to protect the information and label it as “confidential information”. It does not matter what the contents or information are as people rely on this trusted path to convey the information to the authorised receiver.

Even confidential information is shared between servers and users through the transit channel, although only those with granted or authorised access are able to access the information. This can only be done with help from the email clients that make the forwarding process incredibly easy, with the result that the messages are often viewed by unintended third parties (Whitten & Tygar, 1999). An Internet server is designed to protect the information and confidentiality of the information and to build trust in the sender.

Protecting information throughout the chain is an important goal of Internet design. Engineers and experts are always finding ways to support demand changes on the Internet Of Things (IOT) by introducing many software for servers and advancing Internet communication protocol. The integrity of the transit channel is to ensure in protecting the data that they carry, all web clients used a few standard protocols. For example, a protocol named Secure Socket Layer (SSL) or Transport Layer Security (TLS) was named as a *de facto* form of protection (Oppliger, Hauser, & Basin, 2008). This protocol must ensure that the data exchange between parties is encrypted inside the channel (Chomsiri, 2007). Mobile devices, laptop and many other Internet devices are embedded with antivirus software as a final way to protect their information. Of course, users themselves know their confidential information and this makes them a key target for perpetrators.

Phishing attacks knowingly aim to exploit the weaknesses found in humans (end user) with the users' attitude of easily being tricked into revealing private information (Dhamija, Tygar, and Hearst 2006) reason why phishing becomes challenging to mitigate. For example, (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) found that end users failed to detect 29% of phishing attacks even after being trained with the best user awareness program.

The gap between what users think and what they are connected to (phishing) becomes the primary issue in many studies (Oppliger et al., 2008). Moreover, phishing is designed in chameleon to precisely look like a legitimate entity, although they are malicious. The numbers reported for these emails do not seem to end; hence urgent action is required to stop users from continuously becoming victims of phishing emails.

As the phishing problem takes advantage of human ignorance and a naive attitude, relying only on technology will fail to provide solutions and minimize the impact of these attacks. Awareness programs to educate users by teaching them cues<sup>1</sup> (Kumaraguru, 2009) is popular compared to investing in tools that can distinguish between legitimate and illegitimate websites (D. J. Kim, Ferrin, & Rao, 2008). However, despite many innovations, users still fall victim to phishing emails (Jagatic, Johnson, Jakobsson, & Menczer, 2007) (Coronges et al., 2012). Attackers are always trying to find new ways to succeed. The challenge also comes from users who resist to learned and do not retain their knowledge permanently. Although some researchers agree that user education is helpful (Kumaraguru, Rhee, Acquisti, et al., 2007), others also disagree (Görling, 2006). According to Stefan Gorling (Görling, 2006), “ *This is not only a question of knowledge but of utilizing this knowledge to regulate behaviour and that the regulation of behaviour is dependent on many more aspects other than simply the amount of education we have given to user*”.

In the motivation of finding a solution, many different perspectives and prevention have already been devised. For example, education programs targeted for end-users on identifying phishing emails (Kumaraguru, Rhee, Acquisti, et al., 2007)

---

<sup>1</sup> The sign used to identify phishing email

(Sheng & Magnien, 2007) and enhancing software to distinguish between legitimate and illegitimate websites (Y. G. Kim et al., 2008). The challenge is still growing since users still fall prey to phishing emails (Jagatic et al., 2007), and perpetrators continue to find ways around these solutions. To find the best approach, different views or perspectives in studies known as *non-technical* has been explored.

Phishing is a semantic attack that uses an electronic communication channel to deliver contents in the user's spoken language and other languages to persuade users. The challenge for computers is that there is extreme difficulty in accurately understanding the natural semantic language. Therefore, in this case, only humans are able to understand the true meaning of the contents and decide the direction of action in the first place. It has been shown that people are able to detect deception using non-technical cues, and this vital role is usually based on individual characteristics such as experience, personality and culture, among others (Anderson, DePaulo, Ansfield, Tickle, & Green, 1999). Furthermore, the principle of deception is employed by phishing emails to lure users into erroneous conclusions. The study of deception or sources of vulnerability has become more relevant to date. These factors have not been thoroughly investigated with concerning the users' characteristics and behaviours at work that produces vulnerability in organisations in a real-life experiment without prior training.

Former research has indicated that depending on engineering alone is insufficient to address the critical challenges of IT security. To date, little work has been published on the human facet when performing the standard procedure of security check to protect themselves from various approaches such as phishing attacks (Alsharnouby, Alaca, & Chiasson, 2015)(Arachchilage & Cole, 2011)(Reeder

& Consolvo, 2015)(Liang & Xue, 2010). Therefore, this study will investigate the factors that may contribute to user vulnerability in detecting deceptive messages.

Previous research on phishing emails suggests that there may be a connection between users' characteristics and users' detection behaviour. (Wright, Chakraborty, Basoglu, & Marett, 2010a) in his qualitative research data, he found that most participants used non-technical means to evaluate the legitimacy of phishing emails. This refers to one finding where the participant did not respond to a phishing email that requested private information but responded to a request from a lecturer. Further investigation is required to study this connection.

A demographic study by (Sheng et al., 2010) shows an indirect relation between the victims of phishing emails and their susceptibility to phishing attacks. They conclude that gender and age strongly correlate with phishing susceptibility. (Kumaraguru, 2009) also found interesting demographic differences between users who were able to detect phishing emails (detector) and victims. Other studies investigated demographics in designing phishing emails (Jagatic et al., 2007). However, these studies did not focus on non-technical factors and failed to investigate users' detection ability and behaviour in response to phishing emails.

Culture is another potentially relevant factor to look to in more depth. This is because a study on detecting deception in different cultures via different mediums such as videos shows a high accuracy level compared to studies under poor mediums such as recordings. The poor medium here means communication through it can be misunderstood. It entirely depends on how the recipient interprets the content of the email. Furthermore, email is also lacking in true interactivity and unable to give an

immediate response when required. (Bond et al., 1990)(Paul T. Costa, McCrae, & Löckenhoff, 2019)

Since email is considered a poor medium, this may affect users' ability to detect deception across cultures. The discussion on the results from the effect of culture on detection ability is discussed in Chapter 2.

In the study of phishing emails, researchers should not neglect to investigate the behaviour of users themselves. Further research may help identify the characteristics of users that impact their ability to detect behaviour and the weaknesses in character that may contribute to the threats. Knowing the association of certain characteristics would help the management to identify vulnerable users and provide specific training to improve their defence against phishing attacks.

## **1.4 Research Question**

The following questions were formed to address the problems identified in the above discussion:

- a. What are the factors involved in the process of users' detection behaviour?

It is compulsory to know the differences between detectors and victims. This information will direct us to explain the different behavioural choice (ignore or respond) by comparing their respective detection behaviour. Many previous research lacks or cannot provide sufficient information since most of these research provide users with pre-knowledge about the attacks (for example, by giving them a few samples) before the real experiment was

conducted. Our study did not provide any pre-knowledge to ensure a real case of experimentation can be done with significant results.

- b. What are the Individual factors that influence users' intention towards phishing attacks?

This knowledge is important for the development of appropriate preventive strategies for attacks. Victims of phishing are those who respond to phishing emails. Our research suggests more than one phase (i.e. respond or not) is required to investigate the weaknesses in users that make them vulnerable. Furthermore, this can help us find the results whether victims share the same weaknesses or have different kinds of weaknesses.

If it is proven that victims have different weaknesses in different phases, this provides information that there is no "one-size-fits-all" preventative strategy. For example, many education or awareness programs have successfully improved users' capability to detect phishing emails. Yet, still, many reported cases coming from the victims have an awareness education background (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010) (Tschakert & Ngamsuriyaroj, 2019). For this reason, it is essential to know whether victims share a weakness or maybe have several weaknesses.

- c. Is there any relationship between users' demographics such as gender, age, education, email practice, level of awareness and the characteristics of users' with the susceptibility to a phishing email?

Helping organisations to reduce risks by identifying the source characteristics that influence email users to accept social engineering attacks

can be achieved through policymaking and good training programs (Shahbaznezhad, Kolini, & Rashidirad, 2020). However, knowing ways to tackle employees from different demographic backgrounds is still a challenge. Providing enough information to the management about their staff can help them be well prepared to increase awareness and, most importantly, help reduce costs from recurring inefficient programs.

## **1.5 Research Significance and Contribution**

As email threats increase every day and in multiple ways, the challenge to develop techniques against hackers are becoming more crucial, and so does the impact from the threats. This thesis aims to identify the weaknesses in users' detection ability when they receive a phishing email. Some reviews in literature show that previous research focused on whether users will respond to phishing emails and how users manage emails through behaviour modification (Jackson, Burgess, & Edwards, 2006)(Whittaker & Sidner, 1996). However, this approach is with the assumption that users want to, are willing to, and can also change their behaviour. Hence, this research will investigate the behaviour that contributes to users becoming victims or detectors.

This research is significant in a number of ways. First, understanding the cognition, attitudes, behavioural intentions, and compliance of individuals in response to attacks is the key element of information security. Threats from social engineering are relatively new to information technology; hence it still possesses significant security risks and is a challenge to control (Hadnagy, 2010)(Twitchell, 2006). To the best of the author's knowledge, this research is the first study that



conducted an experiment in a real environment in one of the government agencies and used their resources to explore the factors that influence users' susceptibility and response to phishing emails more realistic environment.

The significance of this study also lies in its attempt to solve a serious information security problem. The study setting also reflects a significant contribution as SNSs are now the most common source of engineering attacks (Chitrey, Singh, & Singh, 2012a)(Jagatic et al., 2007).

Adding to the above contribution and significance of study, the way this study investigated the impact of demographic variables on susceptibility to phishing emails is unique. This is because the study conducted on phishing attacks indicated that there is a relationship between falling victim to phishing emails and demographic variables such as age, gender, and educational level (Darwish, Zarka, & Aloul, 2012).

Furthermore, this research is of particular relevance to the knowledge of understanding the current attacks in phishing emails, and the findings also contribute to the knowledge of Social Engineering attacks on Social Networking Sites in general. Notwithstanding the importance of those solutions, this study focuses on the main and weakest chain, namely, the users. None of the social engineering-based attacks could succeed without users accepting, succumbing and performing the requested actions.

## 1.6 Study Design and Limitation

This study used an exploratory mixed-method approach starting with a quantitative phase followed by a qualitative phase. Using a mixed-method design ensures the validity and reliability of the study because of its ability to provide a comprehensive overview of the problem and eliminate bias and subjectivity interpretation; such bias from a qualitative study where the wrong interpretation from the researcher on important characteristics may be biased happen.

Quantitative data were collected on users' susceptibility (first phase in detection behaviour) to phishing emails, users' characteristics, and demographics. Quantitative data also used to collect data to measure relationships between all variables in the research. The experimental method used involved users in actual detection behaviour with phishing emails. The advantage of an experimental design is its emphasis on internal validity (Recker, 2013b). The aim of this study and the methodology used helped fill the gap in the information systems literature. Based on study from (Cao, Lowry, & Lowry, 2015) and (Osatuyi, Passerini, Ravarini, & Grandhi, 2018) we concluded that the future study in SNSs needs to focus on:

(1) SN- specific construct validation development; (2) individual characteristics or factors that play a role in SN; (3) multiple research methods, especially qualitative methods and data analytics; (4) multiple research contexts such as different platforms, industries, and cultures; and (5) different types of use, long-term use, and changing social networks

Human cognition draws a close relation between people and their knowledge from experience in using emails such as personal interaction, membership to groups

or forums, and relationships between interest and concern. Therefore, choosing the correct measurement is required to investigate the whole process of detection behaviour. Previous studies like (Vacca, Jakobsson, & Tsow, 2013) (Kumaraguru, Rhee, Acquisti, et al., 2007) chose phishing emails based on images and record detection after receiving the phishing email failed to investigate all detection behaviour involved in decision-making about phishing emails.

Studies on phishing emails using images or sample emails have several limitations. The studies invoke users directly about what they see and may initiate the detection process (Jakobsson, 2007). This technique is believed to involve judging capability based on users' experience alone. Some users may not get this far, and variations in the emails can reflect their response (Gordon et al., 2019).

Another limitation reported is from the actions that users have to choose their response (Downs et al., 2007). This is unlike a real-life situation where users can respond immediately or later because some users may wait for the requests (Wright et al., 2010a). Therefore, it is not suitable to conclude user final behaviour (respond or ignore) by using these studies.

## Chapter 2 Literature Review

Phishing is synonymous with cybercrimes that affect many online transactions and is increasing in frequency over time. It affects electronic commerce by causing online customers to lose their trust in online transactions and leads to severe issues that are constantly discussed nowadays at most of Internet security conferences worldwide due to the huge impact on economic growth.

Phishing that affects online transactions is primarily due to an open network that is exposed to the unsecured World Wide Web. For example, Google bots uncover 9500 new malicious web pages every day (Nguyen & Nguyen, 2016). It is often unnoticed where tracing and prevention are almost tricky. In general, phishing is used to collect information on users' private data and manipulating the data to become valuable information for hackers, such as usernames and passwords (Polakis, Kontaxis, & Antonatos, 2010). Based on a Microsoft Security Intelligence Report in 2018, 53% of phishing attacks targeted SNSs users (Lume, 2018). (Jagatic et al., 2007)(Vishwanath, 2015) claimed that SNSs could easily and effectively attract victims to respond to phishing links developed by the attackers.

The main objective of phishing is identity theft. The first phishing activity was in 1996 when thousands of America Online (AOL) accounts were stolen using emails as a "hook" to steal passwords from AOL users. Microsoft defines phishing as the following,

*“A type of deception that is designed to steal your identity. Phishing scams will try to get you to disclose valuable personal data - like credit card numbers, passwords and account data by convincing you to provide it under false pretences. Phishing schemes can be carried out in person or over the phone and delivered through spam e-mails or pop-up windows”.*

The flow and information to illustrate a phishing attack are shown in Figure 3 below:

- A user receives a deceptive message from the phisher.
- The user responds to the email by revealing their confidential information.
- The phisher obtains confidential information from the server.
- The information is used to impersonate the user.
- The phisher gains access online and attempts fraud.

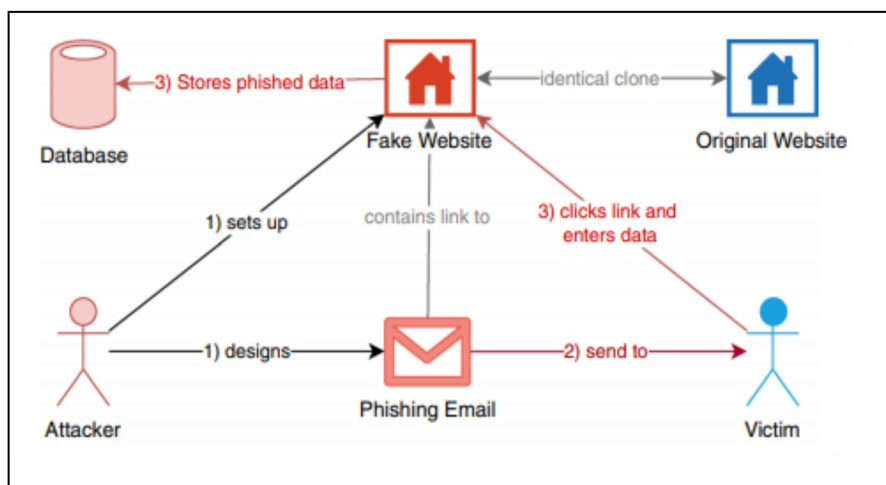


Figure 3: Email-based phishing attack (Jampen, Gür, Sutter, & Tellenbach, 2020)

## **2.1 The Evolution of Phishing Attacks**

In June 2001, attackers started targeting payment systems on E-Gold. However, it was not successful, although it established a new target for phishers (Almomani, Gupta, Atawneh, Meulenberg, & Almomani, 2013). Then in 2003, phishers targeted more famous websites such as eBay and PayPal by using their new group domain. They tried to send spoof emails to PayPal customers with a fraudulent link embedded in the email body. When the user entered his/her information, the information will automatically be copied to the phishers' database and later used for illegal activities. Starting from that, phishing attacks achieved tremendous success year after year. These attacks reportedly cause a loss of billions of dollars of customers' money a year (Khonji, Iraqi, & Jones, 2013).

The popularity of Voice over Internet Protocol (VoIP) around the year 2006 provided opportunities for phishers to spread their attacks called Vishing (Voice Phishing) (Castiglione, De Prisco, & De Santis, 2009). With the vishing technique, phishers will set up a voice system using VoIP in the first stage. Then the phishers will use an automatic dialer to call the victims in their list and play the recorded message. The recorded message will ask the customers to call a phone number provided in the message and update their personal information.

There was less success in vishing or over the phone phishing; hence phishers returned to email phishing. Phishers created a new kind of attack launched in late 2007, called spear phishing (Krombholz, Hobel, Huber, & Weippl, 2015). This type of innovation was known as the most successful trick and had a high success rate because it was a targeted phishing attack. Rather than sending phishing emails to just anyone, the phisher sent spoof emails to targeted customers or consumers by

pretending it came from a known sender. This technique was extended dramatically between the year 2009 to 2011, and it has claimed responsibility for a data breach of high profile cooperate data (Caputo, Pfleeger, Freeman, & Johnson, 2014).

In summary, until now, phishers are still improving their tactics by using new techniques, targeting specific groups and channels, and have not failed even with many research done on preventing attacks and defending data. Defending phisher attacks have been studied since the first attack. Many technical solutions like phishing detection tools, phishing prevention tools or correction techniques (Khonji et al., 2013) have been developed. However, none of these could guarantee a hundred per cent success in prevention if the users still ‘open the gate’ to the attacks. Besides awareness programs that have become compulsory for many organizations, human behaviour when dealing with attacks is the focus. Therefore, the present research focuses on non-technical solutions. This is the leading role that makes most of the attacks successful. If technology fails to fully defend the attacks, people should act smarter on making decisions as an optional defence aid.

## **2.2 Types of Attack**

It is impossible to list or predict all the types of attacks associated to phishing, however, we will explain the most common attacks such as social engineering-related attack which is the most used and popular in phishing at the time of writing. Moreover, this type of attack uses less technical skills than Technical Subterfuge categories that require certain tools or experts to complete the mission.

## 2.2.1 Social engineering attacks

Social engineering attacks are acts to influence others in order to gain information from them or to persuade them to perform an action that will benefit the attacker in some way (Hadnagy, 2010)(Thornburgh, 2005)(Workman, 2008). Therefore, it is a quite complicated and broad concept in the virtual environment of SNSs because it involves understanding and controlling social engineering threats that arise from different research backgrounds such as information technology, sociology, psychology, behaviourism, marketing, and human communication. Spear phishing is a popular social engineering attack and is generally known as “phishing” only. Regardless of what it is called, the objective is always the same which is “to direct users to comply with attackers’ request”. The following are a few types of attacks that fall under social engineering attacks:

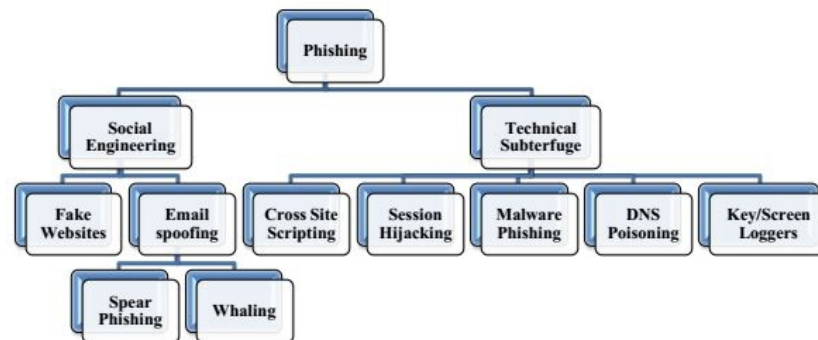


Figure 4: Classification of phishing attacks based on types of fraud (B. B. Gupta, Arachchilage, & Psannis, 2017)

- Clickjacking – The clickjacking technique tricks users into clicking on an object that may harm the users’ system. The object is normally embedded with a hyperlink containing a malicious program that will give the attackers full access to the system. The objects are normally in different types such as



videos, photos, links and attachments (Coronges et al., 2012). An example of this type of attack is the “Please update your profile here” or “Don’t Click” trick, where the attacker creates a link that contains a masked URL. Once the victims click on the message, the malicious program will spread automatically into the victims’ computer system and open the systems to be manipulated by the attackers (Robert McMillan, 2009).

- Farcin – Farcin is the type of phishing where the attackers use a phoney SNS profile to befriend the victims before they can spy or solicit personal information directly from them (Vishwanath, 2015).
- Spear Phishing - Spear phishing is a famous attack that targets specific receivers, usually executives and high profile executives who have access to company data and corporate credentials. They use spoof emails with the primary objective of obtaining control of the entire organization by using an authenticated identity.
- Identity theft – This type of phishing involves stealing personal information on credit card details, social security number, identity card number, and date of birth for financial or masquerade identity, which is then used in some purpose such as online ordering products from the Internet or money transfer. Users who are willing to share critical information with other people such as health information (Mao, Shuai, & Kapadia, 2011)(Torabi & Beznosov, 2013) and location (Cheng, Caverlee, & Lee, 2010)(Humphreys, Gill, & Krishnamurthy, 2010) are identified as possible victims.
- Spamming - Spam emails are defined as electronic messages sent to users who are either ‘targeted’ or at random with the specific objective in the form

of advertisements or profits. The objective of spam email is to transform them into phishing emails that seek users' confidential data and access their bank accounts with the purpose of financial fraud. Attackers may direct the user to a phishing website by attaching a link in the email. Some emails may contain attachment-based spam and phishing content that enables them to pass through spam filters by designing imitation emails that look like real emails. Besides their content (design of email body), the attachments and words used to contain a de-obfuscation technique that may also fool the spam filter.

- Reverse Attack – In a reverse attack, the attacker does not need to make contact with the victims. Rather, the social engineer will trick the victims to make contact with them. Here, trust plays an important role where extreme trust with the attacker will give the opportunity for the attacker to ask the victim to reveal their information (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011).

### **2.3 Influence of spam/ phishing attacks**

Spear phishing attacks are the new and popular attacks that target executives and higher officials who have access to company data and corporate credentials. Spoof emails are sent with the primary objective to obtain confidential data and take control of the entire organization by using authenticated identities. The report from Trend Micro Midyear 2017 (TrendLabs, 2017) states that 38 billion threats were found using spam email as a propagation method. From this number, emails with attachments are still the best technique used by the attackers to create cyber propaganda which threatens targeted enterprises. Spam without attachments,

including messages that have been embedded with malicious links, can be classified as commercial, medical, insurance and scam spam.

Spear phishing emails trick users by sending fake emails asking for confidential information without showing any suspicious entities. Through their fine design, the attackers impersonate legitimate organisations to persuade users to comply with their request. This type of attacks mostly relies on the users' ability to distinguish between legitimate and imitation emails. Unaware users will easily fall victim and give the attackers the chance to pursue their objectives.

RSA in 2017 revealed that the total number of phishing attacks in the global market is 123,929 cases. From the report, Canada endured the largest attack distribution with 56% compared to the United States in second place with only 10%. However, the United States led for countries that host phishing emails with 51%.

## **2.4 Email**

Over the years, email has become a popular communication medium over the Internet. The fast acceptance and popularity of emails are supported by its features on supporting many communication services such as document attachments, embedded links, design, ease of use, and protocol. The volume of emails received and created everyday are numbered in billions worldwide. This is similar to the growth of the number of new registered users. Estimated email accounts worldwide is expected to grow 6% annually over the next four years, with 3.9 billion accounts in 2013 to over 4.9 billion accounts by the end of 2017.

Meanwhile, the total number of daily business and customer e-mails was expected to exceed 319.6 billion in 2021 (S Radicati & Hoang, 2017).In most online

registrations, the compulsory email field shows that every user who wants to use and deal with the Internet must have an email address. This is the biggest contribution to the reason of email growth.

## **2.4.1 Phishing Email features**

Phishing emails are employed to make the design appear credible, and we have used this design in our own phishing email experiment (see Section 4). The discussion below is discussed based on two main studies (Akbar, 2014)(Wang, Chen, Herath, & Rao, 2009) to examine these techniques.

### **2.4.1.1 Email Design**

As mentioned earlier, phishers will employ various techniques to trick victims to access their fraudulent websites. One of the popular ways is by sending illicit emails but claiming as from legitimate institutions. The email content will usually imitate the official look of an actual website with the logo, wording structure, and often forged email headers.

These techniques are explained by the experiment done by (Wang et al., 2009) when he analysed 195 phishing emails using the elaboration likelihood model (ELM)(Petty & Cacioppo, 1986). The finding shows that phishing emails are well designed to reduce suspicion.

For example, the ELM proposes that the quality of the message will influence the users' acceptance of the email. Quality here means the argument used in the email design that is able to convince users (Bhattacharjee & Sanford, 2006). This

feature is important for a phishing attack to succeed. For example, the content of the email is to

inform that a certain amount has been debited into the user's account and request the user to confirm for the transaction to be made urgently; otherwise, the account will be suspended. Figures 5a and b below show an example of an email created by phishers when they attacked Malaysian National Bank customers. They used the ELM technique to alleviate suspicion from the customer's view.

```
-----Original Message-----  
From: Bank Negara [mailto:tonya.r.durant@vanderbilt.edu]  
Sent: 10 October, 2016 9:31 AM  
To: Undisclosed recipients:  
Subject: Important notice - Incoming funds on hold  
  
Important message regarding an incoming payment to your account.  
  
Download the attachment to view details.  
  
Thank you  
Bank Negara Malaysia
```

a.

```
From: Bank Negara Malaysia  
To: Undisclosed, recipients:  
Subject: Incoming payment (Action Required)  
Attachment: BNMNOTICE.pdf, 146.6 KBytes  
  
You have a credit instruction for an incoming payment. As our security precaution, all payments above Ten Thousand Ringitt (RM 10,000), require extra verification from Bank Negara Malaysia.  
  
Kindly download the attachment to complete the verification and receive this payment.  
  
Thank you  
Bank Negara Malaysia
```

b.

Figure 5(a), (b): Examples of Malaysian National Bank phishing emails

The attacker is smart enough to design a phishing email in order to increase user acceptance. (Wang et al., 2009) identified four key design features that are used to meet the objectives, as shown in Table 1.

*Email Title/Generic greeting:* Phishing emails are generalized such as “Dear User” or “Dear Customer”. An interactive title increases users’ motivation to read and open the email. In psychology, motivation is defined as a “state or condition where can be described as a need, desire or want that giving direction to behaviour” (Kleinginna & Kleinginna, 1981).

Table 1: Key design features

Dimension	Features
Title	Impact, company name, urgency
Message appearance	Authentic looking email sender, email signatory, personalization, media type, typo, third party icon for trustworthiness, copyright, company logo
Email content quality	Event, impact, urgent, courtesy, justification, response action requested, penalty
Assurance mechanism	Third-party icon for assurance, Anti-fraud/privacy statement, SSL Padlock, general security lock, Help link/feedback, mechanisms, authentication, HTTP link

*Email body:* The body of email consists of an argument that expresses a sense of urgency and offers a valuable proposition forcing the users to take further action. The strength of the argument shows the quality of the argument (Bhattacharjee & Sanford, 2006) . In ELM, this will become the central route of the decision-making

process. If users agree and accept the arguments, they will comply with the request and response.

*Message Design:* Most phishing emails use a valid looking design such as logo and copyright information to increase message credibility. In ELM, this will fall under the peripheral route of decision making (Petty & Cacioppo, 1986). A misjudgement in the appearance of the message is the main reason users fall victim to the peripheral route (Dhamija, Tygar, & Hearst, 2006).

*Assurance Mechanisms:* Phishers try to gain as much trust from the recipients by assuring that the transaction is secure. Phishers use the TRUSTe symbol to spoof users and they may use Secure Socket Layer (SSL) by using the https protocol. (Grazioli, 2004) suggest that users who take action based on their judgement on the assurance cues are vulnerable and at high risk of becoming victims.

## **2.4.2 Persuasion techniques**

(Akbar, 2014) studied over 400 suspected phishing emails in English. Categorical analysis and semantic network analysis were used to investigate how these emails were able to persuade the victims. The study was to find the dimension that was most influential in the persuasive technique credibility. In her study, she identified three characteristics in emails that are able to show the persuasion technique:

- 1) Authority of the email or source of credibility - Source of credibility is the most popular persuasion technique regardless of their target and reason. It refers to the message which appears to come from the inside or a trusted organisation. Emails that come from an organisation domain, a legitimate

sender and clear specific sender are most trustworthy. It can appear to engender fear, where users must obey to the command to avoid negative consequences such as losing privileged company data, punishment, humiliation or will be charged for legal action.

- 2) Scarcity, consistency and likeability or message credibility – This refers to the appearance of the message. (Sharma, 2010) identified three categories of message appeals (rational, emotional and motivational) of the message.
  - a. Rational appeals use formal logic rules as a persuasive technique. The importance of rational appeals in design is supported by (Wang et al., 2009) where he said that phishing emails always present a justification in the action (see Figure 2.2).
  - b. Emotional appeal refers to an “inside “message argument that focuses on users’ emotions. According to (Witte, 1992), users who have negative emotions such as fear, anxiety and distress have been found the most fragile and easy to respond to phishing emails.
  - c. Motivational appeal refers to a message that targets users’ perceived needs (Seiter & Gass, 2007). People are easily motivated to achieve certain needs and dreams when it comes to psychological, safety, belongingness/love, self-esteem and self-actualisation (A. Maslow, 1943)(A. H. Maslow, 1969)(A. H. Maslow, 1954). This opens the opportunity for phishing emails to exploit users’ need for safety by suggesting extra protection to their saving accounts as cyber threats have attacked the bank; thus, creating fear for the loss of savings.



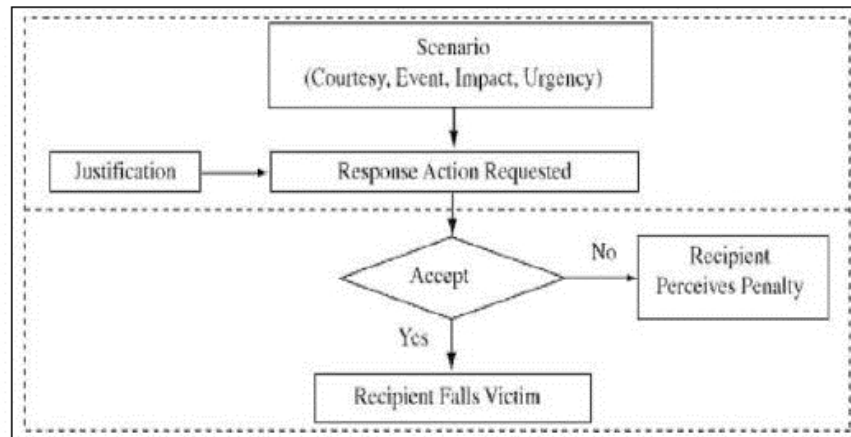


Figure 6: Quality measurement framework (Wang et al., 2009)

3) Account related concerns – The use of account related reasons with the current situation is the most popular technique to persuade users. This is similar to the above-mentioned message credibility but normally more generalized and not specific. For example, emails regarding a data breach on PayPal accounts was sent to everyone. Those who are related may be fearful of the issue but those who do not have an account with PayPal will easily notice the strange event. The message structure elements in persuasive message are shown in Table 2.

Table 2: Message structure (Sharma, 2010)

Index		Frequency	Percentage
Message	Explicit	136	90.67
	Implicit	14	9.33
Repetition	Repetition	50	33.33
	No.-Repetition	100	66.67
Order	Climax	150	100

In comparison among the types of message structure in Table 2 above, explicit message has been found to be more persuasive than implicit message (Perloff, 1993)(Trenholm, 1989). However, repetition message has a negative impact on users' attention and interest which contradicts to a less repetitive message with a positive impact (Trenholm, 1989)(Dillard & Pfau, 2002). A message is more persuasive when it has a strong argument in it (Seiter & Gass, 2007). Also, the length of message plays a role in the persuasive technique and success rate (Robert H. Gass & Seiter, 2015).

The following section will discuss the decision making process that has been studied from the view of phishing emails.

## **2.5 Decision Making**

It is our concern to identify the weaknesses in users' decision making that leads them to respond to phishing emails. Their judgement towards phishing emails is a part of the cognitive process for their subsequent actions. We examined a few main decision-making models, namely the model of detecting deception (MDD), Elaboration Likelihood Model (ELM), and the theory of acceptance model (TAM). These examples were selected because they can help us identify the area of weaknesses in users' decision-making regarding a phishing email.

### **2.5.1 The model of detecting deception (MDD)**

According to the theory of deception, detection is a cognitive process which involves examining different cues (e.g., words, tone with body language)(P. E. Johnson, Grazioli, & Jamal, 1993)(P. E. Johnson, Grazioli, Jamal, & Zualkernan,

1992). In the early age of deception study, the theory was applied to a high rich medium (face-to-face) where the medium can provide much information that guides the detectors to identify deception. Some of the information provided are the intonation of voice and face expression. Besides that, is about two-way conversation action. When it comes to a computer-based environment, a two-way communication only happens when people make a video conference. However, video conferencing quality is still less than real-time conversation, especially in detecting gestures and tone due to signal delay. Other than that, another challenge in a computer-based environment that is concerning is one-way communication such as using email. This type of conversation is not like a face-to-face environment where a user can ask questions and observe the real-time response. A one-way communication requires a user to make a decision based on the available information that they receive in the form of a message.

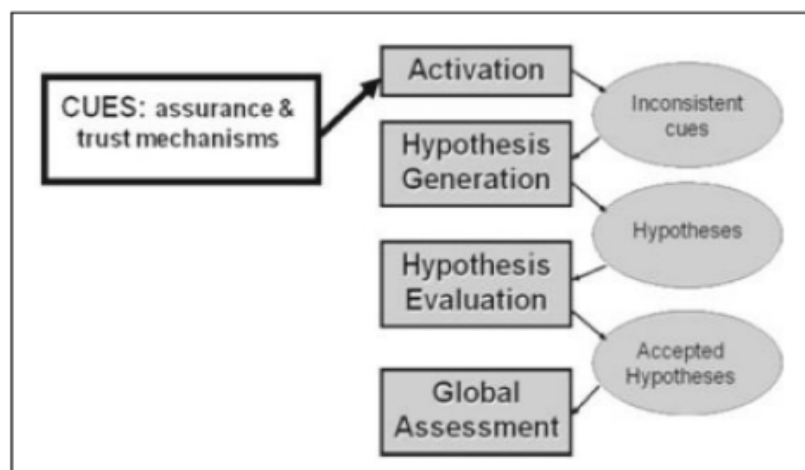


Figure 7: Model of detecting deception by (Grazioli, 2004)

Based on the MDD model introduced by Grazioli above (figure 7), the phases involved in decision making consist of four main phases: activation, hypothesis

generation, hypothesis evaluation, and global assessment. The details for each phase are as below.

*Activation* – the beginning of the process where users observe the inconsistency cues.

*Hypothesis generation* – developing an explanation for the difference between expectation and observation.

*Hypothesis Evaluation* - employ different evaluation methods.

*Global assessment* – the last stage where the evaluated hypotheses are summarized, and a decision should be made followed by the action to be considered.

Grazioli in his work (Grazioli, 2004) advised that hypothesis generation and evaluation should necessarily be a one-time process. This gives the user a chance to make as much as hypotheses and evaluation. However, only one result should be produced for each of the hypotheses before the conclusion can be made at the final stage.

Most importantly, according to him, the detectors and victims that went through the four phases of the model of detecting deception does not always guarantee that they will be a detector. Only detectors are able to detect deception while victims are always those who failed to detect it .

In our research, the MDD model was used to study users' detection behaviour when faced with phishing emails. Furthermore, in a study done by (Wright et al., 2010a), two additional factors were found to be responsible for activating users' suspicion in the early phase of MDD (see Figure 8). These factors are priming and individual factors. Priming is defined as a cognitive structure of mind that is developed by the experience it has found.

Based on the study by (Higgins & Kruglanski, 1996), training in the priming phase produces different results on users' response to phishing emails. Some of the users are able to change from victims to detectors while some remain as victims. The strongest explanation for the situation is the individual factors that make them detectors or victims, and these factors should be investigated and identified in order to reduce the number of victims.

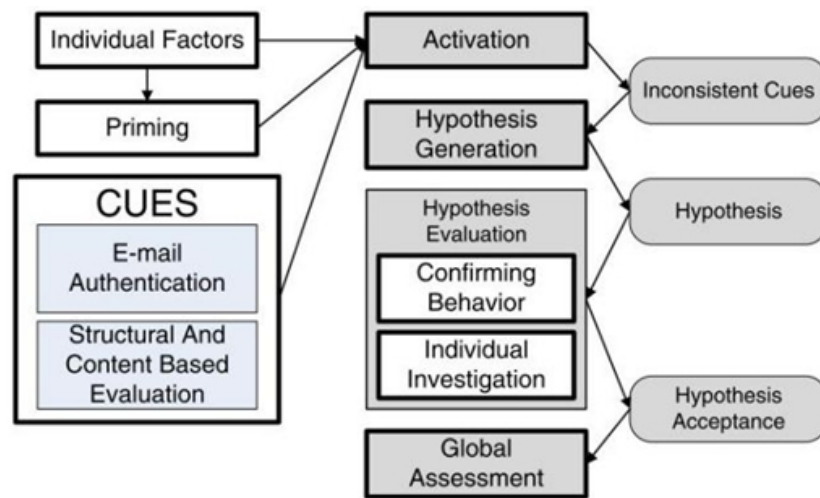


Figure 8: MDD model by (Wright, Chakraborty, Basoglu, & Marett, 2010b)

Based on the MDD cognitive process, we extracted the detection behaviour into two phases; susceptibility and response. Susceptibility is the first phase in the users' detection behaviour. In this phase, the users will decide upon their intended behaviour for the suspecting phishing email.

Response is the last phase in the users' detection behaviour. In this stage, the user's final decision whether to respond to the attacker's need or to ignore is important in order to categorise them as a victim or detector. Victims are those who respond to the phishing email.

## 2.5.2 The Decision-Making Model

Cognition is defined as the act or process of knowing, which includes both awareness and judgement (Morgan, 1979). The decision making model by (Dong, Clark, & Jacob, 2008) was developed to explain the cognitive process in relation to phishing emails (See Figure 9). Two of the main features in the model, which are the type of selected cues and interpretation of the cues were used to identify the main area of the users' decision weaknesses. For example, an email that contains a well-known bank logo. The user might think that the content of the email is legitimate without knowing that the logo is simulated. This drives the user to give wrong cues in judging the email. Another type of area is the incorrect interpretation of cues; for the same example, the user may interpret the email request from the bank as correct and assume that it is a normal bank procedure.

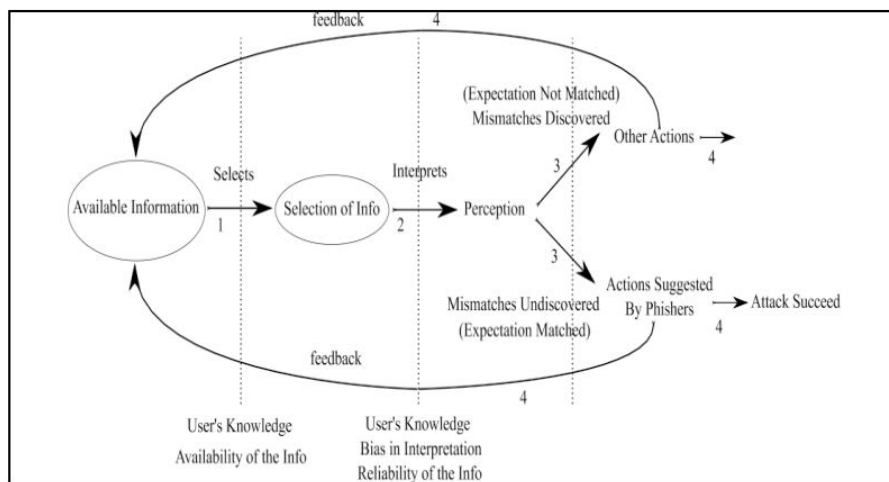


Figure 9: Differences between detectors and victims (Grazioli, 2004)

### **2.5.3 The Elaboration Likelihood Model (ELM)**

A study done by (Pfeiffer, Theuerling, & Kauer, 2013b) showed that users pay more attention to the content of an email compared to metadata such as “From” email address. On the other hand, (Aburrous, Hossain, Dahal, & Thabtah, 2010a) found that some users ignore the phishing email cues but enjoy judging based on the attractive appearance of the email such as colours, animation and image. ELM proposes that users process messages using two routes: the central route and the peripheral route (Petty & Cacioppo, 1986). If the message is processed using the appearance like the given example, it is called the peripheral route process. However, if the message is processed using the argument it contains and the instructions (cognitive processing), the process is called the central route processing. As a result, users who rely more on the design and appearance of a message are more vulnerable because phishing emails are normally designed in interactive ways.

From these three cognitive process models explained, we narrowed down the effectiveness of the models into the users’ judgement of the legitimacy of phishing emails. It is suitable with the aim of the study to “understand users’ detection behaviour phase” which is the main objective. Therefore, the MDD model is the most suitable and appropriate for the study. The difference between the MDD model and the two other models is the ability of the MDD model to explain the cognitive process outside the design features of phishing emails. The weakness of ELM and the decision-making model is that they are only able to explain the cognitive process based on the design features of phishing emails. For example, ELM explains the detection based on users examination of the emails. The judgement is based on what the user is able to see on the email including its argument quality. The decision-

making model, however, depends on the cue selection and cues interpretation of the design features. Both of these models were unable to help the research in relation to identifying users' behaviour.

## 2.6 Detector and Victim Cognitive Process

Before further studying the users' behaviour, we identified the foundation factors behind the behaviour. Many studies on identifying the difference between detectors and victims show significant differences between both. Based on our anchor reference study (Grazioli, 2004), the differences can be identified in two main cognitive phases; namely the evaluation and global assessment phases (See Table 3). Also, the study found that a detector is able to use different cues in evaluating the hypotheses and judge the legitimacy of the websites. However, it does not mention "what" factors make detectors better in evaluating the hypotheses and "why" they used different cues on judgement.

Table 3: Differences between detectors and victims

<b>MDD</b>	<b>Detectors</b>	<b>Victims</b>
Activation	Inconsistence cues	Inconsistence cues
Hypothesis generation	Priming <sup>2</sup> not significant	Priming is significant
Hypothesis evaluation	Competence at evaluation	Incapable of evaluation
Global assessment	Assurance cues	Trust cues

In 2010, (Wright et al., 2010a) Wright updated Grazioli's MDD model to investigate the impact of individual user characteristics on detection behaviour. They managed to interview only detectors to identify the factors that helped them detect

---

<sup>2</sup> Priming is a way of warning users about deceptive behaviour.



phishing emails, although no victims were included in the interview which made the comparison between detectors and victims impossible. Our research, however, managed to fill the gap by conducting the interview with the victims in order to further understand why they respond to phishing emails. Based on Figure 8, priming and cues were added because it was found to increase the awareness about deception that can be used to warn a user about possible deceptive behaviour. It is also well established in education and training materials to train the users to pay more attention in the field of phishing emails. However, individual factors lead the users to make wrong judgement and actions. Our research aims to fill the gap by investigating the impact of users' ignorance of themselves and organisations on each phase of detection behaviour.

In summary, users are a weakness in ability to identify phishing threats. The vulnerability should apply equally to phishing emails, which employ similar deceptive tactics. The attitude of users who rely on advanced technology alone to protect them does not show a reduced number of users who have fallen victim to phishing. The following section discusses and evaluates the existing countermeasures that are still in dilemma.

## **2.7 Current Countermeasure**

In recent years, the topic of social engineering attack has attracted many researchers. Many different types of countermeasures that are implemented at different levels have been investigated and highlighted associated with social engineering especially in SNSs (e.g., (Boorman et al., 2014)(Chitrey, Singh, & Singh, 2012b)(Dimension Research, 2011)(Fire, Goldschmidt, & Elovici, 2014b)(Position

& No, 2007)(Jagatic et al., 2007)(Krombholz et al., 2015)(Shariff & Zhang, 2014)). Many from those studies suggested that SNSs are the most common sources of social engineering attacks and most of the researchers tried to come up with solutions to overcome the problems. Figure 10 presents these solutions: spam detection, the detection of bot-operated accounts, cloned profile detection, the classification of profile owners' identities, and the detection of users' susceptibility.

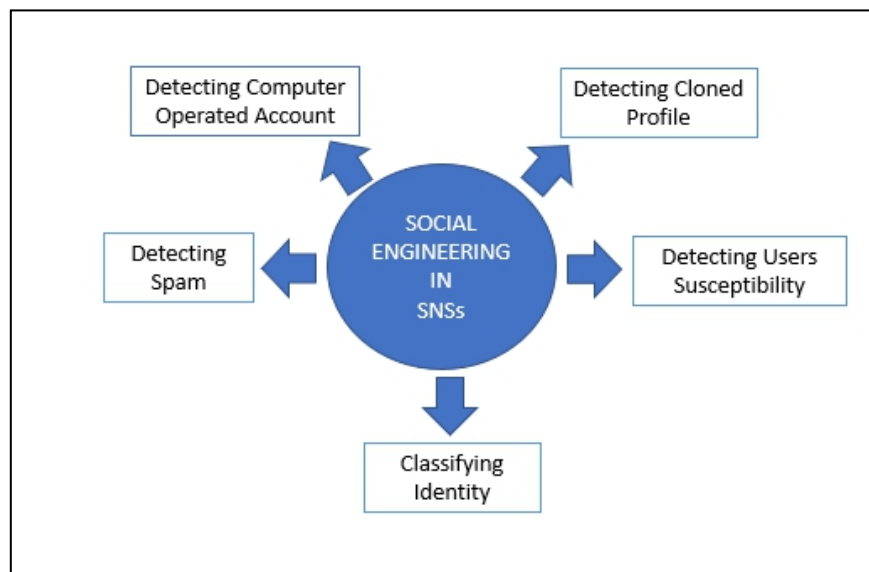


Figure 10: Proposed Solutions in the literature

Even though our study is only targeted to phishing emails, we took into consideration the preventions suggested to be applicable to all types of social network attacks including phishing emails.

### 2.7.1 Spam Detection

Spam detection is used as a solution to identify the legitimacy of the message. This solution relies mainly by comparing the similarity of the messages. Spamming messages are usually similar in their specifications. Based on a study by (Gao et al.,

2010) on spam messages, 70% of all malicious wall posts advertised phishing sites. (G. K. V. Stringhini, 2010), studied the characteristics of spam messages to detect them automatically. The findings showed that spamming messages were usually in the form of advertisements and contained URL links to particular websites. The low traffic spamming campaign was unable to capture more spamming messages compared to using greedy bots in this experiment.

(Rahman et al., 2012) also used the similarity features in order to detect spamming messages. They used the scoring technique to sum up the value for all messages with a similarity in URL link and computed the standard deviation for all posts. It seems to be the best solution than (G. K. V. Stringhini, 2010). Motivated from the success of the URL link in a spam attack, we included in our study an experiment with an email with a link that directed users to our experiment website. It is to test the vulnerability in user awareness and see users' cognitive ability to differentiate between legitimate and spam emails.

### **2.7.2 Detecting Computer Operated Accounts**

One of the solutions suggested is to detect whether the profile is operated by a human or computer (bots). Bots are known as “automatic or semi-automatic computer program that is able to mimic humans and/or human behaviour in online social networks” (Wagner, Mitter, Körner, & Strohmaier, 2012). In emails, this is normally done by email filtering that acts as the first line of defence against phishing email attacks. Email filtering acts in two ways; deletes identified phishing emails without user involvement or issue warnings to the users. The first type of detection uses a machine learning system that learns phishing emails features that can be adapted to recognise newly developed features. Additionally, email signatures have

been proposed to improve detection ability (Garfinkel, Margrave, Schiller, Nordlander, & Miller, 2005). Several researchers (Castillo, Mendoza, & Poblete, 2011)(Chu, Gianvecchio, Wang, & Jajodia, 2012)(Huber, Kowalski, Nohlberg, & Tjoa, 2009)(McCord & Chuah, 2011) (G. Stringhini, Kruegel, & Vigna, 2010) used content-based techniques in relation to spam detection to detect if the account operation is automated or human.

The second type of detection is designed to warn users about phishing emails. It cannot detect all forms of phishing emails; hence the final decision is still made by the users who may choose to ignore the warnings (Fette, Sadeh, & Tomasic, 2007a) (Maldonado & L'Huillier, 2013).

However, email filtering is unable to detect all types of phishing emails (Chandrasekaran, Narayanan, & Upadhyaya, 2006)(Maldonado & L'Huillier, 2013). The reason is that many phishing email designs are constantly created; thus frequently making updates on the email filter is a difficult option. In some situations, users really need to rely on their own ability to detect phishing emails when the email filter is out-of-date.

### **2.7.3 Detecting Cloned Profiles**

A few studies (Jin, Takabi, & Joshi, 2011)(Khayyambashi & Rizi, 2013)(Kontaxis, Polakis, Ioannidis, & Markatos, 2011) have proposed solutions based on the similarity principle. It starts by analysing and characterizing the behaviours of the identity clone attacks and proposing the framework of their analysis. (Kontaxis et al., 2011) proposed a prototype system that can help users in investigating or predicting their susceptibility to a cloning attack. The idea is to

identify the information which contains the users' profiles that identifies them. The results are able to show an acceptable level of efficiency.

(Conti, Poovendran, & Secchiero, 2012), Introduced a new model in an attempt to mitigate fake account attacks. Their model depends on temporal evolution that tries to characterise real user accounts, and the data are collected in need to identify a set of features in a dynamic mode of users. This profile is then studied with a particular profile under test that can detect any major deviation from the expected behaviour. The idea is to know whether the attacker is impersonating the victims on a particular SNS where the victim has no prior account in place. This technique frequently happens in a phishing attack where users sometimes receive emails from unknown organisations or business companies claiming to be the users' registered company and applicable to some membership benefits. For example, emails from a bank, Facebook or insurance company that they have never registered before. Users should always be aware of these tricks and should not simply reveal important information to the sender. At this point, cognitive ability plays an important role in the user's decision to avoid becoming a victim. The new idea in this model is that it does not rely on the similarity measurement between the profiles. Therefore it has become a challenge and limitation especially when it only relies on "trust" to the sender alone.

#### **2.7.4 Owners' Profiling Classification**

The owner classification technique is usually used to classify the identity (usually the gender). It is considered the best solution in helping to detect false information about users' profile. Many algorithms have been used to classify user profiles, some of them are stack-SVM-based algorithm (Rao, Yarowsky, Shreevats, & Gupta, 2010). Rao uses statistics on the users' account as well as the n-gram and

stylistic features. (Pennacchiotti & Popescu, 2011) Was studied on Twitter by using features that extract the content of users' profiles in order to find explicit links pointing to outside sources, content structure features, lexical features, and text content sentiment features. Another algorithm used is the Bayesian classifier by (Alowibdi, Buy, Yu, & Stenneth, 2014) that compares gender indicators obtained from different profile characteristics, including the user name and layout colours, using a weighted technique. In his approach, he used only a few hundred features compared to millions of features in (Zamal, Liu, & Ruths, 2012)(Liu & Ruths, 2013) (Rao et al., 2011) and(Burger, Henderson, Kim, & Zarrella, 2011).

In conclusion, the classification technique is valuable in dealing with social engineering, which involves detecting deception concerning identity, especially gender. However, it is still challenging to date, and there is no evidence showing it is an effective solution in combating social engineering attacks.

### **2.7.5 Detecting user susceptibility to Social Engineering Victimization**

All this while, the solutions involved with detecting social-engineering attacks such as spam/phishing emails and clone attacks were studied and researched through technical methods. Although these studies are valuable, social engineering attacks are still popular and attracts attention due to the success despite all the technical methods available today. This is because most of the research focused on the weaknesses of technology only and targeted less on the weaknesses of the users. None of the attacks are believed to be successful unless the users themselves accept,

succumb and perform the requested actions which finally harm them and benefit the attackers. Moreover, not all e-service providers are keen to employ an expert and buy expensive tools or software to protect users. When technical solutions fail, users are the last option of defence against threats. For this reason, in this research, we are trying to look further into user weaknesses behaviour that may contribute to susceptibility to phishing emails.

(Rashtian, Boshmaf, Jaferian, & Beznosov, 2014) Investigated the behaviour of friendship and relationship in social networks and found four factors that significantly impacted users' decision. The factors are knowing the requester in the real world, having common hobbies or interests, having mutual friends and closeness of mutual friends. The strength of the study is that it was done using exploratory qualitative research. This qualitative method is a new and useful virtual-oriented method in social network studies since it is able to give a significant difference between human behaviours in real life and virtual environment (Zinoviev & Duong, 2009).

The study that relates closely to susceptibility in social engineering victimisation is farcing done by (B. B. Gupta, Arachchilage, et al., 2017) . As discussed , farcing is a type of phishing attack where the attacker uses a phony profile to befriend with victims (Level 1 attack), and then solicit personal information directly from them (Level 2 attack). The experiment was done on undergraduate students and used an online survey that included their Facebook accounts. The researcher then created four fake profiles on Facebook using a factorial design, and friendship invitations were sent to the subjects. From the findings, the study suggested that those who fell victim was the one who relied primarily on the number of friends or the requester's picture in the fake profile

(Level 1). On the other hand, those who managed to receive (Level 2) the information request used the sender's picture in the message as a credibility cue. This study is among the first studies dedicated to susceptibility to deception in phishing attacks and was one of the strong experiments because it was performed using the actual Facebook environment. One of the limitations in the study is that the researcher used only one offer to trick the user ("offering internship") that might not impact users who were not interested in the incentive. The study also required the user to examine based on the profile picture only. The number of friends does not show the demographic diversity when the study only focused on undergraduate students.

Our study was inspired by the Vishwanath study. We note the impact of the limitation in the finding and enhanced our study with some additional strategies to overcome the limitation. Even though our focus on social engineering type of attack is different, the concept of phishing is still the same.

## **2.8 Gaps in Users' Detection Behaviour studies**

We summarise the gap in users' detection behaviour in this topic. We found many studies (as previously discussed) concerning users' behaviour in response to social engineering attacks, but not many of them thoroughly investigated the context of phishing emails.

The design features of phishing emails make the emails credible and easily mimic legitimate organisations to make users believe the originality of the email (Wang et al., 2009). (Chandrasekaran et al., 2006)(Cook, Gurbani, & Daniluk, 2008) and (Fette et al., 2007a) designed security tools that try to be the solution to draw



users' attention to phishing email cues such as using IP addresses or unmatched URLs. Even though these tools were used to warn users about the threats, some of the users still ignored the warnings because it was presented technically that many users hardly understood, especially for non-technical users (Dhamija et al., 2006)(Wu, Miller, & Little, 2006). This shows that usability is an important issue in presenting warnings (Herley, 2009) and users' detection behaviour are different between different types of phishing emails. This suggests that users' ability to detect is the result from the interaction between the users themselves and the type of phishing email they receive.

Some other studies showed the relationship between demographics and the response to phishing emails but failed to thoroughly show the findings. For example, the study done by (Kumaraguru et al., 2009) reported no significant difference between inexperienced users to phishing emails with those exposed to phishing emails after 28 days of the experiment. However, after they conducted the same experiment with a different culture group of users, they found a significant difference between experienced and inexperienced users. This suggests that users' demographics, especially cultural differences, can show the ability to detect phishing emails. However, the researcher did not compare the results between both studies.

Users who fall victim to phishing emails are those who treat warnings as less important and easily ignore it even though the security indicators show hints to the user (Stebila, 2010). This shows that the user characteristics have an impact on the users' ability to detect phishing emails. Besides ignoring behaviour on the cues given, users' awareness is also another important factor (Aburrous et al., 2010a). Hence, the warning indicators are not effective in preventing the users from becoming victims;

the users' themselves should be aware of how to detect phishing emails and be up-to-date on these attacks.

## **2.9 Variables used in User Detection**

On the organisation level, the findings by (Kvedar, Nettis, & P Fulton, 2010) suggest that social engineering attacks can be successful even from inside organisations, although they believe themselves as being aware of the attack techniques. (Marett, Biro, & Knodel, 2010) explained why people are weak and perform poorly in detecting deception because of "bias", where it is assumed that most people are telling the truth. Users' characteristic is the main issue in many studies related to user awareness, as is for our study on the detection capability of phishing emails. Some of the variables in deception have been investigated in relation to phishing emails, while other variables that affect users' ability have not been thoroughly investigated. Furthermore, some studies showed inconsistencies in the results and were unable to give a concrete measurement of finding. The present study tried to address these limitations.

Users can be differentiated by their characteristics and this is also the factor that is able to distinguish between detector and victim in phishing. This research focused on highlighting the characteristics that make users vulnerable to phishing attacks. This will act as an aid to organisations to increase their protection by understanding their employees and reducing their chances of becoming victims. The characteristics that have been chosen in our investigation are personality, culture and experience.

### 2.9.1 Cultural

Culture may play a role in differentiating detectors and victims. Phishing attacks are mainly based on email and uses a complex medium in their deception practice. In an organisation the employee may come from different cultures and backgrounds. Even though the companies are in the same country and are expected to have the same culture, previous studies showed the importance of the cultural factor as a variable in users behaviour. Below is the table showing the criteria study by (Baoshan & Dongming, 2009)(Douglas, 1978)(Furner & George, 2009)(Dow, 1988)(John & Srivastava, 1999). They involved the cultural factor in their study and the definition are as below:

*Individualism*: Degree to which the society reinforces individual vs. collective achievement and interpersonal relationships.

*Masculinity*: Degree to which the society reinforces or does not reinforce male achievement, control and power.

*Uncertainty avoidance*: Level of tolerance for uncertainty and ambiguity within the society.

*Conceptual Style*: Patterns that effect how people identify, recognize, and react to events.

*Self concept*: Effect of culture on how people perceive, define, portray, value and view themselves, including self-esteem.

*Ethics and Constraints:* Moral distinction between good and evil; in extent to which moral behaviour is governed by guilt, shame, saving vs losing and probability of being caught.

## **2.9.2 Personality**

The study that is able to show the correlation between users' personalities and their success in detecting phishing email was first done by (Wright et al., 2010a) based on interviews with detectors. The personality variables identified in the study were sensitivity towards the information value, concern for privacy and security, obedience to instruction, and the Big Five personality domains.

Another study in commerce also found that users were able to show high levels of concern about the privacy of information, but this did not stop them from giving their information when short term benefits were presented (Acquisti & Grossklags, 2005). This shows that concerns about privacy may increase users' suspicions and may lead them to activate MDD; however, this does not mean that users will be aware of attacks and become a detector.

The Big Five personality dimensions are openness, extraversion, agreeableness, conscientiousness, and neuroticism. Based on the same study by Wright, detectors scored highly on conscientiousness compared to victims. The study has some limitations where they did not include all detectors where the detectors who did not inform their findings were excluded from the analysis.

The study from (Kumaraguru, Rhee, Acquisti, et al., 2007) used the Cognitive Reflection Test (CRT) to see how likely would users click on links from phishing emails that claimed to come from trusted companies even though the user

does not have an account with the company. Users with high CRT are ranked as more vulnerable with high potential to click on the link. Phishing emails are known to be very tricky and are able to deceive users by implementing different techniques such as camouflage email to appear as legitimate emails.

While the recent study by (Halevi, Memon, & Nov, 2015) certain personality traits (conscientiousness) and gender are able to influence a person to become susceptible to threats. Therefore, she suggests further study about the effect of personalities in dealing with online attacks.

The three studies above highlight the importance of personality study to defend users from being attacked.

## **2.10 Other Related Variables in Phishing Email Study**

### **2.10.1 Age**

Based on the study by (Dhamija et al., 2006)(Kumaraguru, Rhee, Acquisti, et al., 2007)(Sheng & Magnien, 2007), age was found as not having a significant effect but is able to show the ability in detecting phishing emails (Kumaraguru et al., 2009)(Sheng et al., 2010). It was also concluded that users aged 18-25 years were able to behave significantly different from older users, perhaps because they are the up-to-date generation and more of risk-takers.

### **2.10.2 Gender**

The studies in the relationship between gender and the capability of users detecting phishing emails showed that female users are more vulnerable than males

(Jagatic et al., 2007)(Kumaraguru et al., 2010). This also completes the fact that women have a more agreeableness personality that may affect their vulnerability (Costa Jr., Terracciano, & McCrae, 2001)

### **2.10.3 Education Level**

Studies by (Sheng & Magnien, 2007)(Dhamija et al., 2006) found that education level is not significant to differentiate factors in their vulnerability to phishing emails. However, the studies with pre-educational materials to the users were able to increase their ability to detect phishing emails (Bekkering, Ph, & Hutchison, 2009)(Kumaraguru et al., 2009). The ability to detect phishing emails with a pre- and post-test study can increase users' awareness, especially in increasing their knowledge about the bad consequences (Anandpara, Dingman, Liu, Roinestad, & Jakobsson, 2007) (Tschakert & Ngamsuriyaroj, 2019).

### **2.10.4 Internet Experience**

According to (Dhamija et al., 2006)(Kumaraguru et al., 2010), the number of years in using the Internet was not significant with detecting phishing emails. Internet usage varies between users. Some of them use the Internet for their work only but most use the Internet to play games, social network and online shopping. Even though users have experience with the Internet, not all of them are experienced with secure and sensitive transactions, such as transactions involving money and sensitive data transfer. In this situation, it is mostly related to conducting a study in relation to users' perceptions and behaviour towards the Internet. One study by (Kumaraguru, Rhee, Acquisti, et al., 2007) found an insignificant relationship between online shopping experience with detectors and victims.

## **2.10.5 Email Experience**

When it comes to email experience, most of the studies asked users about the number of emails they receive in a particular time frame (Kumaraguru, Rhee, Acquisti, et al., 2007)(Sheng et al., 2010). A phishing susceptibility study was able to find out that phishing knowledge plays an important role in users' ability to detect phishing emails. However, users are mostly unaware of the importance of knowing the criteria of email that is able to be spoofed and know how to evaluate them. Users may use email frequently, but this does not guarantee that they can be categorized as a detector at all times.

In summary, the problem in phishing emails has two dimensions, users and technology. The technological solution was developed to tackle the problem but only a few are from the users' perspective. Studies on users' characteristics that may impact their ability to detect phishing emails have not been thoroughly investigated in relation to their effect on detection behaviour and vulnerability, especially in the context of phishing emails. As a result, users must remain alert to threats and cannot always rely on current and available solutions.

Improving users' ability to detect phishing emails is believed to be the only way that may help to reduce the number of victims. Nevertheless, what will happen if the users still refuse to learn from the lesson and fail to detect phishing emails? Therefore, a better understanding of the users themselves is the best option to identify user detection behaviour's weaknesses. From the study, we can address the characteristics of the users that need to be focused on and use the findings to best prepare aid such as user training based on their character, a better employee selection filtering process, and technical solutions to help unidentified impaired users. All

these aids are used to enhance user detection capability and turn them to become detectors instead of victims.

## **2.11 Study Group Background**

There are two groups have been chosen in this study. One is a semi-government agency name, Majlis Amanah Rakyat (MARA). Another group is an open respondent, which we named a Public group.

### **2.11.1 The Role and Function Of MARA**

Majlis Amanah Rakyat (MARA), or the Council of People Trust, an agency under the Ministry of Rural Development's purview, was established on 1 March 1966 as a statutory body of the first Bumiputra Economic Congress resolution in 1965.

The council is responsible for developing, encouraging, facilitating and fostering the economic and social development in the federation, particularly in rural areas. The role has been to provide research and business loans to Malaysian students and entrepreneurs, respectively. They oversee the construction of infrastructures, such as factories and shop lots for Malay businesses. These facilities have often been constructed and rented out to Malay entrepreneurs at a subsidized rate to stimulate business growth and stimulate business growth in the Malaysian community. In the education sector, MARA has been granting scholarship to the Malay community since its inception in 1966 to increase the education level of Malays and close the income gap between the other races in Malaysia.



The success of the MARA agency in the two sectors, education and entrepreneurship, has been recognised by the Malaysia government. In 1968 MARA was assigned to involve in one more competitive sector for the Malaysian economy called Investment Sector. MARA Investment Sector was developed to establish equity ownership in the corporate sector and strengthen non-financial asset ownership. The objectives are to control, monitor and enhance Corporate Governance implementation, Commercial and Property Development of MARA investment and assets. This has awarded MARA as the biggest and most significant statutory bodies in Malaysia.

### **2.11.2 MARA as the Studied Agency for This Research Study**

MARA agency was chosen to be studied in this research due to its critical function in developing the Malaysian economy. The agency has changed the socio-economic landscape in Malaysian society. Since MARA has now more well known, there are a few reasons why the study must be done in the agency.

1. The MARA agency's success in all of its sectors makes them one of the agencies that received the government's biggest budget allocation every year. The traditional management control systems in data protection have been no more relevant to the digital era. With the advance, digital technology MARA is facing a challenge in improving their employee's competency level. As a statutory body, MARA must abide by the national employee act to continuously improve employee knowledge to support organisation change culture. It is not as simple as hiring a new employee with a relevant expert

background. Therefore, drastic and urgent change to the situation may be impossible in a critical case scenario, especially for certain departments where their workers' age is almost pensioner age. The increasing and profound change in digital threats have become a new concern for management in protecting their confidential information and data.

2. Many studies of MARA, focused on the management aspect (Ibrahim & Mustaffa, 2016)(R. D. Johnson, Marakas, & Palmer, 2006). However, none of them is related to the threat and security of MARA information and data. As far as my concern, this study will be the first study related to the MARA information security area that looks into the effectiveness of awareness training, age, and employee culture.
3. There is no official report from the newspaper about the attack that focuses on MARA agency. However, MARA IT department has come out with several warning emails recently mentioning serious SPAM and phishing attack at MARA email system. This can be seen in the screenshot of the email in Appendix C. It is shown that MARA nowadays requires more attention on their security implementation and employee to fight against the issue.

### **2.11.3 Public Group**

Many of the study related to phishing email are using University students as their participant. Therefore, our second group for the study comes from the email list from researcher email list in two different email accounts. The reasons for the selected group is.

1. To have a group of participants with different backgrounds, especially on the study scope's culture, knowledge, and training level.

2. To imitate a real-world scenario where not all hackers targeting business email and focus on stealing money. Some hacker hacks people just for fun, disrupting the network, spreading idealism and political agenda. So, this is typically happened to free emails service user.

## **Chapter 3 Research Model**

This chapter explains how the research model was developed. Theoretical perspective was used to examine user behaviour and its attributes. The research model and hypothesis are presented in this chapter.

### **3.1 Model Selection**

Technology acceptance in people is about adapting to technology in their daily lives (Louho, Kallioja, and Oittinen 2006). One technology's success or failure and its features can be viewed in terms of user engagement with the technology itself. Emails are known as a technology that is generally employed to increase user productivity and enhance communication, making them widely used nowadays. However, extensive use of this technology in everyday activities has also increased the abuse of the associated system (de Paula et al., 2005). As a result, researchers are interested in studying technology acceptance issues, focusing on individual user characteristics, such as cognitive style, internal beliefs, and their impact on usage behaviour (Dillon, 2001).

Education programs can increase users' knowledge of cyber threats, specifically in phishing emails, by increasing the rate of users becoming detectors by 40% (Kumaraguru et al., 2009). Significantly, some educational programs have been designed to observe the demographic differences in detectors and victims. However, the research still requires further exploration and study focusing on users'

perspective. Before discussing further, we will explain the leading theory used in our research.

We adapted the theory of deception with the theory of user acceptance in order to:

- i. Define the cognitive process between the deceiver (sender) and deceived (receiver); and
- ii. Study the main factors that support user behaviour that contribute to the cognitive process.

Besides these two theories, we also leveraged the Big-Five Framework, which is the most widely used model when the user's personality is the study's focus (Gosling, Rentfrow, & Swann, 2003). This model can represent the personality and classify the differences in the perception of individuals, which was used to help us support our empirical literature between types of individuals with their susceptibility to phishing attacks and provide structure for future research framework. We will hash out the details around these adapted theories throughout this chapter.

### **3.1.1 Theory of Deception**

In phishing, the hackers' technique is normally by luring the receiver to do the desired action(s) by manipulating the environment and encouraging the receiver to act to a false cognitive representation. This theory was developed in order to explain the deception concept in an information-intensive environment such as face-to-face communication (Grazioli & Wang, 2001)(Grazioli & Jarvenpaa, 2000).

Grazioli, in his work (Grazioli, 2004), applied the theory of deception in a computer-based environment and proposed the MDD (see Figure 8). A phishing environment requires a process that mainly involves a one-way communication where the deceiver sends an email. The user then makes a judgment followed by a conclusion based on the data in the electronic mail. This virtual office experience is more complex compared to a real-time environment where face-to-face interactions can give users a chance to observe the actual state of affairs and ask when in doubt.

Thus, to detect phishing emails, users who open a phishing email fall into two categories: detectors or victims. Detectors can detect the legitimacy of an email and decide not to respond to the email, while victims are unable to notice the reminders in the bogus email and comply with the action request from the email. Using the MDD theory leaves us to follow the behavioural process in detection; susceptibility and response.

### **3.1.1.1 Theory of Acceptance**

The success or failure of one technology can be viewed in terms of user engagement with technology use. In a similar vein, (Iahad & Rahim, 2012) characterize a technology's value by its adoption and uses.

Email is a technology that is broadly used to increase user productivity and enhance communication. Therefore, user acceptance of this technology is not doubted today. However, the extensive use of this technology in everyday activities has also increased the abuse of associated systems (de Paula et al., 2005). As a result, researchers interested in studying technology acceptance issues focus on individual user characteristics, such as cognitive style, internal beliefs, and their impact on

usage behaviour[3]. To achieve this objective, we designed the survey questions related to user acceptance of using email as the technology in action.

### **3.1.2 Unified Theories of Acceptance and Use of Technology Model (UTAUT)**

The Unified Theories of Acceptance and Use of Technology (UTAUT) model proposed by Venkatesh (Venkatesh, Morris, Davis, Davis, & Venkatesh, 2003) integrates eight elements from other prominent models; namely, Theory of Reasoned Action (TRA)(Louho et al., 2006) , Motivational Model (MM)(F. D. Davis, 1989)(F. D. Davis, Bagozzi, & Warshaw, 1992) , Theory of Plan Behavior (TPB) (Ajzen, 1991), Theory of Acceptance Model (TAM)(F. D. Davis, 1989)(F. D. F. D. Davis, Bagozzi, & Warshaw, 1989), Innovation Diffusion Theory (IDT) (Rogers, 1995), Social Cognitive Theory (SCT) (Bandura, 1986) , Motivational Model (MM) (F. D. Davis et al., 1992), and Personal Computer Utilization (MPCU) (R. L. Thompson, Higgins, & Howell, 1991). Venkatesh claimed that UTAUT could explain 70% of technology acceptance behaviour and affords a better explanation for factors influencing the individual's intention and usage. UTAUT consists of four core determinants of intention to use: performance expectancy, effort expectancy, social influence, and facilitating conditions. Other information such as gender, age, experience, and voluntaries of use are also recorded to find out the contribution of the entity to user behaviour.

Expending by adding an extension has been applied to the study of various technologies [19](Venkatesh, Thong, & Xu, 2012) in both organizational or non-organizational. Over 400 articles in our concern cited the original UTAUT as their extension to work with more or less of the extended and modifying elements.

The UTAUT model is demonstrated in Figure 11. According to the study, adding factors in support of the investigation of the theories may reveal a breakdown of the theories' results and create new knowledge and generalizability of UTAUT (Neufeld, Dong, & Higgins, 2007).

The UTAUT model is believed to be more suitable for this research because the focus of UTAUT is more specific to the consumer (end-user) who uses and the effort in using the technology regardless of the motivation of use (Venkatesh et al., 2012).

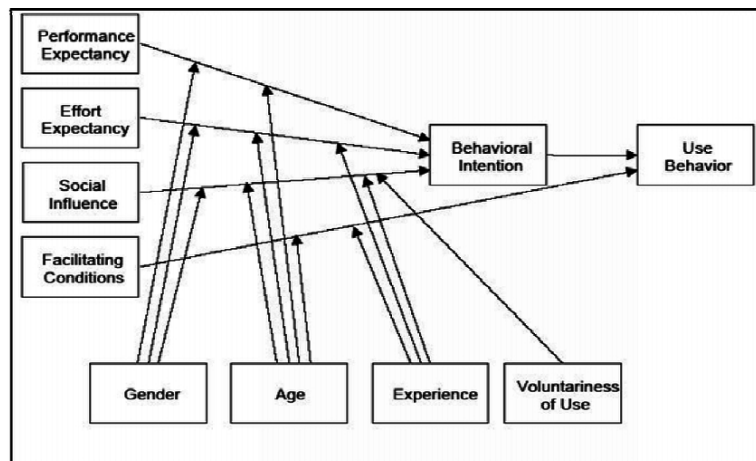


Figure 11: UTAUT Model [178]

### 3.1.3 The Big Five Personality Model

This personality model consists of five broad, bipolar factors representing human personality abstractions that proponents of the model can classify the differences in individuals' personalities. These factors are summarized in specific facets made up of traits (Gosling et al., 2003), as shown in Table 4 below.



Table 4: Facet and Domain of the NEO PI-R Inventory (P T Costa & McCrae, 1992)

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy	Competence	Warmth	Trust	Anxiety
Aesthetics	Order	Gregariousness	Straightfor-wardness	Hostility
Feelings	Dutifulness	Assertiveness	Altruism	Depression
Actions	Achievement Striving	Activity	Compliance	Self-Consciousness
Ideas	Self-Discipline	Excitement Seeking	Modesty	Impulsiveness
Values	Deliberation	Positive Emotion	Tender-mindedness	Vulnerability to Stress

The framework consists of three main groups of factors: Personal, Experience, and Big Five Personality. We represent our related theory with our model in Figure 12, below:

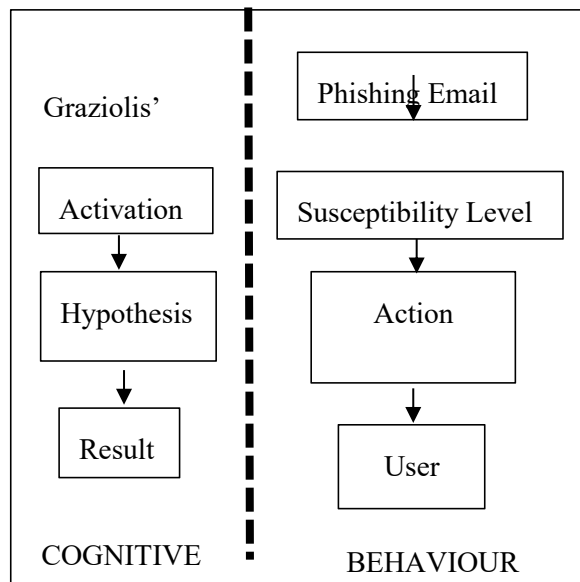


Figure 12: Cognitive and Behaviour in detection process

## 3.2 Research Hypothesis

The research model (see Figure 13) and hypotheses (see Table 6) were developed and empirically tested. Data were collected using a survey, experiment, and interview to obtain a holistic view of the research objective.

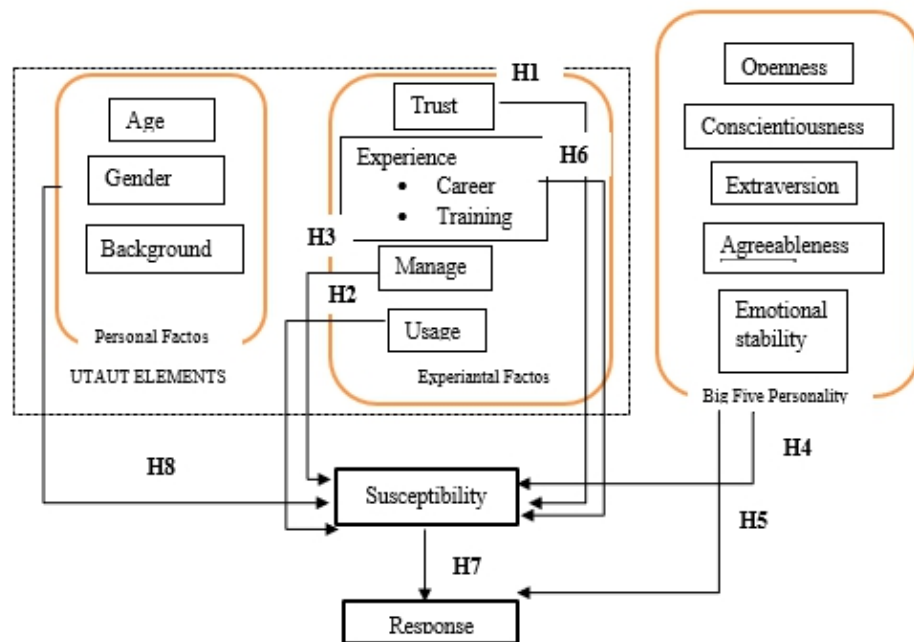


Figure 13: Research model with the hypothesis

### 3.2.1 Trust

The first dimension is labelled “Trust”. Trust is the degree “to willingly become vulnerable to the trustee (another person, institution or people in general) by considering the characteristics of the trustee” (Rousseau, Sitkin, Burt, & Camerer, 1998).

Trust is measured using five items developed by (McKnight, Kacmar, & Choudhury, 2003). Trust can be divided into two types: i) Personal characteristic and

ii) Confidence of reliability for a specific person or organization. Both types of trust are when he/she has dealt with the person or company for a certain period. Since our focus is on user characteristics, our trust measure is more related to the user to email and the organization.

H1: Trust in email influences users' response to phishing emails.

### **3.2.2 Usage**

Usage variable was used as one of the components that came from our selected UTAUT model. This is to see how the user 'usage behaviour' towards technology may affect their decision making towards phishing emails.

H2: Using email in daily activities increases the chances to become a victim.

### **3.2.3 Manage**

The way users manage their email account is essential in a way to understand their effectiveness in dealing with emails. For example, some people may have fewer emails in their account even though they have a longer experience using email. This is because this type of user will often delete unwanted or unrelated emails. Likewise, some people manage to organize their emails using the email developer's features, such as having folders that will help filter emails efficiently.

H3: Users who are able to manage their emails efficiently are less susceptible to phishing emails.

### 3.2.4 Big Five Personality dimensions

The Big Five personality was used to divide individual personality into five main categories; (1) extraversion; (2) agreeableness; (3) conscientiousness; (4) emotional stability; and (5) openness. Each of these categories summarizes more traits that can form different traits in the personality dimension view (Gosling et al., 2003). Many research publications related to the user's personality with the Big Five personality dimension and studied the impact on the users' behaviour and entities (Chiaburu, Oh, Berry, Li, & Gardner, 2011)(Balakrishnan, Khan, Fernandez, & Arabnia, 2019)(Park et al., 2015). Moreover, research in cognitive neuroscience shows that emotion that comes from human personality is able to play an important role in decision-making (Bechara, Damasio, Damasio, & Anderson, 1994). For example, a person who has a high score in extraversion is keen to look into something that gives them excitement. In other words, extraversion could open users to more risks of phishing that uses "offer" or "promotion" as a bite. One other example is the agreeableness personality which involves the potential of believing others with less suspicion. Both of these personality dimensions certainly put users at risk to easily behave in a wrong way.

H4: Dominance in certain personality traits increases users' susceptibility to phishing emails.

H5: Dominance in certain personality traits affect users' response to phishing emails.

We measured the relationship between the Big Five personality dimensions and users' susceptibility and response to phishing emails. The hypothesis for the Big Five dimensions are:

Extraversion (H4a, H5a); Agreeableness (H4b, H5b); Emotional stability (H4c, H5c); Conscientiousness (H4d, H5d); Openness (H4e, H5e). The items were measured using the items developed from the present study, containing ten items altogether (Gosling et al., 2003).

### **3.2.5 Experience**

Email is the primary medium used in deception in a phishing attack, but it is a poor medium for transferring information[26]. This statement does not guarantee that a decrease in email usage can prevent users from becoming phishing victims. Experience is also not a guarantee of awareness level in individuals, especially considering the many new types of attacks created every day.

H6: Users with experience in using email are less susceptible to phishing email.

### **3.2.6 Susceptibility**

We see the susceptibility level in reference to users' ability to suspect any unusual events in emails. Under the MDD model's cognitive phases (see Figure 7), users will go through four cognitive phases before making their decision. The activation cognitive level will only be triggered when inconsistencies happen between the expected cues and observed cues (Burgoon, Buller, Guerrero, Afifi, & Feldman, 1996).

We define user susceptibility by looking at their ability to identify the cues in the email from the survey that asked them to rate the level of response to the email sample. The characteristics of the email are listed in Table 10. According to (Stiff,

Kim, & Ramesh, 1992), suspicions can cause users to focus more on making judgments about what they face based on situational characteristics. In this study, we represent this by the susceptibility variable.

H7: Users with high susceptibility will respond to phishing emails.

Susceptibility is the first phase in users' detection behaviour. Failure to detect phishing cues will lead them to misjudge the email. Therefore, we tested users using four different types of email.

### **3.2.7 Demographic characteristics**

Many researchers have focused on demographic features (gender, age, and education level) as predictors of phishing susceptibility. The results of these approaches were varied; for instance, (Flores, Holm, Nohlberg, & Ekstedt, 2015) found the relationship between cultural differences and personal determinant (Sheng et al., 2010) did not find any significant correlation between age and gender to the susceptibility. It is still relevant to relate demographic characteristics in every research in order to see the relevancy of the subject used in research with the overall research environment.

Compared to the victims, normally, detectors are aware of the attackers' tricks and rely on a solid hypothesis to examine more cues. For example, some detectors may look for cues in the logos, while others look for cues from spelling mistakes, graphics and the type of attachment used in the email. However, victims mostly rely on company logos or padlock signs only (Dhamija et al., 2006). In this present work, this behavioural phase is called response.

H8: Users with a high education level are less susceptible to phishing emails.

### 3.2.8 Response

The response is the last variable used in our research model. It is the final stage of the users' detection behaviour process. It is measured by the action that users need to comply with the requested email. A response is a final stage in the cognitive phase in the MDD global assessment, where the users need to sum up the results of their evaluation(s) and make a decision (Grazioli, 2004).

When the user complies with the request embedded in a phishing email, the data will be recorded under the response variable. This is the final action by a user in order to classify them as victim or detector. Besides that, this is also the final phase in the cognitive phase of the MDD assessment, where users make the last judgement and come to a conclusion.

Table 5: Summary of constructs

<b>Construct</b>	<b>Definition</b>
Trust	Inclination to trust the email
Susceptibility	Users' inability to detect phishing emails
Manage	Capability in managing emails
Usage	Using email in daily activities
Big Five Personality dimensions	The five dimensions of personality
Response	Last phase in cognitive MDD; users' action in response to phishing email.

Table 6: Research hypotheses

Hypothesis	Includes	Description
H1	Trust	Trust in email influences users' response to phishing emails.
H2	Usage	The use of email in daily activities increase the chances to become a victim.
H3	Manage	Users who are able to manage their email decreases susceptibility to phishing emails.
H4	Extraversion, agreeableness, conscientiousness, emotional stability, and openness	Certain personality traits increase users' susceptibility to phishing emails
H5		Certain personality traits affect users' response to phishing emails
H6	Experience	Users with experience in using email are less susceptible to a phishing email
H7	Susceptibility	Users with high susceptibility will respond to phishing emails.
H8	Educational Background	Users with a higher education level are less susceptible to phishing emails.

Table 5 shows the summary of constructs used in the present work, while Table 6 lists all the hypotheses. Some of the hypotheses consist of several constructs under the main hypothesis, which explained in the “includes” column. For example, H4 and H5 are used for the Big Five personality traits, including five constructs under the personality traits.



This chapter has presented the design of the present study. It also explained the process used in identifying the detection ability and behaviour, which is defined as the relevant parameters used for the investigation and then presented in the research model and hypothesis.

## **Chapter 4 Research Methodology**

This chapter explains the choice of methodology consistent with our research model for this work. Specifically, it explains why this particular methodology was chosen and the advantages and limitations of the selected approach.

### **4.1 Methodology/model choice**

In the overall research process, we adopted three approaches or methods that involved information systems and human behaviour in general. Those approaches are the mixed methods, quantitative method and qualitative method (Cresswell, Plano-Clark, Gutmann, & Hanson, 2003)(Hanson, Creswell, Clark, Petska, & Creswell, 2005)(Tashakkori & Teddlie, 2003).

Our main intention of work is to explore and identify the user characteristics that influence email users to respond to social engineering attacks, namely phishing emails. The research also aims at identifying the relationship between those characteristics with users' demographics and backgrounds. To achieve the objective, the research method was combined in a sequential order beginning with the first phase, which involved a literature study associated with users' characteristics in their ability to detect phishing emails, followed by a quantitative method in the second phase, and a qualitative method in the final phase.

## 4.2 Participant Selection

Our target participants in this research are users from an organization which we named as Business Company MARA (BC) and Public (PB) users. The involvement of participants is voluntarily for MARA. The distribution of surveys and experiments is conducted randomly; however, it is still within the allowed departments by the authorities. Anyhow, it still considers the departments that involved more with internet usage, especially email. Unlike MARA, Public email users, as stated in Section 2.11.3, no priority in selections' made. It was chosen because they usually used free email service and came from various background. If the attacker intends and has a different perception of users, they must learn the nature of users.. Moreover, they need a different way of attack and expected response from the attack. This may also contribute to our discussion later, where we also look into demographics features as our study variables.

We did not initially engage the participants in this field, meaning users involved in the first stage were not required to be engaged in the second stage. This is because we did not want to give the users any clues about the experiment and get invalid data due to their cognitive awareness. The main point was to ensure the experiment could be done in a natural environment with no possibility of the users giving fake responses. Therefore, our survey for the public was blasted randomly from the collection of emails we got from the researcher's email account. However, we carefully chose MARA workers' level to ensure the survey and experiment were fairly distributed to all levels for MARA. The selection involved help from IT support in the IT department.

This research involved data collection starting from the initial data with an agency under the Ministry of Rural Development (KKLW), known as Majlis Amanah Rakyat (MARA). It was compulsory to get consent from the top management of the governing body and the department involved. The target of this group consisted of the top management and officers only. These categories were selected because of their work environment that made emails compulsory as a medium of communication. The number of users in these two groups was too large to conduct a direct observation as it seemed impossible and inappropriate to monitor all the users. At this stage, the characteristics of this group made it appropriate for the survey method. Since this experiment was conducted using only the email system, permission from the IT support was required to use the company emailing system. A temporary email under the organisation's domain was requested to test the 'Trust' variable in users and support our hypothesis,  $H_{T1}$ .

Inductive, deductive and experimental approaches were used in the research design during the initial data collection. The inductive study used exploratory research to identify the potential relationship between the dataset and the variables used in our theoretical framework. Theoretical knowledge is often used to find a relationship with the view of literature, and it is often missing insight about the direction and strength of the relationships [4](B. Thompson, 2004). However, less rigorous than the confirmatory approach method, the exploratory method provides more freedom to explore and conduct observations pertaining to the study, particularly discoveries that strengthen and support the conceptualization of the theoretical framework's independent and dependent variables subsequent posited hypothesis. However, the main disadvantage when relying solely on exploratory

research is when the researcher does not interpret the event observed clearly [6] that can causes biases in the results.

A literature review was conducted as the primary procedure to identify the characteristics of the users' ability to detect phishing emails. From here, we developed the conceptual model (see Figure 14). This conceptual model was tested using a mixed-methods approach which comprised a survey, an email experiment, and interviews with the victims and detectors in the final round.

Based on Figure 14 below, the research commenced with a literature review to define the strategy to cater to our objective. It was also used to examine the relationship between the proposed variables with the previous research used in the study under the same domain. We designed the relevant variables for the proposed experiment, survey and email experiment from the findings. We also generated the hypotheses for the study at this stage.

The subsequent step involved conducting the second phase of the research based on the first phase findings. In this phase, we identified the participants' susceptibility level and classed them into detectors and victims. This process involved several tasks and stages, which will be explained throughout the thesis.

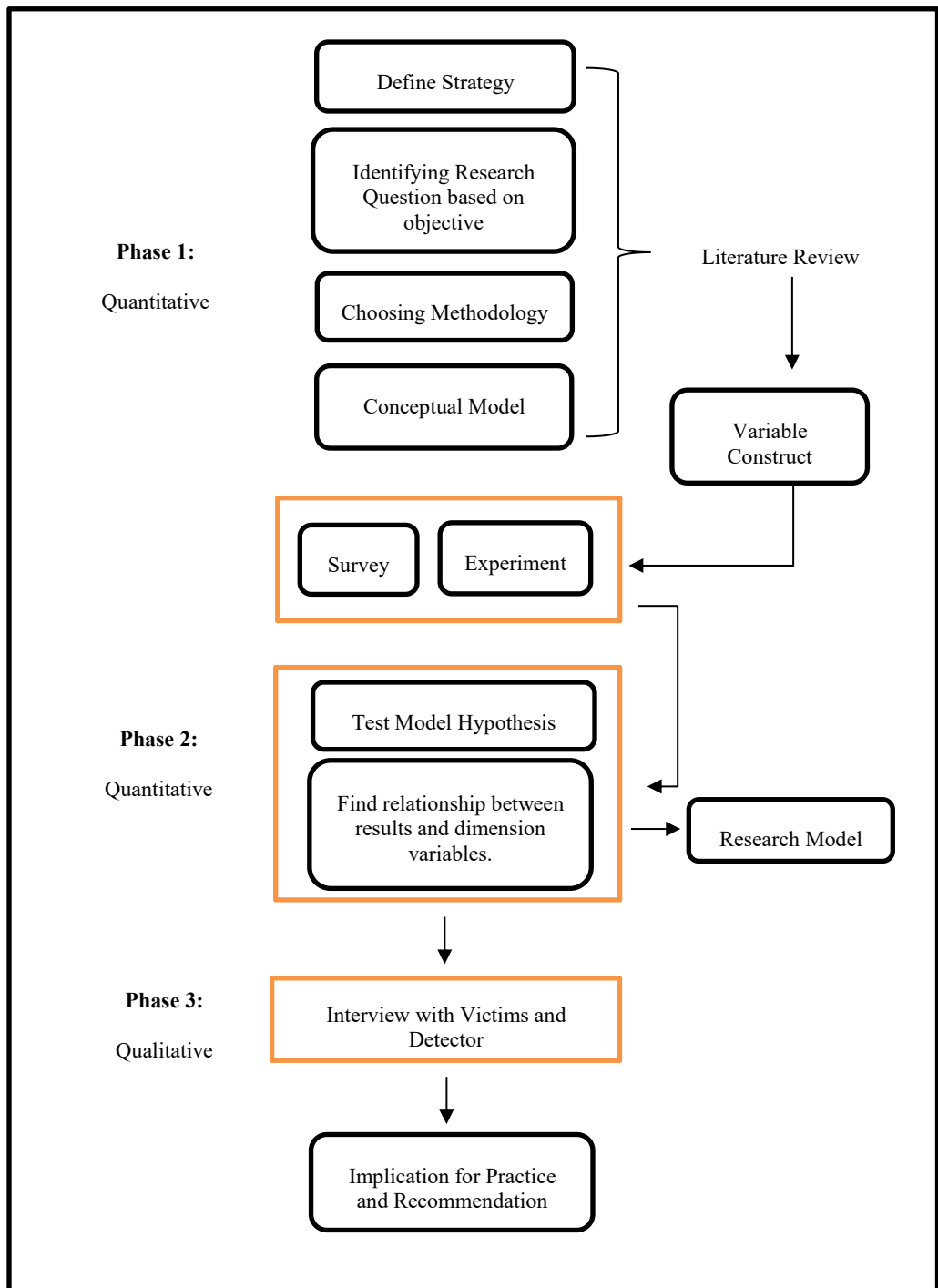


Figure 14: Proposed Research Design

Finally, in Phase 3, we conducted Study 3 - interviews with several victims and detectors to finalize the truth behind their actions. Several questions were given to identify the reason for their action to support the quantitative method results

identified in Phase 2. This method is in reverse order from other research where the interview is regularly conducted at the first phase. Our method is to know the precise reason behind participants' actions and, most importantly, to educate them with the recommended training needs. This is our study's speciality compared to most researchers who usually leave the participants after data has been collected.

### **4.3 Data Collection Method**

In order to fulfil phase 2 and 3 in our research design objectives. We split the discussion about the approach in data collection into three different studies. Study 1 and 2, which represent Survey and Experiment study, is used in collecting quantitative data. In contrast, Study 3, an interview, was constructed to gain in-depth participants experienced in dealing with phishing emails. Different data collection approaches or so-called triangulation process was used in the study to strengthen our finding. Furthermore, it is believed the most flexible and able to collect rich and comprehensive data. (Kusrini, Subagyo, & Masruroh, 2017).

#### **4.3.1 Study One ( Survey )**

Our first study method is Survey. The survey or questionnaire is a research method that includes cross-sectional and longitudinal studies in data collection using structured interviews and various types of the questionnaire (Cresswell et al., 2003). This inquiry type is likewise suited for gathering information from a population with a huge amount to discover. There are a few strengths and weaknesses in the survey method as listed by (Babbie, 2001):

- a. Useful for extracting information from large samples;
- b. Many questions can be asked on each topic; and
- c. No bias – meaning all respondents will answer the same question.

Some of the weaknesses of surveys are:

- a. They are inflexible as there is no change of instrument in the middle of the study;
- b. Standardization may be troublesome for some objectives as the questions given may not all be related to some respondents; and
- c. They rely entirely on answers from the respondents and not the actual action taking place.

A survey is a way to determine the user level of awareness and is used to evaluate a security awareness program(Kruger & Kearney, 2006)(Hansche, 2001). It can also provide the benchmark for research and is proven to be the most efficient way to collect quantitative data from large samples (Darlington & Scott, 2002).

The target users for both groups are large and come from varied locations, making it difficult for the researcher to conduct a direct observation method. Furthermore, this group's characteristics made it appropriate for a survey; it is also considered a sensible method, as indicated by this method's strength. The survey method was used to collect information about the end-users and their characteristics (independent variable), besides measuring these characteristics' impact on detecting phishing emails in both studies' domain.

The survey asked the information related to all the categories in our research design such as demographics, practice and usability, trust, and user experience can be



extracted using this method. The information obtained from this questionnaire was triangulated with the data collected from other studies, which helped compensate for the survey method's weaknesses.

To overcome our limitations in the number and categories of target users and demographics, the online survey questionnaire was chosen as the means to conduct an investigation. Moreover, this method has been used in various systematic studies (Couper, Blair, & Triplett, 1999) and found to be an acceptable methodology (Solomon, 2001).

#### **4.3.1.1 Survey Method**

Online web surveys are now broadly used in many research areas because of the distinct advantages over traditional methods, especially when it is more environmentally friendly, cost minimal, save time and trusted in terms of data integrity. For this research, the questions were designed using Qualtrics software that is compatible for both mobile and desktop and can be accessed from anywhere, making it more suitable and convenient.

The survey constructs were developed by considering as much data that can be collected to cater to the investigation categories in our research model and also by adopting main online survey criteria as follows: response efficacy, self-efficiency questions and general security attitude questions (Ng, Kankanhalli, & Xu, 2009), perceived severity and vulnerability questions (Workman, 2008)(Ng et al., 2009), and user security practice and experience (Rhee, Kim, & Ryu, 2009).

The questionnaire was divided into five sections (see Appendix A). The first section collected general information about users demographic such as their gender and age. The second sections then collect information about the perceived vulnerability, perceived severity, response efficacy, internet practice, user behaviour and experience. The following sections collected information about user security orientation and awareness. Here, users were asked to indicate their awareness of selected security issues and their level of confidence about the current implementation of security in terms of the ability to protect themselves against threats. The fourth section asked users about their perception of themselves using the big five personality items. Finally, users were asked about their potential action towards the email sample given. A seven-point Likert scale and multiple-choice was used for most of the questions.

#### **4.3.1.2 Survey Pilot study**

To produce the best survey, the instrument was tested to avoid potential lead to incorrect conclusions concerning the reliability and validity of the item scales measures. This includes ensuring that the survey system is compatible with all potential devices and platforms. For this study, we applied the pilot-tested to establishes whether the research instrument could be considered reliable. Alternatively, in this study, ten people from college(s) that were not participating in the main study were used (Bachmann, Elfrink, & Vazzana, 1996)(Medlin, Roy, Ham Chai, & Chai, 1999). Respondents were instructed to provide feedback relating to any misinterpretations about what the questions expected from them. To ensure the survey was clear and unambiguous, we included synonyms in parenthesis where necessary for some personality scale items. To encourage honest responses, the

respondents were informed of the purpose of the study, and it is voluntarily where there are no right or wrong answers, and they could withdraw from the survey at any time. The main reason why we need to cater to all of the aspects is simple; to avoid distractions to the users while answering the survey questions which may drive to invalid results.

### **4.3.1.3 Survey Questions**

The aim of the survey is to answer the second and third questions:

- To what extent does the user demographic and characteristics influence the susceptibility level in respond to phishing emails?
- Is there any relationship between the influence with the users' response to phishing?

Our hypothesis is that users' characteristics have a significant impact on their detection behaviour. Therefore, the survey aims to collect data on the below characteristics:

1. Trust
2. Usage
3. Manage
4. Email experience
5. Susceptibility/Vulnerability
6. Big Five personality dimensions
7. Response
8. Age

9. Gender

10. Internet activity

The questions for Trust, Manage and Usage variables were measured on a 7-point Likert scale where 7 is strongly disagree, and 1 is strongly agree. The explanation for each variable is as below.

#### **4.3.1.3.1 Trust**

Trust is a personal characteristic, and it differs from one individual to another. Sometimes, it is not worthwhile to trust entities. Email is one of the entities that users should not trust because attackers will always try to design phishing emails to look like something that people can trust. We measured participants' disposition to trust by using instruments from (McKnight et al., 2003)(see Table 7).

From the literature review, trust is generally expressed as an individual's optimistic expectation for the effect of a consequence or other user behaviour. It is said to be relational when the evidence from previous interactions shows positive expectations about the other party's intentions (Denise, Sim, & Ronald, 1998).

Risk and trust are a path-dependent connection where trust and risk are both in a mutual relationship. It means that a risk-taker can create an opportunity for trust.

The question designed does not ask the user directly about trust, but we try to view how the respondents feel about emails while indirectly giving us information on how they trust emails and rely on emails in their life. Our research wanted to find the impact of trust on users' behaviour or vulnerability with phishing emails.

Table 7: Code items for Trust

Code	Item
Trust1	I found email is a good way to maintain relationships
Trust2	Email is very important in my daily life
Trust3	I look professional when using emails
Trust4	I always choose email as an option for communication
Trust5	I easily trust conversations in emails

#### 4.3.1.3.2 Usage

The usage items asked about users' common email practices. As we know, different users have different ways of usage practice. For instance, some people might use emails for their work only, while some others may use emails for almost all their daily activities such as notification alert, social network, and relationship bonding.

Table 8: Code items for Usage

Code	Item
Usage1	I use email to keep updated with my work activities
Usage2	I use email for my social network activities
Usage3	I use email to pass the time
Usage4	I find email is easy to use

#### 4.3.1.3.3 Manage

The manage variable is used to know how users manage their email. Some people may use some of their time to clean their personal inbox, but some think it is just a waste of time. The question we asked also included whether they are willing to tell others about their email.

Table 9: Code items for Manage

Code	Item
Manage1	I manage to control incoming emails myself
Manage2	I have no problem telling others my email address
Manage3	My email use is effective
Manage4	I always monitor my incoming emails
Manage5	I only respond to emails from known senders
Manage6	I delete emails from unknown senders

#### 4.3.1.3.4 Experience

Users are inclined to become victims from a lack of cognitive involvement in dealing with scam emails (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Experience in email richness increases the potential to extract rich information inside the email (Carlson, 1999).

Users might face difficulties in extracting information and guessing the objective from the email directly. However, phishing is famed to have the same pattern or writing style in content (Iqbal, Khan, Fung, & Debbabi, 2010), such as keywords (Hong, 2009) (Papers & Anderxon, 2006), URL features (McGrath & Gupta, 2008) (Basnet, 2014), language, situational emotion usage (Lampert, 2010), and template (Iqbal, Binsalleeh, Fung, & Debbabi, 2010) that are used in their emails.

Moreover, the number of emails in the user's inbox cannot guarantee the experience level, but it can show the richness of the media used. This is because some users might not read all of their incoming emails and fail to manage their inbox effectively by keeping the unwanted emails in their account.

#### **4.3.1.3.5 Big Five Personality Traits**

The Big Five is known as broad categories of personality traits. Personality traits show the consistencies of individual characteristics over their lifespans across broad situations (Pervin & John, 1999). The dimensions are 1) Extroversion: The character is described by excitability, sociability, talkativeness, assertiveness and a high amount of emotional expressiveness. (Landers & Lounsbury, 2006) in his research found that people who have high extroversion are more involved in their social activities that do not involve computers or Internet usage; 2) Agreeableness: This personality includes trust, kindness, affection and other prosocial behaviours. It is believed that people who have more agreeableness tend to be more cooperative and fall victim to attacks; 3) Conscientiousness: This describes people who are more organized and determined to complete tasks. They are more thoughtful and have good control and goal directive behaviours; 4) Neuroticism: This trait categorises individuals with high instability in emotions. People who have a low level of this trait tend to be calmer and more stable in emotion; 5) Openness: People with high openness are believed to have more range of interest. In other words, openness could be a high-risk measurement for those who are risk adventurers.

Indirectly, risk levels depend on each of these entities. For example, the attacker might design a phishing email that promises the victim a massive amount of returns such as prize, money and benefits to target users with a high dimension in openness. Emails with threats like the potential of losing money, closure of accounts and service destruction are often used for people in the neuroticism dimension. Furthermore, phishing emails are well designed to avoid suspicion among victims. In

relation to the Big Five personality dimension with a phishing email, (Parrish Jr., Bailey, & Courtney, 2009) in his article explored the users' susceptibility to phishing email with the Big Five dimension and agreed that effective intervention requires the understanding of the roles of individuals in the success or failure of an attack.

#### **4.3.1.3.6 Susceptibility**

The first recognition step in MDD is activation, where the users normally will suspect the phishing attempt. The users' subsequent actions will reflect their detection ability. We captured this dimension by designing four phishing emails with different criteria (see Table 10). We added the response value and found the average for each user. Users who average above five will be categorised as susceptible.

The survey asked users to pretend to be the person who received these four emails. They then must rate the possible action they will take when faced with these types of email in real life. The rating used a 7-point Likert scale where 7 is "definitely will respond", and 1 is "definitely will ignore the email". A scale of 5, which rates "maybe will respond," was considered when the users might become susceptible to phishing. Therefore, the average value of five was used to measure the susceptibility level of users.

The selection of emails was carefully chosen to give a real scenario and feel to the users and consider the current attack situation. The instructions for both studies are similar. The participants were advised not to take too much time to answer the question, which gets them to role play by assuming that they have an account and are members of the company used in the experiment, PayPal, Maybank and student. This means that they have to answer the question once they have finished reading the



email. The time gap between reading and answering may allow them to change their attitude towards the question.

The criteria for the four emails are described as below:

Table 10: Characteristics of Phishing emails

Email	Sender	Design	Response	Justification
Email 1	unknown	Text	Action	This email asked the user to check the sender's Facebook
Email 2	Known company	Text + Link	Click	Information update required
Email 3	Known company	Text + Link	Click	Internet banking notification
Email 4	Known	Text + Instruction	Action	System administrator email about storage status

#### 4.3.1.3.7 Age, experience and gender

This is to measure the influence of participants' age, year of experience using email, and gender on their ability to detect the threats (Jagatic et al., 2007)(Bekkering et al., 2009)(Sheng et al., 2010). We asked the users to input their birth year to get their exact age. Other items were asked in the given range.

Table 11: Experience and Gender Items

Code	Items
M	Male
F	Female
O	Others
Y_Exp1	Less than a year
Y_Exp2	1-2 years
Y_Exp3	3-5 Years
Y_Exp4	6-10 Years
Y_Exp5	More than 10 Years

#### **4.3.1.3.8 The Internet for email usage and priority**

Internet access is essential in order to use emails. However, some people may use the Internet to do many other things such as surf websites, play games or online shop but do not have an email account, while others may use the Internet to access emails only. Therefore, it is necessary to know users' practices in using the Internet, the reason they need the Internet, and how vital the Internet is to them to see the level of addiction that may contribute to the wrong usage of the Internet that may expose them to vulnerabilities.

Our expectations of the experienced users are that; they are high in awareness which provides users with the foundation of knowledge for comparison obtained from Internet usage and email usage (Burgoon et al., 1996). We also expected that people with more than two email accounts are more vulnerable because of their addiction to email usage, H6.

Internet usage was measured based on years of usage and the hours that they used the Internet daily, and the rank was based on the priority of the Internet in their life. For email usage, we asked the participants about the number of emails in their inbox, the number of emails they responded to in a day, and the priority of emails in their daily life (refer to survey appendix A). Our research wanted to know whether users' behaviour towards the Internet and email activities will affect the ability to detect phishing emails.

Hypothesis H6 states that "users with more experience in the email will reduce their chances of becoming victims". Therefore, we asked users about their

experience and email richness to measure this hypothesis directly and a few indirectly designed questions to cater to the item measurements in Table 11. For these questions, we provided an interval level of answer for users to choose from. A nominal type of question was used to categorize users' experience level.

Therefore, a literature review was conducted to identify users' behaviour characteristics that expose and make them vulnerable to phishing emails. The detailed examination of the relationship between the independent variable (users' characteristics) and dependent variables (susceptibility, response and risk level) was used to develop a conceptual model.

#### **4.3.1.4 Response**

Due to the limitation on implementing the same approach for tracking response variable in both groups, we proposed two strategies to measure how users respond to email stimuli and phishing requests. For MARA, we captured the actual response of users to the phishing email by using the Study two experiment (see section 4.3.2). Since we were unable to do the same experiment for the Public group users, we introduced an alternative, potentially more ecologically valid measure of a response variable by asking a question about their email credential information. This simulates the real scenario where the vulnerable users usually fail to judge the importance of credential information and respond to attacker question (Schram, 2019).

The response variable was used to label users as victim or detector for further analysis. The two alternative methods for measuring response can produce acceptable results (see section 5.2.4.7), showing that logical validity allows

participants to use their cognitive factors to interact with a situation that reflects their real life.

### **4.3.2 Study Two (Experiment)**

We manage to set up an email experiment using two newly created account under the MARA domain with approval. The account is created purposely for this experiment with the limited time given. To do the experiment study, we designed a tracking system using Microsoft Outlook to track the email open, link- click and user IP address. The main purpose of study two is to track users' who responded to the phishing email that enable us to categorise them as the victim. This response IP was then recorded using an analytic software used to map with the users' survey IP. Users who responded to the phishing email experiment and survey was marked as "1" (victim) for their response variable, and those who were answering the survey and received the phishing email but not doing anything to it will be marked as "0" (detectors).

Categorizing user as victims and detectors are very important to support our third study on digging insight view of both users' categories characteristics that may be hidden and unable to be captured during Study one and Study two. Details about Study three will be discussed in section 4.3.5.

#### **4.3.2.1 Email Experiment Method**

The experiment method is known as a cause and effect relationship study through the control of specific variables and the isolation of other variables. This will

give strength to experimental studies due to emphasising internal validity (Recker, 2013a).

To measure the effectiveness of the factors under a study, each variable under examination must be tested, and any variables that can affect the decision-making process are isolated. The experimental method is considered the most suitable method due to its strength and advantages.

The challenge is to ensure that the experiment is similar to the real environment and is harmless to the participants. Therefore, we needed to comply with the organizational ethical conduct (see Appendix B). This is to make sure that the experiment does not affect productivity and trust in the organization.

The experiment was conducted using three sets of emails (see Figures 15 - 17) and during an office hours (7.00 am to 6.00pm). This is to imitate a hacker's objective to gain the users' trust on the source of the email and study the vulnerability and trust of users towards its existing protection provided by their IT support. This was also to support the current threat where vulnerability can come from the inside organisation.

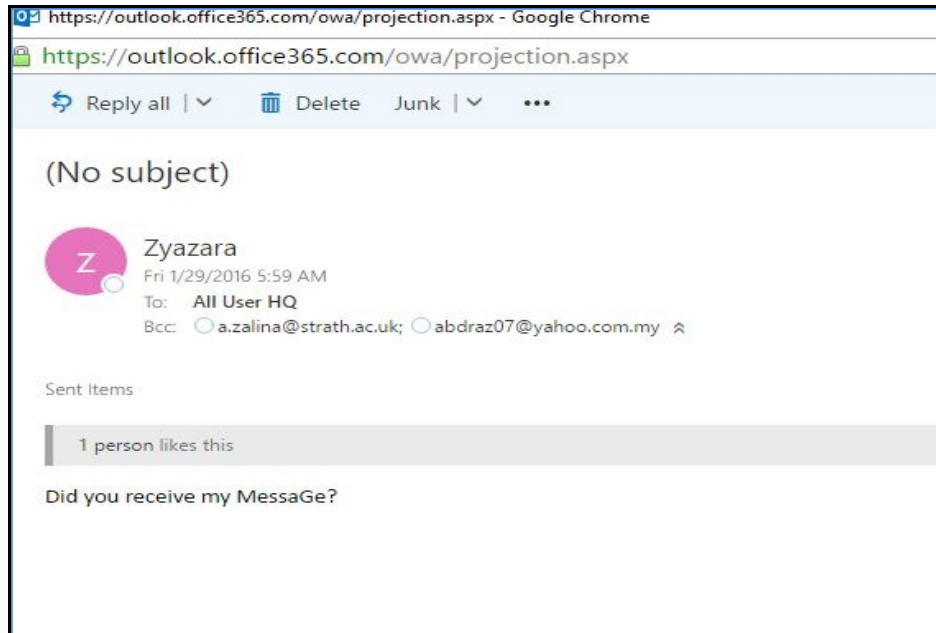


Figure 15: Email Experiment 1

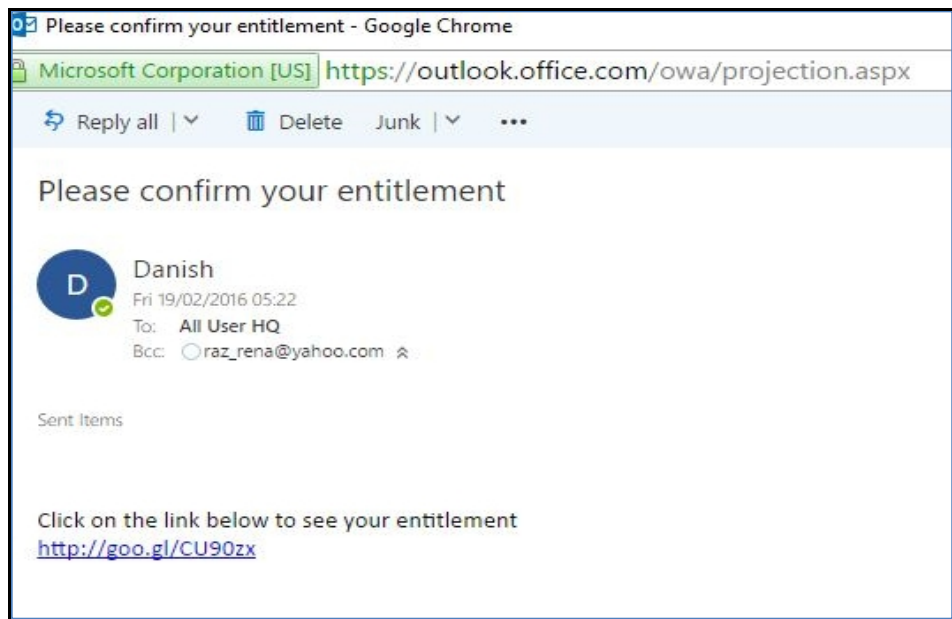


Figure 16: Email Experiment 2



Figure 17: Email Experiment 3

The three emails design characteristics are described and displayed in Table 12.

Table 12: Characteristics of email

Email Experiment	Sender	Design	Response	Justification
1	Known	No Subject, Text, Ask a question	Reply	This email asked if the user has ever received any message from the sender.
2	Known	With subject, Link click	Link click	Asked to check user entitlement
3	Unknown	With subject, ask for a response, text	Reply	Promote user to check sender's Facebook

In this study, we designed email experiments with a simple look to minimize the complicated design and avoid wasting users' time reading the email. This is to cater very busy and lazy people to read long messages and make the email distinct from normal emails. We believe people only read the first few lines to decide whether to stay or leave the message. To avoid users from leaving the message without responding or making any decision, we finally decided that the best technique is to create a simple phishing email design that can catch user interest and response but still keep the email look like a legitimate email for user judgement.

### **4.3.2.2 Experiments Ethical Consideration**

This experiment was conducted in an actual situation and undoubtedly involved critical ethical issues to avoid harming the participants. For the survey study, we manage to get ethical approval from our institution, Strathclyde University. We also manage to get ethical approval to run our experiment in MARA by the IT technical support department head. This is very important and crucial because it involves a deception study and is believed to be harmful to the participants, especially on their trust in the organization and they may feel upset by the deception. To make sure that the experiment causes minimal risk of harm, we carefully tried to control the responses and took care of the participants' privacy. Therefore, for the Mara group, the option is by mapping the IP address from experiments with the IP address from the survey with the help of IT support.

We addressed the ethical concerns when considering our design, as recommended by (Finn & Jakobsson, 2007)(Oh & Obi, 2012). Respondents do not need to reveal their secret information related to accounts (e.g., address, full name and ID number), and we are not advised to store their personal information. The response and results (e.g., vulnerability and staff behaviour) during the study remain undisclosed and will be destroyed at the end of the research. Only the final report will be given to Mara to be used to plan suitable training opportunities for the staff.

### **4.3.2.3 Experiments Pilot study**

Two pilot studies were conducted for Study Two before the actual experiment is release. We minimize the number for a pilot study to minimise the impact of the experiment study, especially for MARA group. Many complaints will be receiving if



too many phishing emails sent to company email accounts. The activity also can give a bad impression on IT support credibility. Furthermore, the pilot study ensures that the features for email study, such as tracking email open, tracking email response, and the link embedded in the email, are working as expected. Since this study is to record the expected user behaviour when dealing with phishing emails, we asked ten people who are not involved in the study about our question and sample of the phishing email.

We did not do the pilot study to our experiment candidates because we did not want to give them any priming study that may provide hints about the experiment, which may affect the study. Users who have a good cognitive level will easily remember the priming study and remain aware of the study. Besides, no one wants to fake ignorance for things that they already know.

The pilot study conducted for our experiment is only to ensure the functionality of the email system used. The most important is to make sure the specified user can receive the email, the link reaches the study page, and the click tracking link from google analytics works well.

As mentioned above, no email phishing training is made to reduce the impact on the organization and user psychology. However, the experiment's content resulted from screening, discussion and selection through analysis of the study literature in the same previous field. Discussion about the email was discussed in the next section.

### **4.3.3 Development Of Email Experiment**

Our objective was to find those who opened the email and clicked the link or responded to our phishing email. In order to do this, we developed a website to link

to our analytic software. At this point, we developed a simple dummy website under the .com domain name “escapido.com”. Also, under the monitoring of the MARA system administrator, they activated two email addresses to be used for the experiment. The email addresses were zyazara@mara.gov.my and danish@mara.gov.my.

In our research, email phishing was designed for specific targets in the organization. The objective is to mimic the role of a legit phishing email, where the attacker is expected to have information about the victims. Furthermore, the percentage of victims that succumbed in this study are in the expected range (Sheng and Magnien 2007)(Luo et al. 2013).

The design for the email in the survey and experiment was different. The idea was to avoid giving cues to the users that may influence their response.

#### **4.3.4 Content Of Experimental Email And Victims Identification**

The email experiment was sent from three different people. Two of them are authentic users from MARA’s domain, while another is from a Gmail user. The main goal is to see the different responses between the emails from the organization as a known sender compared to the unknown sender. An email open tracker software from Outlook 365 was used in the hidden coding within the emails with the motivation to see how many users opened and responded to the emails compared to those who opened and ignored the emails. This was also an efficient way to know whether the emails successfully reached the targeted users. Besides recording on opened emails, the IP addresses for the participants who chose to reply and click on the email link were also captured using Google Analytic software to match their

responses to the phishing email with their responses to the survey. Furthermore, the study in MARA group used the IP addresses to select the user to be interviewed in our final experiment stage.

The design of the experiment email imitated real emails. However, the content was written in full English text. This is an unusual scenario in the organization where Bahasa Malaysia is the primary language in business emails. The receivers should have first noticed this abnormality if they were indeed aware of the difference. However, the results tracked from the response did not show that they were aware of this unfamiliarity.

#### **4.3.5 Study Three (Interview)**

The interview is used in study three to understand more profound human behaviour and the different reasons governing that behaviour. Moreover, it is conducted to understand a research topic or problem from the perspective of detectors and victims. The interview method is known able to provides complex textual descriptions of people experience regarding a particular issue. This method can effectively identify intangible factors such as the individuals' religious belief, norms, gender roles, and ethnicity. The relevance of which to the research topic may not be apparent from the onset but is believe able to strengthen the finding of the study (Chu, PH. and Chang, 2017)

##### **4.3.5.1 Interview Approach**

Study three aims to explain the source of the behaviour that influences users to accept and ignore the email from the source. (Adams & Sasse, 1999) suggest dividing the study into the category that includes the research factors to explore. This

research followed these suggestions to categorize the targeted users for the interview under Detector and Victim to the phishing email. The suggestions help in designing the content of the interview questions.

#### **4.3.5.2 Interview Pilot Study**

A pilot is a rehearsal study that is conducted before the main study is undertaken (Junyong In, 2017) In the present study, four pilot interviews were conducted to test the proposed interview question. The objective is to test the clarity and effectiveness in exploring participants' experience regarding social engineering attack. Some of the modifications to the interviews questions and protocol were made considering the pilot interview results. The adjustments were made in the interview questions; this adjustment is on restructuring the question and statement used in the question design to be more professional look and have some control from the interviewer to enable the study to conform to both the research project and the question methodology.

#### **4.3.5.3 Interview Protocol**

Semi-structured questions were prepared in order to address all the possible topic under investigation. The protocol was adapted based on the objective and purpose of the interview. The environmental characteristics of phishing and how it impact victims were taken into consideration. For example, the interview included some questions regarding the experience of accepting strange email and distinguishing fake and legitimate email. For victims, the extra question was added to know the reason behind their action. Also, interactivity with the participants during the interview allowed the conversation to cover some important questions and topics

that were not included in the semi-structured question but arose during the interview. This followed the approach suggested by (Wengraf, 2001). The interview was conducted in two ways which are face-to-face and over the phone. The participants may choose any one method to used depends on their suitability. Each of the interviews was audio-recorded and transcribed all interview that was conducted in Bahasa Melayu language. Each interview took about 30 to 60 minutes. To manage and to minimise ethical risks issue, the following guidelines were applied before, after and during the interviews:

1. Ensure the interview sessions are conducted in a friendly environment and manner.
2. Participants were explained about the purpose, types of question and privacy of the information they provide before starting the interview.
3. Inform the participants that they have the rights not to answer the question without any penalty.
4. No collected information will be reported to anyone in a position of authority over them that may threaten their position or status.

#### **4.3.5.4 Interview Questions Design**

Through the interview, a researcher can understand human behaviours and the reasoning that governs those behaviours (Wengraf, 2001). It is focused on ‘how’ and ‘why’ of the decision-making process, rather than just focusing on ‘when’, ‘where’ and ‘what’ questions.

Each question was designed by adding ‘ phishing email’ in the sentence as the reference subject to avoid losing focus in the questions. The interview questions are as the following:

- 1) Have you heard about phishing emails?
- 2) How do you identify phishing emails?
- 3) What did you do when you opened the phishing email? Why?
- 4) Have you checked the link in the phishing email? What did you find?
- 5) Have you checked the reply address in the phishing email? What did you find?
- 6) What did you do when you suspected the phishing email?
- 7) Why did you respond to a phishing email? (*For victims only*)
- 8) What did you do when you discover the phishing email? (*for detector only*)
- 9) What is your reaction if someone accesses your account?

#### **4.3.6 Difference Between Mara and Public Group Studies.**

In general, the research design was the same for both groups (see Figures 18 and 19 below). The first stage involved a survey collecting as much data about users’ characteristics and susceptibility to phishing emails. Since both groups were conducted in English, we did not require any language translation in this study. Next, for MARA, we sent an email experiment to capture those who respond to the phishing email. The process required mapping the IP address. However, for the public, this experiment is impossible due to constraints in location and target. Hence, we included the question asking about their email and password. We ended the studies for the public without a Study Two.

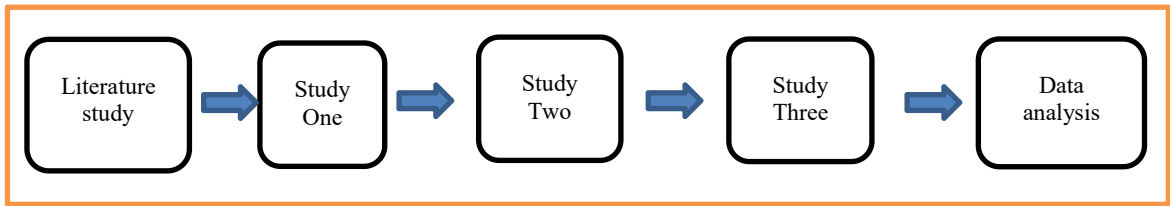


Figure 18: Mara group method



Figure 19: Public group method

## **Chapter 5 Quantitative Results**

### **5.1 Overview**

This chapter presents the results of the quantitative phase. It starts with presenting the profile of the participants, followed by data screening and preparation for exploratory factor analysis and the assessment of the reliability of the measurement. The hypothesis testing is then presented, followed by the demographic analysis, the structural model fit assessment and testing mediation effects. A brief discussion on results was explained at the end of this chapter.

### **5.2 Quantitative Analysis**

A total of 1000 participants from the MARA Organisation (MARA) and 200 from the researcher email list (Public) were targeted. Only those who completed the survey were included in the analysis, which gave the final number of participants 286, with 181 from MARA and 105 from the public.

The reliability and validity of the instruments were examined, and SEM's use to explain the model in the experiment was justified. We analysed the data from both surveys using SPSS version 24 and SmartPLS software version 3.2.7 and presented the final model with structural modelling (SEM) using R software Lavaan Package.



### **5.2.1 Data Preparation**

To ensure the data is ready for analysis, the data was processed using the steps suggested by (Carter, 2010). The steps involved the processes below:

- a) Code Book: A code book was used to arrange the data into coding. For example, the three Years Of Experience in Email groups (1-4), (5-10) and (more than 10 years) were coded as YOE1,2,3, respectively.
- b) Data Cleaning: We conducted the survey online, where the data were entered electronically. Therefore, the dataset had to be cleaned from unrelated entries, blank entries and unsolved questions.
- c) Data eligibility: To ensure no ineligible data were in the analysis, we needed to run two processes:
  - i. Data eligibility - This is used for scale questions where users need to answer from 1 to 7. We ensured that answers were within this range.
  - ii. Response eligibility - This is to ensure none of the responses gave the same answer for all questions.
- d) Raw data was download in Excel format and then exported to the SPSS statistical software.

### **5.2.2 Demographic items**

We tried to make sure of respondents' diversity, which is a priority in demographic characteristics for both studies. However, as a semi-government agency, the policy in MARA only allows for 10% of their staff from other ethnicities than Malay. Therefore, it was one of our constraints to get respondents from other ethnicities in the Mara group. However, we can confirm the diversity of respondents can come from age group, gender, respondent location, and nationality in our public survey.

### 5.2.3 Age and Gender

Besides the steps suggested by Carter, we also look at a few other ways to analyse our result. One of it is dividing the age categories refer to the range suggested by (Fink, 2017) and (Berk, 2015). According to Berk, age 18- 25 refers to the ‘Emerging Adulthood ‘ stage while over 25 is at the ‘Adulthood’ stage. For the Mara group, more than half (55.8%) of the participants were under the category of age 36 years above, and 60.2% (N= 109) were female (Table13). No language and nationality were asked since the study was conducted in the same country, and employment policy is as mentioned above.

Table 13: Age and Gender (MARA)

Age	Frequency	Percent	Gender	Frequency	Percent
18-25	15	8.25	Male	72	39.8
26-35	65	35.9	Female	109	60.2
36 and above	101	55.8			

Compared to the Mara group, the public participants were able to show equality in gender statistic, with male respondents were 50.5% (N=53) while female respondents were 49.5% (N=52).

Table 14: Age and gender (Public)

Age	Frequency	Percent	Gender	Frequency	Percent
18-25	7	6.7	Male	53	50.5
26-35	42	40.0	Female	52	49.5
36 and above	56	53.3			

The age statistic for both studies showed that the participants came from all groups and have the same rank in number distribution, where the most percentage of participants in both groups are from age 36 and above.

Figure 20 below shows the distribution location of our survey respondents. It is from the analytic software used to detect the IP address of the respondents. The red colour represents the survey respondents from the Public group, while blue is from the Mara group.



Figure 20: Respondent distribution

For Public, our respondents came from numerous countries such as Malaysia, Europe, America, Saudi Arabia, and India. It showed we manage to get the diversity of culture among the respondents. Unlike Public, Mara survey showed that the

majority of respondents come from Malaysia. Only one is from America. However, it cannot measure diversity because MARA also has a staff who work at six MARA overseas offices in Australia, United Kingdom, Saudi Arabia, Indonesia, America and India. Therefore, it is within our expectation to have a few responses from them in MARA respondents;

Participants from both groups have also been asked about their email usage. As shown in Table 15 below, both groups show the similar result in a higher percentage. According to the results, it was showing that participants already using email for more than 10 years, receive up to 20 emails in each working day, have more than 500 emails in their inbox, receive only a small number of important emails each day, respond to 1 – 4 emails each day, and sent an average of 1- 4 emails each day.

Table 15: Descriptive statistics for email usage

Statistics	Public		MARA	
	Frequency	Percent	Frequency	Percent
Experience length using email				
Less than a year	1	1.0	1	0.6
1-2 years	1	1.0	4	2.2
3-4 years	10	9.5	13	7.2
5-9 years	18	17.1	38	21.0
>10 years	75	71.4	125	69.1
Number of message receive in each working day				
less than 10	34	32.4	66	36.5
up to 20	59	56.2	100	55.2
more than 20 but less than 50	11	10.5	12	6.6
above 50	1	1.0	3	1.7
Number of email currently in inbox				
50-100	15	14.3	48	26.5
101-500	22	21.0	66	36.5
more than 500	68	68.0	67	37.0
Frequently important emails receive each day*				
none	8	7.6	13	7.2
little	52	49.5	64	35.4
some	38	36.2	79	43.6
a lot	7	6.7	25	13.8
Number of emails respond each day				
none	28	26.7	9	5.0
1-4	55	52.4	89	49.2
5-10	14	13.3	60	33.1
more than 10	8	7.6	23	12.7
Average email send each day				
none	14	13.3	22	12.2
1-4	71	67.6	81	44.8
5-10	15	14.3	60	33.1
more than 10	5	4.8	18	9.9

## 5.2.4 Internet Activities

We asked participants for both studies about their priority in using the Internet based on why they used it. The questions are to see the importance of Internet activities in users daily life.(Kumaraguru, Rhee, Sheng, et al., 2007) Suggest, there is a relationship between users' experience using the Internet with the phishing detection ability. Therefore, this study sought to identify the type of activities that bring to detection ability.

To do so, we grouped Internet usage priority into five primary activities and asked the participants to rank those activities based on their priority. We did not make it an open question to avoid any difficulty in categorizing the results. For both studies, we see the results differ from each other. For the public group, the use of the internet for online games was the main priority, followed by email and social networking (Figure 21). However, in the MARA group, where accessing the internet for the online game is strictly prohibited during working hours, the online game percentage is 0% (See Figure 22). The result shows that the priority of internet usage is suitable for their working environment where the information seeking and searching, 48% and electronic email is 43%. The result showed the suits and expected internet use with the users' task background for both groups. It also contributes information that non of the group showing the major misused of the internet. However, the high percentage of using the internet for online gaming in the public group may come from the participants' age, mostly from teenagers to middle ages. This show the relevancy of the target group with their Age, activity and background.

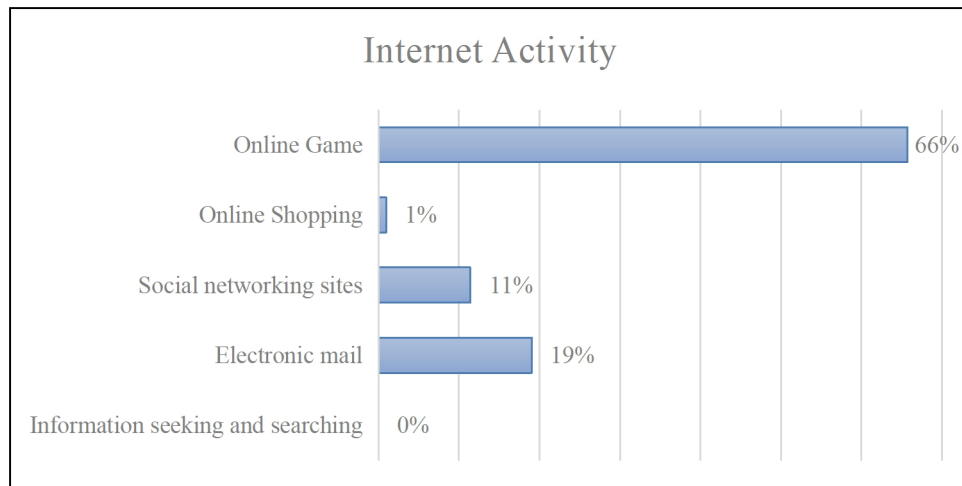


Figure 21: Internet Activity (Public)

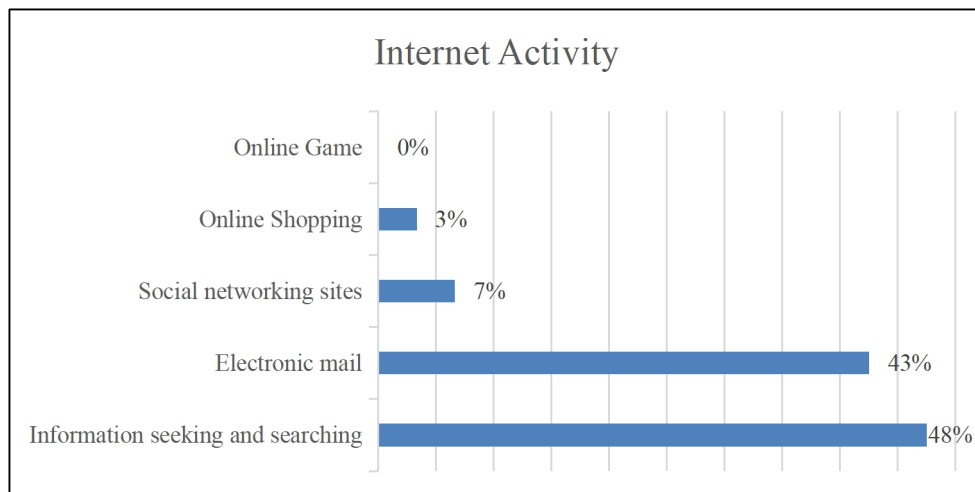


Figure 22: Internet Activity (MARA)

#### 5.2.4.1 Trust

Every variable involved in testing the hypotheses were rated using a 7-point Likert agreement scale (strongly disagree, disagree, somewhat disagree, neither agree nor disagree, somewhat agree, agree, and strongly agree). We used the same question and answer scale for both groups.

For the Trust item, participants were asked five questions. The result is shown in Table 16 below:

Table 16: Trust results for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
I found email is a good way to maintain relationships	5.12	2.73
Email is very important in my daily life	5.39	2.87
I look professional when using emails	5.77	2.07
I trust conversations through emails	4.80	2.89
I always choose email as an option for communication	4.64	1.54

As shown in Table 16, the participants from MARA were able to show that they trust email communication compared to public participants. They do not doubt their ‘trust’ in the email system and have no reason not to trust them. This is not the same as the public respondents where they still have doubted the email system they use.

#### 5.2.4.2 Usage

Participants were asked four questions about their email use. As shown in Table 17, Mara participants rated highest for the easiness of email usage; however, the highest mean for the public respondents is that ‘ email is used to pass the time’.

Table 17: Usage Mean for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
I use email to keep up-to-date with work activities	3.50	2.87
I use email for my social network activities	3.75	2.07
I use email to pass the time	3.10	2.89
Email is easy to use	4.10	1.54



### 5.2.4.3 Manage

We also asked participants six questions about how they manage their email.

This is to see how users deal with and control their emails.

Table 18: Manage Mean for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
I manage to control incoming emails myself	3.99	2.43
I have no problem telling others my email address	3.99	2.06
I always monitor my incoming emails	3.42	2.52
I only respond to emails from known senders	3.99	1.72
I delete emails from unknown senders	3.77	2.58
My email use is effective	4.80	2.42

From the results, MARA respondents were able to show some confidence in how they manage their emails compared to public users, where the average answer is that they somewhat disagree with the way they manage their emails.

### 5.2.4.4 Susceptibility

We measure participants susceptibility based on their rate for four sample emails given. For this question, the 7-point Likert scale was used starting from “Definitely will respond” for 1, “Most likely will delete” for 2, “Maybe will delete or ignore the email” for 3, “I don’t know” for 4, “Maybe will respond” for 5, “Most likely will respond” for 6, and “Definitely will respond” for 7.

Table 19: Susceptibility mean for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
Email 1: Greeting	3.02	3.90
Email 2: PayPal	4.97	3.19
Email 3: Maybank2U	4.78	3.27
Email4: System maintenance	4.01	5.22

Table 19 above shows the highest mean for public respondents is on trusting an email from system maintenance. While for MARA, most respondents chose “Maybe will respond” to the email from PayPal.

#### 5.2.4.5 Big Five Personality Dimension

Participants from both studies were asked to rate themselves with five personality traits based on 10 descriptive items. The items are the components from the five dimensions of the Big Five personality traits. The rated scale used the 7-point Likert scale (Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree and Strongly Agree). The results are shown in Table 20.

Table 20: Big Five Personality Dimension Mean for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
Dependable, self-disciplined	4.60	4.29
Sympathetic, warm	5.91	5.88
Extraverted, enthusiastic	4.50	2.22
Reserved, quiet	2.62	3.71
Calm, emotionally stable	4.07	2.07
Open to new experiences, complex	4.29	2.97
Anxious, easily get upset	3.86	2.93
Critical, quarrelsome	4.30	4.09
Conventional, uncreative	5.02	4.45
Disorganised, careless	4.59	3.80

As shown in Table 20, both public and MARA participants were most likely to agree that they were sympathetic and warm. In addition to that, MARA participants also showed that they agree that they are conventional and uncreative. The results also show that public participants were most disagreeable about being

extroverted, enthusiastic, calm, and emotionally stable. On the other hand, MARA participants mostly disagreed with being reserved and quiet.

For this study, the outcome from 10 items was then combined in pairs to obtain scores related to the primary dimension in the Big Five personality. We used a procedure suggested in (Louho et al., 2006). The procedure involved adding related pairs with the negative item reverse score and dividing the result by two to obtain the mean score. The results are presented in Table 21.

Table 21: Five dimension mean for Mara and Public

	<b>MARA</b>	<b>Public</b>
<b>Statistics</b>	<b>Mean</b>	<b>Mean</b>
Conscientiousness	4.00	4.24
Openness	3.63	3.26
Extraversion	4.93	3.25
Emotional	4.10	3.56
Agreeableness	4.80	4.89

From Table 21, MARA participants almost agreed that they are extroverted and agreeable. Public participants almost agreed that they are in the agreeableness dimension.

#### **5.2.4.6 Response**

The final variable for this study is the dependent variable, Response. This variable is used to identify users' detection behaviour. In the MARA group, we sent three sets of phishing emails created to determine the victims. The score was calculated based on whether the users responded to any of the experiment emails. For the Public group, we calculated the score based on those who responded "YES" for the question asking their willingness to share their email and password in the survey.

Based on the results from the MARA group, out of the 181 survey respondents who also involved in Study Two (Email Experiment), 26% (N=47)<sup>3</sup> responded to the phishing email. This percentage fulfilled the range of the percentage of users who fall victim to phishing email incidents as studied by (Finn & Jakobsson, 2007) and (Knight, 2004). Our study first response recorded within 24 hours after the email was sent. This supports the study done by (Iuga, Nurse, & Erola, 2016) where they also found that victim responds to phishing email within 24 hours of the attack.

Out of 105 respondents to the survey in the public group, 13.3% (N=14)<sup>3</sup> are considered victims. Both studies showed the normal range of fall victim users in an experimental study setting (Sheng et al., 2010)(Alseadoon, Chan, Foo, & Nieto, 2012). The reason users fall victim will be discussed in more detail in Chapter 7 (see Section 7.2.1).

## **5.2.5 Demographic Analysis**

There is not much difference in age and gender from the study in Public and MARA from the results. Both studies showed the same highest percentage category for age and only a slight difference in the gender category.

### **5.2.5.1 Age**

We used the study by Sheng et al. (Kumaraguru et al., 2010) in categorizing the age group. We had users from all groups in both groups (See Table 22 and Table 24), which produces the 3 X 2 table for cross-tabulation. The number of minimum expected frequency cell below five also exists in our tables; however, it is accepted for analysis using chi-squared tests because the number of cells expected frequency

---

<sup>3</sup> This number was calculated based on the response to at least one of the emails in any way.

of 5 or more is greater than 80%. The chi-square test was used to test the relationship between age and users' responses to a phishing email.

A chi-squared test for MARA participants indicated no significant association between age and users' response to phishing emails. However, the chi-squared test for participants' age in the Public group was able to show a significance between age under study with the response to phishing emails with  $p = .044$ . There is not much difference in terms of the age category frequency from both groups that supports why only one group can show the significance in results. However, something that may differ between both is the education background of respondents. MARA users were considered users with a higher education background due to the employment entry policy in government organizations. This cannot be so sure for public users where their background varied. Figures 23 and 24 show frequencies chart for both studies.

Table 22: Frequency age - MARA

		Action		Total	
		Detector	Victim		
Age	18 - 25	Count	10	5	15
		Expected Count	11.1	3.90	15.0
	26 - 35	Count	43	22	65
		Expected Count	48.1	16.90	65.0
	36 above	Count	80	20	101
		Expected Count	74.8	26.2	101.0
	Total	Count	134	47	180
		Expected Count	134.0	47.0	180.0

Table 23: Chi-Squared Test Age - MARA

	Value	df	Asymp.sig (2 sided)	Exact Sig (2-sided)	Exact Sig. (1 sided)
Pearson Chi-Square	4.519 <sup>a</sup>	1	.104	.098	
Likelihood Ratio	4.500	1	.105	.121	
Fisher's Exact Test	4.659			.091	
Linear-by-Linear Association	3.701 <sup>b</sup>	1	.054	.066	.038
N of Valid Cases	180				

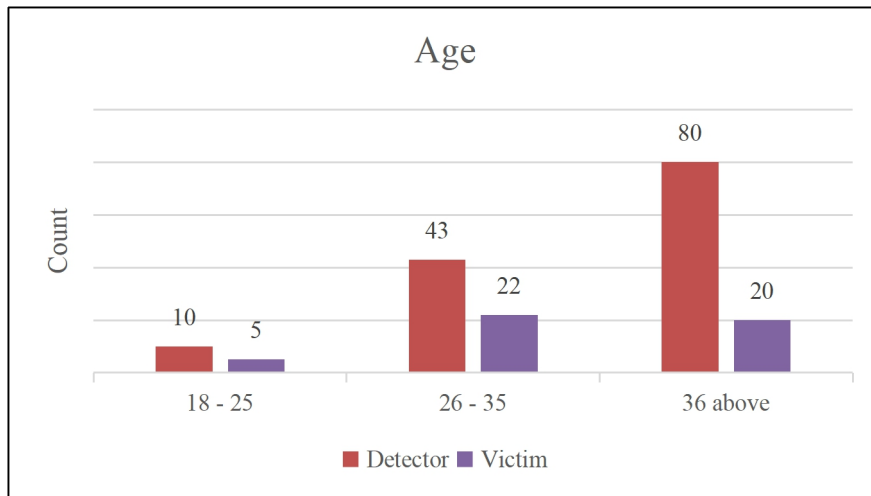


Figure 23: MARA Respondents Age Frequency Chart

Table 24: Frequency age - public

		Action		Total	
		Detector	Victim		
Age	18 - 25	Count	4	3	7
		Expected Count	6.07	0.93	7.0
	26 - 35	Count	36	6	42
		Expected Count	36.4	5.60	42.0
	36 above	Count	51	5	56
		Expected Count	48.5	7.47	56.0
	Total	Count	91	14	105
		Expected Count	91.0	14.0	105.0

Table 25: Chi-Squared Test Age - Public

	Value	df	Asymp.sig (2 sided)	Exact Sig (2-sided)	Exact Sig. (1 sided)
Pearson Chi-Square	6.253 <sup>a</sup>	1	.044	.052	
Likelihood Ratio	4.752	1	.093	.106	
Fisher's Exact Test	5.333			.059	
Linear-by-Linear Association	4.389 <sup>b</sup>	1	.036	.041	.034
N of Valid Cases	105				

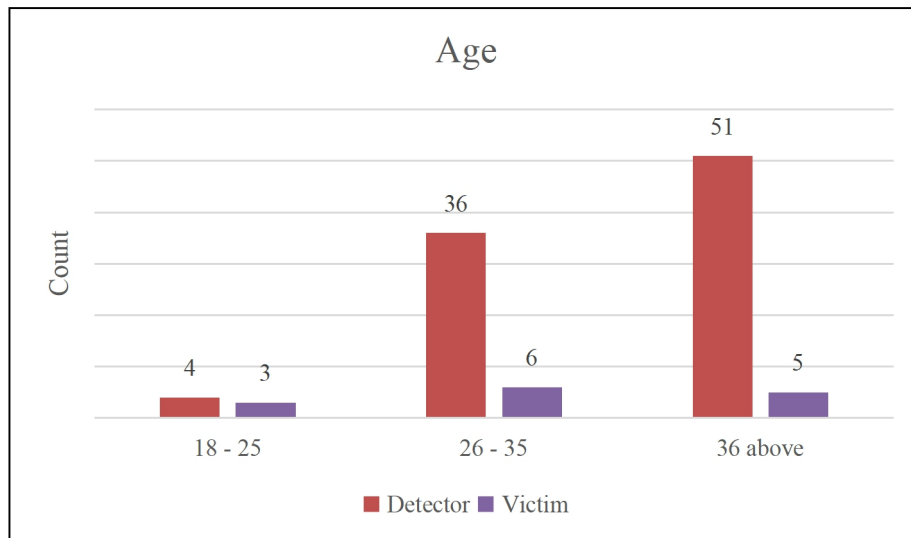


Figure 24: Public Respondents Age Frequency Chart

### 5.2.5.2 Gender

For both groups, the result was unable to show the significance in gender with response to phishing emails. This is consistent with the result obtained by (Sheng et al., 2010), who also found gender was not significant in predicting a victim's. Table 26 and Table 28 show that the number of victims is mostly male users.

Table 26: Frequency Gender - MARA

			Action		Total
			Detector	Victim	
Gender	Male	Count	49	23	72
		Expected Count	53.3	18.7	72.0
	Female	Count	84	24	109
		Expected Count	80.7	28.3	109.0
	Total	Count	133	47	180
		Expected Count	133.0	47.0	180.0

Table 27: Chi-Squared Test - Gender MARA

	Value	df	Asymp.sig (2 sided)	Exact Sig (2-sided)	Exact Sig. (1 sided)
Pearson Chi-Square	2.222 <sup>a</sup>	1	.136		
Continuity Correction	1.736	1	.188		
Likelihood Ratio	2.198	1	.138		
Fisher's Exact Test				.166	.094
Linear-by-Linear Association	2.210	1	.137	.166	.0
N of Valid Cases	180				

Table 28: Frequency Gender - Public

			Action		Total
			Detector	Victim	
Gender	Male	Count	43	10	53
		Expected Count	45.9	7.07	53.0
	Female	Count	48	4	52
		Expected Count	45.1	6.93	52.0
	Total	Count	91	14	105
		Expected Count	91.0	14.0	105.0

Table 29: Chi-Squared Test - Gender MARA

	Value	df	Asymp.sig (2 sided)	Exact Sig (2-sided)	Exact Sig. (1 sided)
Pearson Chi-Square	2.837 <sup>a</sup>	1	.92		
Continuity Correction	1.952	1	.162		
Likelihood Ratio	2.922	1	.87		
Fisher's Exact Test				.150	.080
Linear-by-Linear Association	2.810	1	.94		
N of Valid Cases	105				



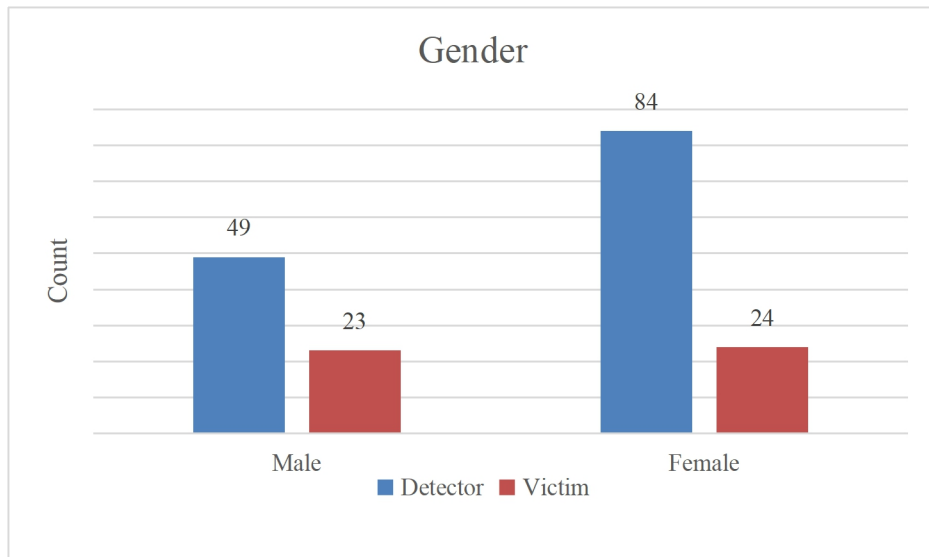


Figure 25: Frequencies chart gender (MARA)

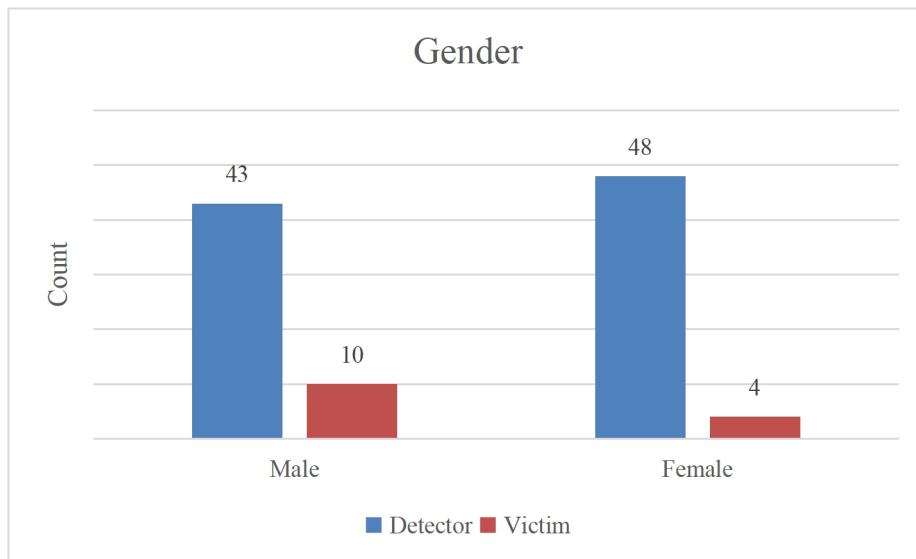


Figure 26: Frequencies chart gender (public)

### 5.2.5.3 Usability

The correlation between two variables was measure using Spearman's test. The results show a significant correlation between only two items measuring users' usage with their response to phishing emails (Table 30). From the finding, the negative relation between frequency of important email receives each day ( $\rho = -0.210, p < 0.001$ ) and the positive relation of hours using the internet in a day ( $\rho = 0.330, p < 0.001$ ) with response was indicated. It shows that with the increasing number of important emails received each day, user response to phishing will decrease. However, the positive relationship between hour spend using the internet shows that the more time users spend using the internet, the more likely users respond to phishing.

We conclude that users with heavy use of the internet by spending much time on the internet are more prone to become victims, while users who do their everyday tasks dealing with important email seem to be more careful when responding to email. The public group did not show any significant correlation between variables which might contribute to the number of low victims in the study.

Table 30: Spearman's rho test on email usage in MARA

		Response	Email_Ex	Em_Receive_InWorkingDay	Num_of emails in inbox.	Freq_imp_Em	Num_Em_RespInDay	Num_Em_Active	Hr_InternetInDay
Response	Correlation Coefficient	1	-.278	.077	-.117	-.210**	.158	-.230	.330**
	Sig (1-tailed)		.000	.000	.000	.002	.000	.001	.000
	N	180	180	180	180	180	180	180	180
Email_Ex	Correlation Coefficient	-.278	1	.131	.196*	.014	.100	.171	.225*
	Sig (1-tailed)	.000		.000	.000	.000	.000	.000	.001
	N	180	180	180	180	180	180	180	180
Em_Receive_In WorkingDay	Correlation Coefficient	.077	.131	1	.092	.317**	.493**	.140	.142
	Sig (1-tailed)	.000	.000		.002	.001	.000	.000	.000
	N	180	180	180	180	180	180	180	180
Num_of emails in inbox.	Correlation Coefficient	-.117	.196*	.092	1	.175	-.155	.135	.129
	Sig (1-tailed)	.000	.002	.000		.000	.000	.000	.000
	N	180	180	180	180	180	180	180	180
Freq_imp_Em	Correlation Coefficient	-.210**	.014	.317**	.175	1	.247**	.112	.174
	Sig (1-tailed)	.000	.000	.001	.000		.000	.000	.000
	N	180	180	180	180	180	180	180	180
Num_Em_Resp InDay	Correlation Coefficient	.158	.100	.493**	-.155	.247**	1	.004	.250*
	Sig (1-tailed)	.002	.000	.002	.000	.000		.002	.010
	N	180	180	180	180	180	180	180	180
Num_Em_Active	Correlation Coefficient	-.230	.171	.140	.135	.112	.004	1	.162
	Sig (1-tailed)	.001	.000	.000	.001	.000	.000		.000
	N	180	180	180	180	180	180	180	180
Hr_InternetInDay	Correlation Coefficient	.330**	.225*	.142	.129	.174	.250*	.162	1
	Sig (1-tailed)	.000	.021	.001	.190	.000	.010	.000	
	N	180	180	180	180	180	180	180	180



## 5.3 Instrument Validity

This section will discuss the process used to measure the reliability and factor analysis to determine and test the dimensionality and validity of variables.

### 5.3.1 Reliability

The function of reliability measurement is to find the consistency between items to the measurement constructs. The reliability measurement concerns consistency and stability of measurement (Lean, Zailani, Ramayah, & Fernando, 2009). Cronbach's alpha was used to measure the reliability in each construct, and the value obtained from the test using SPSS is presented in Table 31. Based on scholars, Cronbach's alpha result of 0.7 is acceptable for the cut-off value (Hair, Black, Babin, Anderson, & Tatham, 2010). However, according to (Pallant, 2011), a Cronbach's alpha of 0.5 is acceptable if the number of items is low.

Table 31: Reliability measures

Variables	MARA		Public	
	Alpha	Item	Alpha	Items
Trust	.685	5	.729	5
Usage	.915	4	.622	4
Manage	.859	6	.741	6
Susceptibility	.688	4	.596	4

All constructs complied with the reliability measurement requirements in both groups, and therefore, all variables are accepted for further analysis.

### **5.3.2 Variable validity**

Once the reliability of the variables is measured, we used exploratory factor analysis (EFA) to measure the variables' validity and uni-dimensionality. Besides using EFA, variable validity can also be measured by obtaining convergent validity and discriminate validity using confirmatory factor analysis (CFA).

#### **5.3.2.1 Exploratory Factor Analysis (EFA)**

The principal component of factor analysis with varimax rotation was used to measure the reliability construct in the survey. The analysis was using SPSS version 24. This step is essential to determine the items with the weak factor loading. It is to ensure that we only retain the items with the strong factor loading in the study. Another advantage of EFA is to identify the items that can be used for the same construct. If more than one variable item can measure the same construct, we might need to choose only the best items to represent the constructs.

Based on Table 32 and Table 33, the EFA results show that there were only three constructs in the MARA group and two constructs in the public group after the analysis. This happened because the items variables for Usage and Manage in the MARA group able to measure the same construct. Therefore, we had to choose only one construct for the factor. At this stage, we decided to remain the Manage variable. We choose Manage because the question given is more related to the objective of the thesis, where we want to see how users behave towards phishing. The same thing happened in the Public group, where three constructs fell under the same factor. This made only one construct chosen to represent the factor, and we decided to use the Manage variable for further study for the same reason as the Mara group.

Furthermore, items that had a high load factor outside their construct were omitted from the study

Table 32: MARA Group Exploratory Factor Analysis (EFA)

	1	2	3	4
Usage 1	<b>0.883</b>		0.199	
Usage 2	<b>0.832</b>	0.109		
Usage 3	<b>0.852</b>		0.197	
Usage 4	<b>0.904</b>			-0.103
Trust 1	-0.276	0.298	<b>0.719</b>	-0.234
Trust 2	-0.330	0.130	<b>0.688</b>	-0.288
Trust 3	-0.282		0.217	<b>0.698</b>
Trust 4	-0.394		<b>0.493</b>	
Trust5	-0.318	0.425	<b>0.540</b>	0.105
Manage 1	<b>0.864</b>			
Manage 2	<b>0.774</b>			
Manage 3	<b>0.909</b>			
Manage 5	<b>0.797</b>	0.141	0.107	
Manage 6	<b>0.826</b>		0.131	
Manage 4			0.275	0.661
Email 1		<b>0.562</b>	-0.233	0.103
Email 2		<b>0.751</b>	-0.287	
Email 3	-0.205	<b>0.667</b>	-0.112	-0.207
Email 4	-0.105	<b>0.704</b>	-0.291	0.131

Table 33: Public Group Exploratory Factor analysis (EFA)

	1	2	3	4
Usage 1	<b>0.627</b>	0.539	0.347	-0.139
Usage 2	<b>0.819</b>	-0.255	0.130	
Usage 3	<b>0.681</b>	-0.108	-0.644	0.105
Usage 4	<b>0.608</b>	-0.474	0.379	0.374
Manage 3	<b>0.722</b>	0.355		-0.275
Manage 6	<b>0.543</b>	0.159	0.197	
Manage 5	<b>0.426</b>	-0.369	0.212	0.123
Manage 4	<b>0.714</b>	-0.137	-0.553	
Manage 2	<b>0.825</b>	-0.233	0.123	
Manage 1	<b>0.407</b>	0.232	-0.155	-0.201
Trust 1	<b>0.693</b>	0.428		-0.214
Trust 2	<b>0.627</b>	0.539	0.347	-0.139
Trust 3	<b>0.819</b>	-0.255	0.130	
Trust 5	<b>0.681</b>	-0.108	-0.644	0.105
Trust 4	<b>0.608</b>	-0.474	0.379	0.374
Email 1		0.545	-0.108	<b>0.571</b>
Email 2	0.126	0.354		<b>0.677</b>
Email 3		0.308	-0.195	<b>0.565</b>
Email 4	0.119	<b>0.509</b>	0.198	

An explanation for the result can be attributed to the biased answers given by the public participants (Ali Hussein Alkahtani, Ismael Abu-Jarad, 2011).

### 5.3.2.2 Confirmatory Factor Analysis (CFA)

Confirmatory factor analysis has a strong relationship with structural equation modelling (SEM); it can also examine the construct validity of all the variables. However, CFA cannot be analysed using SPSS. In this study, we used partial least square software (SmartPLS 3.8) to do the CFA.



(Fornell & Larcker, 1981) suggested that the average Variance Extracted (AVE) minimum requirement for each construct is 0.5 and above. On the other hand, (Stevens, 1992) suggested using a cut-off of 0.4 as acceptable for factor loading irrespective of sample size.

The results shown in Table 34 and Table 37 support the assumption that convergent validity can be obtained within the construct for both groups. Only one item in both the public and MARA group study did not meet the minimum suggested factor loading. This means that this item does not contribute to measuring the construct and can be removed. Therefore, the item is removed from further analysis.

Tables 35 and 36 for the MARA group, while Tables 38 and 39 for the Public group show the AVE for each variable. From the results, the value of AVE met the suggested rule of discriminant validity where it should be greater than the square correlation between a pair of latent variables.

Results from both convergent and discriminant can be concluded that our variables have satisfied the construct validity in both study groups.

- Even if the AVE is higher than 0.5 is an acceptable value for the validity of the construct. However, according to (Fornell & Larcker, 1981), “Evaluating structural equation models with unobservable and measurement error” (journal of marketing research pp39-50,1981), an AVE less than 0.5 is still acceptable if the composite reliability is higher than 0.6.
- In the MARA and Public group study, both constructs met the suggestion by Fornell for composite reliability higher than 0.6.

Table 34: Factor Loading MARA

	MANAGE	SUSCEPTIBILITY	TRUST
<b>Email 1</b>	0.069	0.038	-0.030
<b>Email 2</b>	-0.018	<b>0.454</b>	0.040
<b>Email 3</b>	-0.175	<b>0.952</b>	0.177
<b>Email 4</b>	-0.064	<b>0.570</b>	0.003
<b>Manage 1</b>	<b>0.905</b>	-0.176	-0.333
<b>Manage 2</b>	<b>0.849</b>	-0.177	-0.408
<b>Manage 3</b>	<b>0.897</b>	-0.197	-0.310
<b>Manage 5</b>	<b>0.764</b>	-0.039	-0.244
<b>Manage 6</b>	<b>0.831</b>	-0.165	-0.243
<b>Trust 1</b>	-0.172	0.125	<b>0.746</b>
<b>Trust 2</b>	-0.245	0.107	<b>0.738</b>
<b>Trust 4</b>	-0.377	0.067	<b>0.732</b>
<b>Trust 5</b>	-0.249	0.210	<b>0.731</b>

Table 35: Discriminate validity (MARA)

	MANAGE	SUSCEPTIBILITY	TRUST
MANAGE	<b>0.851</b>		
SUSCEPTIBILITY	-0.187	<b>0.600</b>	
TRUST	-0.374	0.170	<b>0.737</b>

Table 36: Composite Reliability (MARA)

	Composite Reliability
MANAGE	<b>0.929</b>
SUSCEPTIBILITY	<b>0.613</b>
TRUST	<b>0.826</b>

Table 37: Factor Loading (Public)

	MANAGE_	SUSCEPTIBILITY
<b>Email 1</b>	0.190	<b>0.806</b>
<b>Email 2</b>	0.158	<b>0.658</b>
<b>Email 3</b>	0.068	<b>0.527</b>
<b>Email 4</b>	0.194	<b>0.628</b>
<b>Manage 1</b>	<b>0.646</b>	0.119
<b>Manage 2</b>	<b>0.475</b>	0.009
<b>Manage 3</b>	<b>0.825</b>	0.180
<b>Manage 4</b>	<b>0.459</b>	0.002
<b>Manage 5</b>	<b>0.029</b>	-0.095
<b>Manage 6</b>	<b>0.686</b>	0.178

Table 38: Discriminant Validity (Public)

	MANAGE	SUSCEPTIBILITY
<b>MANAGE</b>	<b>0.578</b>	
<b>SUSCEPTIBILITY</b>	0.249	<b>0.662</b>

Table 39: Composite Reliability (Public)

	Composite Reliability
<b>MANAGE</b>	<b>0.709</b>
<b>SUSCEPTIBILITY</b>	<b>0.753</b>

## 5.4 Hypothesis Testing

In this section, we present the results from our hypothesis testing and structural model. R software with Lavaan package was used to test the overall model (Rosseel, 2012b). The Lavaan package was proposed to test the SEM models, including categorical variables as dependent variables (Rosseel, 2012c). It is needed

to cater to the categorical dependent variable (response) used in our research and logistic regression to test the hypothesis.

Our research has two dependent variables (susceptibility and response). Therefore, we chose multiple linear regression for susceptibility and logistics regression for response variables to test both hypotheses. The final model was then tested with R software, which can test SEM that includes a categorical variable as a dependent variable, in our case is the response variable. The analysis for the study was organised as below in order to show the results.

#### **5.4.1 The need for regression for hypothesis testing**

Earlier in the study, we applied linear and logistic regression to test the regression coefficient (Beta value) for each variable used in the study. The advantage of logistic regression is the ability to test the regression coefficient for a binary categorical dependent variable which cannot be done using SEM. However, both regressions have one limitation where it is limited to measure only one dependent variable. Since our research has two dependent variables, we used SEM to measure the overall model.

Besides the limitation, regression still is the best way to investigate the impact of variables on their dependent variable. The hypothesis testing involves investigating the impact of the predictors on a singular dependent variable (Hair et al., 2010).

##### **5.4.1.1 Regression analysis steps**

The three main analytical steps used to test the research hypothesis in the study are:

1. Factors are obtained from the average score for the items in each factor.
2. Testing predictors individually with their related dependent variable.
3. Applying the regression and interpreting the results.

#### **5.4.1.2 Factor score**

The factor score is calculated by computing the score for every item presenting the factor (Raykov & Marcoulides, 2019)(Gudgeon, Comrey, & Lee, 1994). The score is then divided by the number of items that contribute to the scale to get the average. For example, susceptibility was measured using four items. Therefore, the final score for susceptibility was calculated as follows:

$$\text{Susceptibility} = (\text{Email 1} + \text{Email 2} + \text{Email 3} + \text{Email 4}) / 4$$

#### **5.4.1.3 Relationship testing between variables**

The first step in regression is to test the impact of each independent variable with the dependent variable (susceptibility and response). Only those with a significant relationship with the dependent variable were grouped in the model in the final model. The reason for this step is to prevent any insignificant variable(s) from entering our final model. The results for this procedure are shown in Table 40 to Table 43.

Table 40: Linear regression with Susceptibility as a dependent variable for MARA

Independent variables	Test Results
Trust	There is a positive and significant relationship between trust and users' susceptibility
Manage	There is a positive and significant relationship between manage and users' susceptibility
Openness	There is a negative and significant relationship between openness and users' susceptibility
Extraversion	There is a positive and significant relationship between extraversion and users' susceptibility
Agreeableness	There is a negative and significant relationship between agreeableness and users' susceptibility.
Usage	There is a negative and significant relationship between usage and users' susceptibility

Table 41: Logistic regression with Response as dependent variable for MARA

Independent Variable	Test results
Susceptibility	There is a positive and significant relationship between susceptibility and response to phishing email.
Openness	There is a positive and significant relationship between openness and users' response to phishing email.
Trust	There is a positive and significant relationship between trust and users' response to phishing email.
Agreeableness	There is a negative and significant relationship between trust and users' response to phishing email

Table 42: Linear regression with Susceptibility as a dependent variable for Public

Independent variables	Test Results
Agreeableness	There is a positive and significant relationship between openness and users' susceptibility

Table 43: Logistic regression with Response as a dependent variable for Public

Independent variables	Test Results
Openness	There is a positive and significant relationship between openness and users' response.
Usage	There is a positive and significant relationship between usage and users' response.
Susceptibility	There is a negative and significant relationship between susceptibility and users' response.

#### 5.4.1.4 Interpreting regression results

This section describes the results for the significant independent variables obtained from testing with susceptibility and response variables. Our main hypothesis is that the predictor variables have an impact on users' susceptibility. The results obtained from the quantitative analysis for the hypothesis is as below:

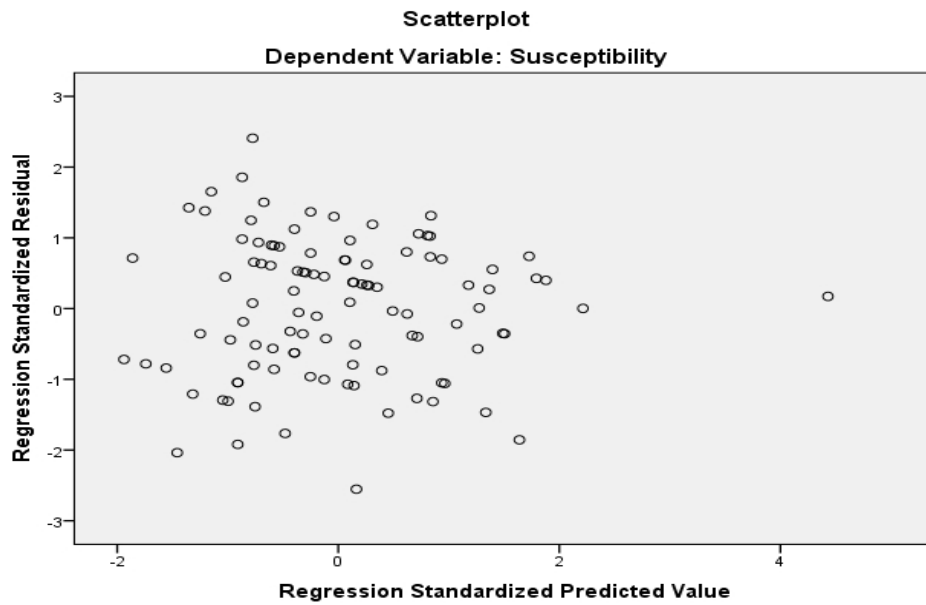


Figure 27: Regression scatter plot (Public)

The linearity for both groups can be examined from the scatter plot in Figure 27 and Figure 28. As can be seen, the residuals did not show any major nonlinear pattern (Hair et al., 2010). The data points in both scatter plots are shown in random. Therefore, we conclude from the result that the linearity and homoscedasticity are satisfied for both groups.



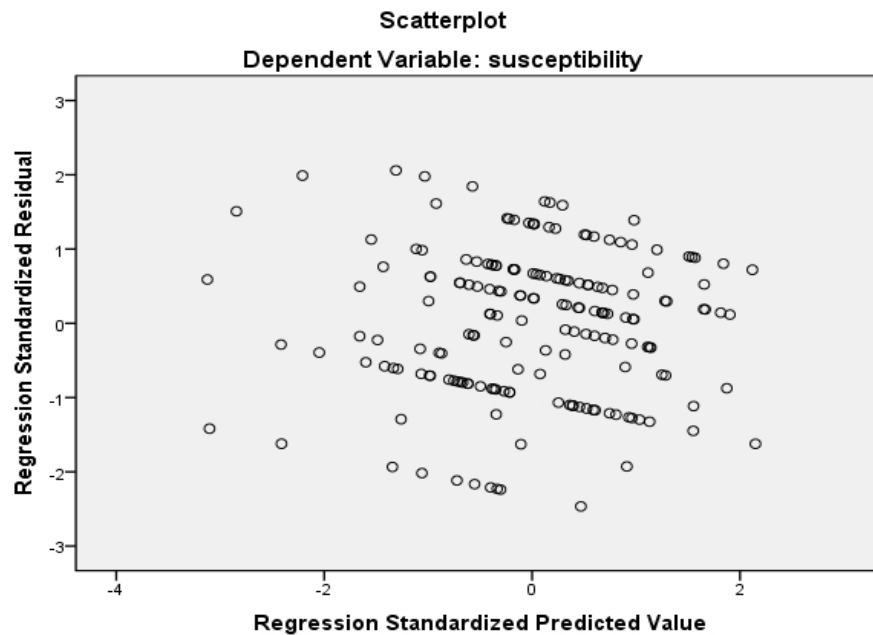


Figure 28: Regression scatter plot (MARA)

Normality, however, can be examined by looking at the value provided in the skewness and kurtosis. The normal distribution of data is close to zero of these two measures. Also, some scholars suggested that normality can be achieved if the study has a large sample size (more than 40 cases) (A. Field, 2013)(A. P. Field, 2018). Our studies, the number of participants met the suggested criteria and, therefore, satisfies the normality requirement.

Multicollinearity measures the relationship between the predictors and suggests a strong predictor relationship (Hair et al., 2010). Two types of measures are used to satisfy this requirement: variable inflation factor (VIF) and tolerance level (TOL), where VIF should be below ten and TOL should be above 0.1 in order to conclude the absence of multicollinearity (Andy Field, 2009)(Hair et al., 2010). The public group does not require multicollinearity measures since the regression test only had one independent variable. Table 44 shows that the predictors examined in our research are suitable for multiple regressions for the MARA group.

Table 44: Collinearity statistics

Predictors	Collinearity Statistics	
	Tolerance	VIF
Trust	.298	3.356
Manage	.276	3.3620
Openness	.822	1.217
Extraversion	.785	1.274
Agreeableness	.341	2.931
Usage	.255	3.919

To measure the dependency of residuals for variables, we used Durbin-Watson measures. The Durbin-Watson test values obtained for both groups are 2.137 for MARA and 1.864 for the public. These values are acceptable for the Durbin-Watson test where the value should be close to 2 in order to show the independence between residuals (Andy Field, 2009).

The results from linear regression in the Public group show a positive and significant relationship between agreeableness and susceptibility. Agreeableness explains 3.1% of the variance in susceptibility. The overall model shows a significant impact on susceptibility with the proposed model as nearly ( $p < 0.05$ ) (see Table 45 and Table 46).

Table 45: Linear regression result - susceptibility (Public)

Model	Unstandardized Coefficients		Standardized Coefficient	t	Sig.
	B	Std. Error	Beta		
(Constant)	3.928	0.907		4.322	.0000
Agreeableness	.218	.119	.329	1.837	.053

Table 46: Model Summary - Susceptibility (Public)

Model	R	R Square	Adjusted R Square	Std. Error of the estimate
1	.176	.031	.029	1.381

Results from multiple regression (Table 47 and Table 48) for the MARA group show that two positive and significant relationships between Manage and Trust with susceptibility as the dependent variable. There is one relationship with a negative and significant relationship between Openness and Susceptibility from the result obtained. The result shows that Manage, Trust, and Openness can explain 84% of the variance in susceptibility. The overall model shows a significant impact on susceptibility by the proposed model ( $p < 0.001$ ) (see Table 46).

Table 47: Linear Regression result - susceptibility (Mara)

Model	Unstandardized Coefficients		Standardized Coefficient	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.780	1.287		1.320	.155
Trust	.198	.065	.210	2.345	.011
manage	.534	.071	.190	7.101	.003
Openness	-.215	.066	-.210	-3.10	.006
Extraversion	.048	.065	.043	.823	.450
Agreeableness	-.093	0.835	-.073	-1.122	.323
Usage	.125	0.90	.072	.999	.186

Table 48: Model Summary – Susceptibility (MARA)

Model	R	R Square	Adjusted R Square	Std. Error of the estimate
1	.920	.8464	.921	1.215

#### 5.4.1.4.1 Response as an outcome

A major hypothesis is that the predictor variables impact users' response (he/she would respond to phishing email). Basically, we need to satisfy the logistic assumption from the logistic regression for the binary categorical dependent variable

with a sample size above 50 (Hutcheson & Sofroniou, 1999). Our two studies were able to fulfil these two assumptions since our dependent variable, ‘response’, is a binary category (detectors or victims). We present our results from the logistic regression below.

Both predictors, openness, usage and susceptibility, were significant at the  $p < 0.05$  level in the public group. These three variables increased the users’ response to phishing emails (see Table 49)

Table 49: Public Logistic regression with a response as an outcome.

	<b>B</b>	<b>S.E</b>	<b>Wald</b>	<b>df</b>	<b>Sig.</b>	<b>Exp(B)</b>
Susceptibility	-.432	.209	5.021	1	.025	1.432
Openness	.548	.255	4.876	1	.019	1.650
Usage	.390	.201	1.323	1	.049	1.925

Table 50: Model summary – Response (Public)

<b>Step</b>	<b>-2 Log likelihood</b>	<b>Cox &amp; Snell R Square</b>	<b>Nagelkerke R Square</b>
1	91.88	.073	.168

Based on Table 50, the Cox and Snell R-square formula, this model is able to explain 7% of the variance, with the Omnibus model coefficient statistically significant at the  $p < 0.01$  level. This gave a consistent between model significance and percentage of the variance. Openness and Usage variables have a positive and significant relationship with a Response, while Susceptibility has a negative but significant relationship with a Response. From the results in Table 49, we can conclude that those higher in Openness and users’ Usage behaviour effect two times more likely than others (Exp(B)) with Response to the phishing emails.

Table 51 shows that predictors such as Openness, Susceptibility, Trust and Agreeableness were significant at  $p < 0.01$  level in the Mara group. Openness and Susceptibility show the significance for both groups. However, MARA predictors that significantly include Trust and Agreeableness can increase users' response to phishing emails.

Based on the Cox and Snell R-square (see Table 52), this model is able to explain 38% of the variance, with the omnibus model of coefficients statistically significant at the  $p < 0.001$  level and consistent with the model by explaining a significant percentage of variance. Susceptibility, Openness and Trust have a positive and significant relationship with the Respons with  $p < 0.01$ . Agreeableness, however, shows a negative and significant relationship. This means that Agreeableness is more likely to increase users' ability to detect phishing emails. The significant level for agreeableness is shown at  $p < 0.05$  level. The result for agreeableness shows a similarity to linear regression, where Agreeableness also shows a negative relationship and significant to susceptibility.

Table 51: Final MARA Logistic Regression on Response result.

	<b>B</b>	<b>S.E</b>	<b>Wald</b>	<b>df</b>	<b>Sig.</b>	<b>Exp(B)</b>
Susceptibility	.872	.229	10.231	1	.001	2.360
Openness	.772	.213	8.970	1	.000	2.495
Trust	1.032	.187	11.020	1	.002	1.720
Agreeableness	-.328	.189	3.465	1	.034	.652

Table 52: Model summary – response (MARA)

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	112.987	.382	.543

As indicated in Table 52, both high susceptibility and openness were almost two and a half times more likely than others (Exp (B)) to respond to phishing emails. Those with a high Trust score were two times more likely than others (Exp(B)) to respond to phishing emails, and those with Agreeableness is one time likely than others (Exp(B)) to detect the phishing emails. Table 53 below shows the supported hypotheses obtained from both regression models in both studies.

Table 53: List of supported hypotheses

No.	Variables	Public		MARA	
		Result	Supported	Result	Supported
H1	Trust		N/A <sup>4</sup>	$\beta = 0.210^5$ and $p = 0.011$	Yes
				$\beta = 1.032^6$ and $p = 0.002$	
H2	Usage	$\beta = 0.39$ and $p = 0.049$	Yes		No
H3	Manage		N/A	$\beta = 0.190$ and $p = 0.003$	Yes
H4	Personality traits	$\beta = 0.329$ And	Yes		No
	Agreeableness	$P = 0.053$			
	Openness		N/A	$\beta = -0.210^7$ and $p = 0.006$	Yes

<sup>4</sup> N/A means we did not test the construct because it did not satisfy the validity measurements or not significant.

<sup>5</sup> Blue indicates from linear regression result

<sup>6</sup> Black indicates from logistic regression result

<sup>7</sup> Red indicates negative impact

No.	Variables	Public		MARA	
		Result	Supported	Result	Supported
H5	Personality traits				
	Openness	$\beta = 0.548$ and $p = 0.019$	Yes	$\beta = 0.534$ and $p = 0.003$	Yes
	Agreeableness		N/A	$\beta = -0.328$ and $p = 0.034$	Yes
H6	Experience		N/A		N/A
H7	Susceptibility	$\beta = -0.432$ and $p = 0.025$	Yes	$\beta = 0.872$ and $p = 0.001$	Yes

## 5.4.2 Structural equation modelling (SEM)

We used SEM in analysing our multiple independent and dependent variables. The only issue when using SEM, is measuring the latent variable instead of the manifest variable. To overcome SEM software constraint, we used R software with Lavaan Package in analysing the overall model because of its ability to analyse SEMs with categorical dependent variables (Rosseel, 2012a).

The measurement model has provided satisfactory reliability and validity. This means that all items used in our research are able to measure the construct they are expected to measure. We continued evaluating the research model using structural equation modelling (SEM) in the next step. SEM is widely used in testing the behavioural of studies (Baumgartner & Homburg, 1996)(Henseler, 2017)(Novak, Hoffman, & Yung, 2000).

We investigated users' behaviour when they faced phishing emails. Figure 29 and Figure 30 show that the model is explained from the goodness of fit for the

research model. Both groups have different values to explain their responses to phishing by referring to the variance value. For the Public group, the overall model explains that 17% of the variance users' behaviour will respond to the phishing email ( $R^2 = 0.172$ ). In the MARA group, the overall model is able to explain that 39% of the variance is responsible for the users' behaviour in response to phishing emails ( $R^2 = 0.390$ ). Table 54 to Table 57 provide details about the outcome of the models. We will discuss the reason for the difference in Chapter 7.

Figure 29: Structural model for Public group

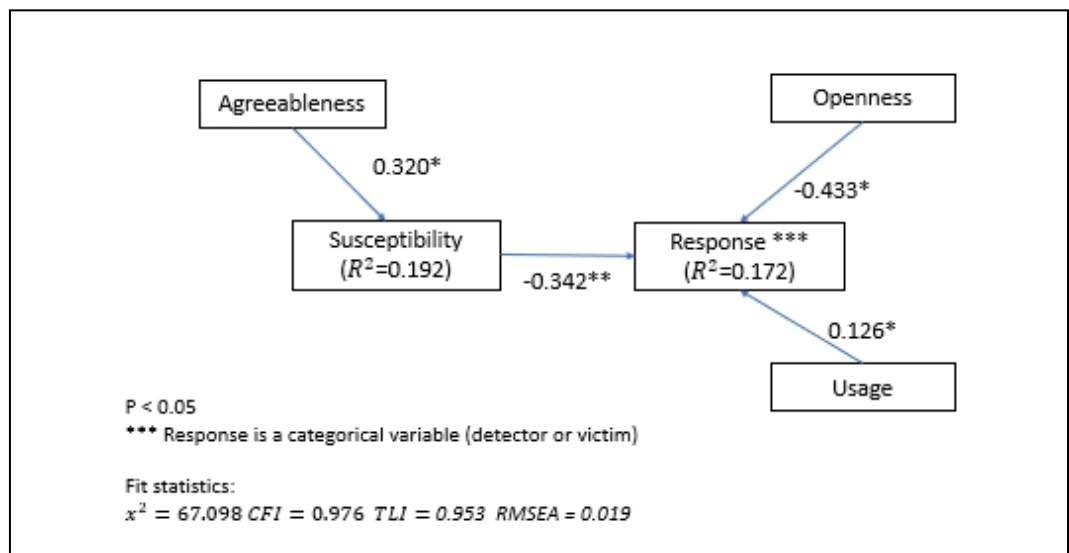


Table 54: R Software results - Public

Path	Path	Standard	P-Value	
ID	DV	Coefficient	error	
Agreeableness	Susceptibility	0.320	0.045	0.012
Susceptibility	Response	-0.342	0.064	0.000
Openness	Response	0.433	0.019	0.018
Usage	Response	0.126	0.029	0.032



Table 55: R square value - Public

	R square
Susceptibility	0.192
Response	0.172

Table 56: R Software results - MARA

Path		Path	Standard error	P-Value
ID	DV	Coefficient		
Manage	Susceptibility	0.120	0.023	0.012
Trust	Susceptibility	0.412	0.051	0.023
Openness	Susceptibility	-0.322	0.082	0.018
Susceptibility	Response	0.542	0.034	0.000
Trust	Response	0.223	0.032	0.015
Agreeableness	Response	-0.310	0.079	0.021
Openness	Response	0.232	0.027	0.000

Figure 30: Structural model for MARA group

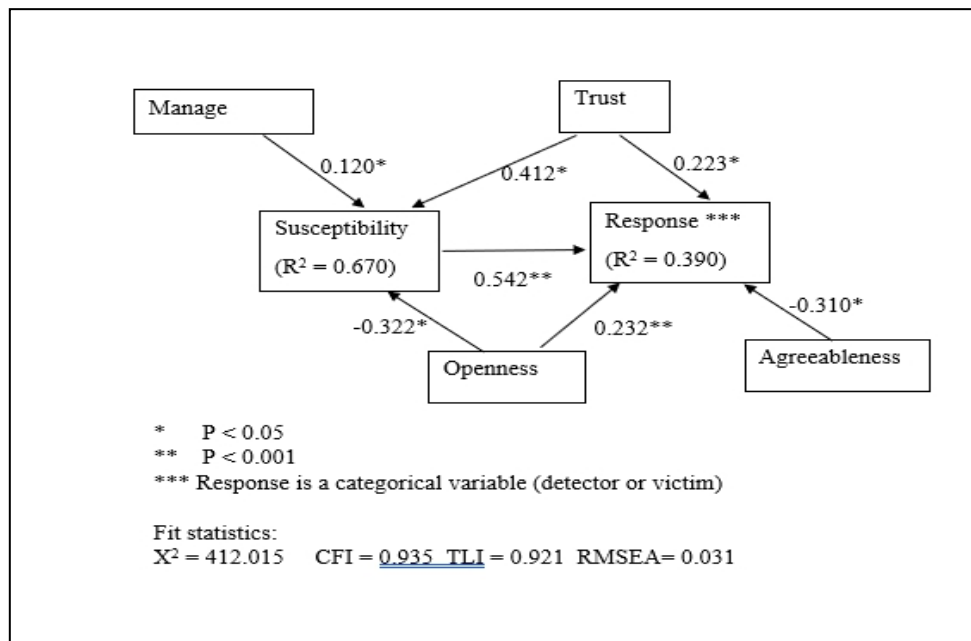


Table 57: R square values - MARA

	R square
Susceptibility	0.670
Response	0.390

## 5.5 Summary

We have discussed how we analysed the data for both groups in this chapter. The steps of analysis began with cleaning the data to be entered into the analysis software. Validity and reliability were tested in the first stage for each variable to ensure the final models' construct is reliable.

We also explained how we tested our hypothesis and proposed the final model. Hypothesis testing was conducted using multiple regression and logistic regression, while the final model was tested using R software with Lavaan Package.

The study for the Public group showed that users with a high level of agreeableness would increase their susceptibility to phishing emails from the final model. However, a high level of susceptibility does not influence users to respond to phishing emails. It can be seen by the negative relationship between response and susceptibility for the study. On the other hand, another two constructs are able to increase users' response to phishing as found in the model, which is Openness and Usage.

The result from the MARA model is able to show the positive relationship between susceptibility with the response to phishing emails. Moreover, the susceptibility behaviour increased by how the users managed the email and trust

behaviour but were negatively impacted by users' openness. Although openness has a negative relationship to susceptibility, it shows a positive relationship to the phishing email and trust behaviour.

## **Chapter 6 Qualitative Analysis**

The results from interviews with the victims and detectors are presented in this chapter in a qualitative analysis format. The primary purpose of this method is to gain a deeper understanding of why the victims responded to the phishing email and differentiate between the behaviour of detectors and victims.

This chapter begins with the introduction of the measurements used in the analysis on reliability and validity. Then, the process used to analyse the data is described. Finally, the results are presented and interpreted.

For the MARA group, we selected participants based on the matching IP address captured in the Google Analytics software (used to track click to email – see Chapter 4.3.2) with the IP registered under MARA business. Whereas for the public group, matching IP addresses were impossible to do. Alternatively, we selected and contacted the victims based on their response in the survey question asking for their password. A total of 13 participants agreed to be interviewed, where six of them were classified as victims and seven as detectors.

### **6.1 Reliability and Validity**

We measured the reliability of the interviews using Cohen's Kappa index of inter-rater reliability method (Carletta, 1996), which is often used to measure an

agreement between coders in qualitative research. Six of the interviews were analysed by two different coders. Both were provided with the transcript and interview codebook. The coding was designed based on prior topic categories that were derived from the MDD model. The results in Table 58 shows the level of an agreement satisfactory, K is above 0.7. The codebook is presented in Table 59. The validity of the findings was assessed by comparing them with the findings from the survey (i.e., data triangulation) (Eriksson & Kovalainen, 2011)(Sekaran, 2003).

Table 58: Inter-coder reliability

Participant	Activation	Hypothesis generation	Hypothesis evaluation	Global assessment
1	1	1	0	1
1a	1	1	0	1
2	1	0	1	1
2a	1	1	1	1
3	1	0	1	1
3a	1	1	1	1
4	1	1	1	1
4a	0	1	1	1
5	0	0	1	1
5a	0	1	0	1
6	1	1	1	1
6a	1	0	1	1

		b	
		Agree	Disagree
a	Agree	12	6
	Disagree	8	10

Pr(a):= [(Coder 1 agree & Coder 2 agree) + ( Coder 1 disagree & Coder 2 disagree)/all cases ]

And the equals 0.90

$\Pr(e) = 0.5$

$$k = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)}, \quad (\text{Galton (Francis Galton, 1893)})$$

$K = 0.80$

*The inter-coder reliability is satisfactory because  $k > 0.7$ .*

## **6.2 Analytic Procedure**

Most of the interviews were audio-recorded to ensure the interviewer not missed any important information. It was also done in both Malay and English language. All participants had no problems with the recorded procedure. Each recorded interview was transcribed in full, yielding 14 transcripts, with two or three pages for each.

The qualitative data were analysed in four phases. The first three phases were data reduction, data display and conclusion drawing (Miles, M.B & Huberman, 1994). The final phase is data interpretation, which integrates finding from the previous three phases (Silverman, 2006)(Silverman, 2011).

### **6.2.1 Data reduction**

Data reduction aims to segment the raw data into a manageable form so that researchers can transform it into their focused information. See Table 59 below.

Table 59: Codebook for analysis of the interviews

Phase	Activation	Hypothesis generation	Hypothesis evaluation	Global assessment
Description	Phase which user suspects they have been attacked by phishing email.	Phase in which user develops an explanation for the activation situation.	Refer to the processes that a user chooses to test their explanation.	The final decision a user makes based on the combined results from hypothesis evaluation.

### 6.2.2 Data display

Once the raw data have been organized, it is then presented into a table in which the participants were divided based on their groups (detectors and victims). Their responses were listed under each priori topic category. The data that could not be used and classified under any of the categories were grouped separately for further analysis (Braun & Clarke, 2006).

### 6.2.3 Data interpretation

The final phase in qualitative data analysis is interpretation, in which the results from each phase were integrated. At this phase, dominant and emergent themes were identified. From here, we identified the dominant theme for detector behaviour and victim behaviour, each of which contained several sub-themes. The

emergent themes were perceived email importance, communication between users, awareness of phishing email cues, and choosing the type of consult to be given.

## **6.3 Results**

We present the results obtained from the interview analysis in this section.

### **6.3.1 Detectors' behaviour**

From the analysis, we reveal three factors that are able to differentiate between detectors and victims. Those factors were concluded and can be seen in Table 60. Next, we categorised the answers as below:

*Negative consequences:* Detectors ignored the phishing email because they believed the email might cause harm to them.

*Knowledge about phishing email:* Detectors were able to detect cues in the phishing email. Knowledge of existent techniques used in phishing emails was able to help most of the detectors not respond to the phishing email. This is unlike the victims in this study who were unaware of the existing cues.

*Importance of the requested information:* Some of the victims ignored the cues because they thought the requested information was too important and the email was from a trusted sender. Table 60 below illustrates the level of responses from detectors when asked why they did not perform any action requested from the email.



Table 60: Detectors response

Code	Excerpt from transcript
The importance of the requested data	“I did not respond because I know my password is important and cannot be share with an unknown person.”
Low-level security behaviour	“I did not respond because, in my knowledge, it is the common request in the phishing email.”
Negative consequences	“I am afraid if my respond will bring more harmful email my inbox.”

Based on the responses, we can conclude that detectors felt more responsible for their email account by intentionally protecting their information and behaving securely. This also can be seen when they were asked to identify their source of knowledge about phishing emails. Some of the answers are:

- a. General publicity about the negative consequences of cyber threats.
- b. Attended awareness programs in their work associated to cyber-attacks, including identity theft.
- c. Personal experience when working with online applications such as websites, games, and emails gave insight into their weaknesses and the capability of these weaknesses to be exploited by attackers.

### 6.3.2 Victims behaviour

Most phishing email studies identify users as victims and detectors based on their final behaviour (i.e. respond or not). However, based on our investigation, we

classified victims into three types of victims based on users' detection behaviour. They are naïve victims, doubtful victims, and risk-taker victims.

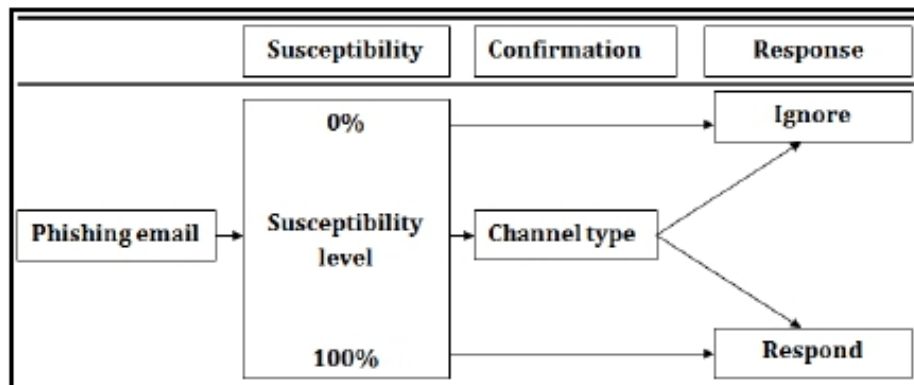


Figure 31: Users' action when dealing with phishing emails

### 6.3.2.1 Naïve victims

We categorise naïve victims as a person with almost no suspicion of phishing emails. Even though they believe in phishing emails, they cannot generate or evaluate the deception of the hypothesis. Significantly, they had no doubts about whether it was a legitimate email.

Table 61: Naïve Victims response

Code	Excerpt from transcript
No suspicion	“I have no doubts because the email looks like real email. Another email with no subject also made me think it came from a known sender.”
Trust	“I thought the email was for work and from an employee in the same organisation. Therefore I have no doubt because it comes from trustworthy organisation email.”

The findings in quantitative data also suggested that certain personality characteristics, including *Trust* and *Usage*, showed an increase in users' susceptibility and response to phishing emails. Thus, the results also support the findings from the interviews, whereas users with no suspicion is categorised under victims' characteristics.

### 6.3.2.2 Doubtful victims

Another type of victim is doubtful victims. This type of victims showed their suspicions but was unable to confirm it. Their weakness was that they lacked helpful information about phishing and were high in openness to the email. See Table 62 below for the answers from doubtful victims.

Table 62: Doubtful victim response

Code	Excerpt from transcript
Lack of previous knowledge	“As far I remember, I never received this kind of email characteristics before, so I have no experience in it”
Openness to new friends within the same organisation	“At the beginning, I have doubt, but in the end, I felt safe even I don't know the sender, but I am kind of open to making new friend.”
Managing emails	“It comes to my mind to ask my colleagues if they received the same email but I usually will do it after responding to the email.”

The quantitative data support these findings. The openness and managing email characteristics have a significant impact on users' accuracy in detecting phishing emails. Users who fail to manage the flow of their response to emails tend

to respond without getting confirmation in the first place. Their openness to making new friends and accepting any ideas without studying the sender's background were more likely to make them victims.

### 6.3.2.3 Risk-taker victims

Risk-taker victims choose to respond to phishing emails because they do not see any harm that may affect them in future from their actions. These victims did not lack the knowledge in phishing but were high in ignorance. They also believed that they could counter the event if the attack seems to occur continuously. Besides that, they want to see how the attacker wants to play with their strategy. The interview with the victims showed the answer as in Table 63 below.

Table 63: Risk-taker victims' response

Code	Excerpt from transcript
No important data to show	“The email seems will have a continuation from the sender, I want to see how the attack looks like, that is why I respond.”
My data is not important	“I believe my data is not important. My level of position does not show that someone wants to use me as a victim.
Knowledge in a phishing attack	“ I have experience in a phishing attack. None of the attacks will succeed if they ask the user password directly. I believe they more tricky than this. Therefore, I respond to see what will they do next.”

Our findings from the quantitative analysis were able to show a significant relationship between certain personalities such as agreeableness and openness to users' response to phishing emails. Users with a willingness to accept the experience

and new ideas fall under the agreeableness characteristic. Some users respond to challenge the attacker on the next move, which shows the openness of new experiences in victims who believe they can counter back if they use new ways later on. This is hazardous behaviour where failure in identifying new cues might cause more harm to the user.

### **6.3.3 Awareness of phishing email cues**

Phishing email education often aims to educate users on the importance of awareness to increase users' protection against attacks. From the qualitative results, we found that awareness alone cannot prevent participants from responding to a phishing email. A majority of the victims said they have heard and were aware of phishing email issues from social media and the Internet and have attended courses in the past. Table 64 shows the idea and specific knowledge about how phishing emails work and how detectors identify them, and why victims are unable to identify those emails.

Table 64: Awareness of phishing emails

Code	Excerpt from transcript
Participant 1 <i>Detector</i>	“I often received emails like the experiment email. I also get information from the news on the internet. It is maybe because I love to surf the internet and get the latest information about current issues in IT.”
Participant 2 <i>Victim</i>	“I heard about it (phishing email), but I am not interested in exploring more about it.
Participant 9 <i>Victim</i>	“I did attend a few courses about cyber security awareness, but unfortunately, my busy schedule made me sometimes careless and unaware.”
Participant 11 <i>Detector</i>	“I often received an email from our IT support department to warn us about the latest look of cyber threats including Spam and phishing email. It is the reason I do not respond to the email that looks suspicious.”

## 6.4 Summary

This chapter has presented the findings from the analysis of our qualitative data. The main factor that shows the difference between detectors and victims, such as knowledge and awareness about phishing cues, plays a vital role in users’ decision-making process.

Our findings were also able to identify three categories of victims:

- i. Naïve victims: Users who respond to phishing emails without suspecting anything.
- ii. Doubtful victims: Users who are suspicious of phishing emails but still respond to the email due to confirmation failure.

- iii. Risk-taker victims: Users who know the consequences of their action (respond to suspicious email) but still perform the action because they perceived it to be harmless.

Unlike victims, detectors demonstrated more responsibility in protecting their password and personal information by behaving rationally in any situation. We also found unexpected results where most detectors tend not to warn others about the threats they experienced and preferred not to take any action. However, some just warned the person closest to them.

## **Chapter 7 Discussion**

This chapter will summarise the findings of our research. It will begin with confirming the three main phases that detected users' behaviour and certain users' characteristics. Secondly, we summarise the differences between the two group studies (Public and Organisation, MARA). Lastly, we discuss the implications of our findings concerning strategies to improve users' protection against phishing emails. We also conclude the best recommendations for the organisation and personal in search of the best solutions to phishing emails problems for the victim, organisations and IT professional.

### **7.1 Summary of Findings**

The main objective of our research is to identify users' characteristics that affect the response and detection behaviour. Based on our results, several characteristics contributed to detection behaviour that differentiated between the detectors and victims. Figure 32 below presents an answer to our first question in our research (Q1) with the summary of the findings based on the three phases: susceptibility, confirmation, and response.



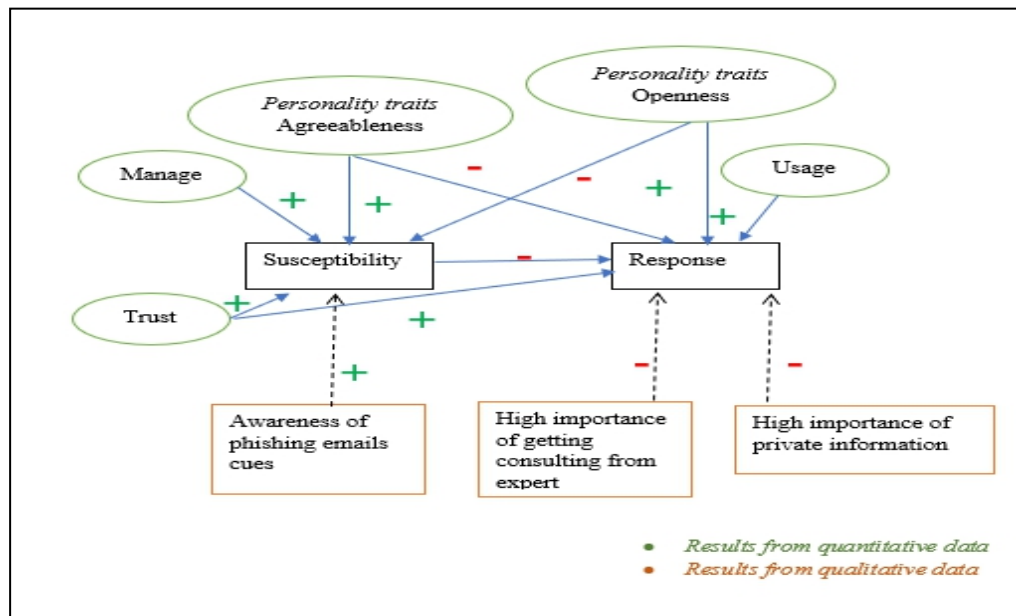


Figure 32: Impact of users' characteristics on response to the phishing email

Knowledge and awareness are key and essential in identifying phishing emails in order to reduce their susceptibility. This result also supports the finding from (Stembert, Padmos, Bargh, Choenni, & Jansen, 2015). The process of detection starts with an awareness of phishing email cues.

Email is a poor medium to present insufficient cues for reliable judgement. Therefore, users' characteristics are affected by susceptibility, where cues are another way to help users judge whether they face legitimate or fake emails. In other words, the more cues, the more chances of users to become a detector.

Phishing email cues will trigger detection and the process of identification. These cues require users' attention to certain features where some ordinary users may neither notice nor understand. At this stage, users with email richness (experienced user) are believed able to extract useful information.

Another two significant characteristics, Trust and Agreeableness, are believed to increase user susceptibility level. This is because phishing email attacks easily exploit both characteristics. Users with a high level of Trust and Agreeableness are more vulnerable to attacks as they are less questionable. Their trust somehow makes them reckless person in action.

High agreeableness in user character is another possible reason that increases users' susceptibility as they are likely to obey orders. Phishing emails always target users with high agreeableness character. They will make sure users will comply with the specified action request in the phishing email.

The second phase in detection behaviour is confirmation. Our findings from qualitative data showed that users are less likely to get confirmation from other resources before responding to phishing emails. Even detectors sometimes refer to one resource to get confirmation. This step is actually the best action to help users identify phishing emails and reduce the likelihood of responding to phishing emails.

The qualitative data also showed that the person suitable in consulting participants about phishing email detection is someone with appropriate knowledge, such as a server administrator or IT expert. For instance, server administrators are supposed to know whether the email was initiated from legit sources. IT experts, on the other hand, know how the tricks from attackers work. They can consult and warn authorised users about any potential attacks.

The third phase in the study is a response. We identified three personality characteristics from the quantitative results that contribute more to respond to phishing emails: Trust, Openness, and Usage. This supports the study done by (Tzipora, Lewis, & Memon, 2013) where she also found the relationship between

personality and response to a phishing email. She also suggested various phishing email design and types can play with personality. On the other hand, qualitative data provided additional insight by suggesting that the users are more influenced by the request information from an unimportant person and willing to take the risk of responding.

In conclusion, defence against email threats (phishing) require serious attention on all potential weaknesses in detection behaviour in users rather than concentrating on technical defence only. As our qualitative data showed, three types of characters in users make them vulnerable to phishing emails.

Other variables in this study, such as Cultural, Demographic and Internet experience, did not show any apparent difference in both studies. Only in the Public group, participants from cross-cultural backgrounds showed less vulnerability than the MARA group. This may cause by language, where English is not the first language for MARA participants. However, it did not show much difference in outcome for both groups when it comes to experience.

## **7.2 Comparison of results from MARA and Public groups**

Both groups were similar in design, where the first study is a survey that was used to collect information about users' characteristics and their level of susceptibility. In the second study, we recorded users' responses by sending them a few email experiments for the MARA group and analysed the responses for questions asking for users' password in the Public group. This stage provided the key differences between these two groups in a way to label users as victim or detector. In the final stage, we arranged and invited participants with the label as detectors and

victims to an interview to further study their unique characteristics. Even though culture is one of the key differences, especially when the experiment's geographical area exists, study culture differences are not our focus in the research. Therefore, it was omitted from our further discussion.

We conclude our result differences in both groups in two areas: the response rate (see Section 7.2.1) and the number of users' characteristics that had an impact (see Section 7.2.2). The number of victims in the Public group was significantly lower compared to the MARA group. In addition, fewer user characteristics were identified in the Public group than in the MARA group. We discussed the differences in the topic below. However, the results from both groups are able to support each other.

### **7.2.1 Response Rate**

The number of victims from both groups showed a significant difference. This can be seen from the MARA group which had 47 victims (25.9%) compared to the public group, where there were only 14 victims (13.3%). Two factors that might account for the differences are the perceived importance of emails in their daily tasks and user characteristics.

The first factor explained the terms of social presence and users' background. Knowingly, social presence has a direct relation with the ability to include interpersonal involvement for certain tasks (Miranda & Saunders, 2003). The contributing factors are as follows:

1. The background of the MARA participants required to use and work with email as their medium of communication contributes to the importance of

checking and opening emails in their daily activities. This is different from the participants in the Public group, where the background is varied. Some of them may not check their email daily.

2. Based on the experience of the researcher, who is one of the MARA staff, email is viewed as an alternative for any other type of bulletin board or memo, which email is compulsory to use and open during working hours.
3. Since the public group study using public email services, users seemed to be more courteous and aware of any cyber-attack. This mentality may not be the same as MARA users who place more trust in the emails under a private domain (in this case, @mara.gov.my). They prefer to put the responsibility on the IT administrator in order to monitor all threats.

The number of victims in MARA is expected to increase in the future, as emails become a more widely accepted communication medium since it is also easy to access using mobile apps. The increasing number of e-services among government agencies also shows users' importance to use emails in their activities. As more users connect to these services, the chances of users receiving phishing emails can increase. Therefore, appropriate action is needed to educate them not to fall victim to phishing emails.

### **7.2.2 Users' Characteristics**

Both groups did not show much similarities. This may be because of the difference in the environment of study. However, since our study is to try to see the users' characteristics individually, we do not consider the work environment differences that may jeopardize the research findings.

The characteristics from the email usage question show similar results for both studies. This includes the number of emails in users' inbox, the number of emails received each day, and the number of responded emails. The only difference for both is the number of important emails received daily. The MARA group showed a higher number of respondents who received quite a lot of emails compared to the Public group users.

When it comes to Trust, Usage, Manage, and Susceptibility, the MARA group, was able to show more sensible results. For instance, the MARA respondents showed a high level of trust in emails, with a mean score above 4.50 for each question given. Unlike MARA, the public respondents lack in trust level on emails with a mean score below 3.00 for all questions. The sensible reason is that MARA participants do not have any other choice besides using email in their daily activities in the workplace. This is supported by the high score result in the question from the Usage section area where ("email is easy to use") and manage ("my email use is effective") for the MARA group. Each staff must have an email account when they work with the company as it is believed to contribute to a comfortable feeling when using emails. Undoubtedly, this is a strong reason for them not to change from conventional to a new communication technology such as WhatsApp and Telegram applications that can provide almost similar functionalities like emails.

On the other hand, public respondents show high susceptibility when responding to an email from system maintenance. This is different from the MARA respondents who showed susceptibility to the email from PayPal. This latter observation is accounted for because most respondents from MARA have secure monthly incomes that enable them to shop online or use PayPal.

Both groups have no differences in the number of emails received, responded to, sent, and email number in the inbox regarding email and Internet usage questions. The only difference is the number of important emails they received each day and the time spent using the Internet. The MARA respondents had spent more time (9 hours) using the Internet than the Public respondents (5 hours). This latter observation is accounted for because the MARA participants were working for up to 8 hours a day.

Results for Big Five personality dimensions showed that both groups have one similarity in the result. Respondents from both groups show that they are agreed to have more Agreeableness character. Additionally, each group has another extra major character: Extraversion for MARA and Conscientiousness for Public. However, both groups also agreed that they are also Sympathetic and Warm, and Conventional and Creative. Previous research by (Wright et al., 2010b) suggested that users who were able to detect phishing emails score highly in conscientiousness. It has been shown to correlate with the increased susceptibility to phishing emails in the Public group.

It is rational to conclude that culture does not affect users' ability to detect phishing emails. Nevertheless, to some extent, culture can directly impact users' characteristics, and these characteristics directly impact users' ability to detect phishing emails. For instance, the ability to spot English language spelling mistakes in a non-speaking English culture is a big challenge. Identically, certain personality traits are more dominant in some cultures than others. Both groups showed that agreeableness increases users' vulnerability to phishing emails, and having a sympathetic and warm personality besides a conventional mindset limits their ability to explore modern and the latest social engineering threats. This is also supported by

research done by (Srivastava, John, Gosling, & Potter, 2003) where Agreeableness increases throughout early and middle adulthood.

## **7.3 The implication of findings for defensive strategies**

This section will discuss the implication of our findings to develop defensive strategies to increase users' ability to detect phishing emails.

### **7.3.1 Focus on email content tricks**

Users who cannot spot the cues are more vulnerable to threats. Furthermore, a study using eye trackers technology for users with IT and technical background also found that they need more time on email content to judge the metadata of the email's authenticity (Pfeiffer, Theuerling, & Kauer, 2013a). As discussed in Chapter 2, phishing emails usually are designed to imitate legitimate emails to conceal deception and gain trust from the users. According to (Dong et al., 2008), the main weakness in victims is the failure to judge the email's legitimacy. This is the strong relationships in our findings which showed that this weakness is associated with the main characteristics that can increase users' susceptibility to phishing emails. The characteristics are trust, agreeableness, and openness.

Users with high trust and agreeableness are more vulnerable to phishing emails. Changing personality characteristics is complex and challenging but not impossible if done correctly through systematic education. The results might not be able to be seen immediately but may be able to reduce the effect of the submissive personality.



Knowing that users with high agreeableness are more likely to follow instructions, hence direct instruction to protect their private information from trusted sources can increase their protective behaviour (Wright et al., 2010b). Therefore, the best strategy is to use the users' characteristics weaknesses, such as using suitable authorities to give an order to the user with high agreeableness character. Using this way can increase their trust level and make them obey the order from the trustee. This may not only reduce time to educate the users but indirectly can reduce management cost.

Experience in working with emails has been shown to decrease users' vulnerability. This is because users who have more working experience with emails can extract more cues than those who are new to email technology. However, the years of working with email cannot guarantee the efficiency for users to detect cues in phishing emails. This is due to how often the users' face new and different types of emails. The knowledge that comes from email richness can give the users more experience in detecting cues to avoid becoming victims.

However, our qualitative results showed that users with knowledge of phishing emails are still unable to use their knowledge to identify phishing cues. This has resulted when both victims and detectors are said that they are aware of phishing emails but did not know how to identify them. Security knowledge, on the other hand, does not show a significant impact on detection ability. There is also less effort from users to confirm the legitimacy from other sources, causing no alternative way to warn them about phishing emails.

### **7.3.2 Inability to detect cues**

Observing inconsistent cues is an essential aspect of the detection process (Burgoon et al., 1996). In phishing emails, users need to observe the inconsistency cues in the email by referring to different types of resources and opportunities available. For instance, users may validate the legitimacy of the email they received by consulting with an IT expert or doing some research about the email sources.

Failure to confirm and validate the legitimacy of the email can increase the chances to become a victim. Besides, the initiative can increase users' knowledge about phishing emails and increase their chances of becoming detectors.

From the results, we found that the person who gets consulted from their friends can also impact the chances of becoming a victim. The possibility happened when they get consulted from a friend only, who is also the potential victims. Ignoring the warning from the experts make them reckless and unable to authenticate the legitimacy of an email. On the other hand, those who consult the detectors can avoid becoming victims since they received the correct information.

### **7.3.3 Inefficiency in dealing with emails**

The factors that contribute most to user weakness are requested information types and the users' personality.

The type of requested information plays an important role to differentiate between detectors and victims. Victims show low importance in protecting their passwords and are less concerned about losing their information. This can be seen in our qualitative results where some of the victims responded to the phishing email

because they did not think the email may harm them. Moreover, some of the victims knew about phishing emails and had experiences of being attacked in the past. This shows that previous experience does not teach a lesson in not engaging from being attacked again.

This is supported by certain personality dimensions that contribute to users' response. The survey identified three dimensions: Openness, Extraversion, and Agreeableness, which can contribute to users' responses. Users with openness usually are more adventurous and love to explore new experiences. This personality can cause them to become eager to know what will happen based on their action. This personality contributes to the potential risk involved. The extraversion personality embedded in users' behaviour makes them more sociable and easier to interact with others. This behaviour encourages the response to phishing emails. On the other hand, agreeableness discourages suspicion with the requested action and provides an excellent combination to increase users' risk-taking behaviour of becoming a victim. Besides that, this behaviour can be addressed by raising the stakes for risky action (Burns, Durcikova, & Jenkins, 2012).

## **7.4 Recommendations**

Our recommendations focus on the victims, security aid designers and organisation. Each will be discussed as below:

### 7.4.1 Victims

Earlier, we identified the victims based on three types: naïve, doubtful and risk-taker victims. Each type has its own vulnerability to susceptibility and phishing emails.

- a. Naïve victims: The vulnerability for naïve users comes when they fail to observe and interpret the cues in the first place. Zero-knowledge and unawareness of threats are the most common reasons for this type of victims. Their naïve characteristics increase their susceptibility level. This type of users requires training or programs to increase their awareness and knowledge about social network threats, especially phishing emails.
- b. Doubtful victims: This type of victims need to choose the right person or resources to consult before deciding. Working together with an expert and doing further research to overcome their doubtful feelings can help them not become victims and increase their knowledge about current threats.
- c. Risk-taker victims: Users with this type of characteristics are usually those with a strong belief that their actions will not harm them. The belief will increase when they experience success from their actions in the past. Thus, they will continue with their low-security behaviour. In order to cater and improve defences, they need to change their perception about attackers and aware of the impact of their actions which will affect not only them but also other users.

### **7.4.2 Security aid designer**

Limitations such as short lifespan of phishing websites, from hours to days only (Moore & Clayton, 2007), and the limited ability of security tools to prevent phishing attacks on day Zero (B. B. Gupta, Tewari, Jain, & Agrawal, 2017) (Aniket & Sunil, 2018) make it hard for the available tools to cope with the new attacks every day. For instance, email filtering tools like machine learning requires the algorithm to learn from a specific number of samples before it can warn users about the threats. The inability to get enough samples can reduce the efficiency of the system. At this stage, we suggest the involvement of users to detect phishing emails in the early stages in order to help discovery for the tool designer.

### **7.4.3 Organisation responsibility**

Organisations play an important role to their staff in protecting them from being a victim of phishing attacks. Implementing the latest and updated security tools is the standard action to protect employees and prevent phishing emails from reaching users. However, nowadays, using tools cannot guarantee 100 per cent protection to the employee. Many of them are still fall for victims (Williams, Hinds, & Joinson, 2018). Therefore, organisations need to find new ways of improving protection.

Based on our qualitative results, some of the victims revealed that they had attended training about security awareness a few years ago provided by their organisation. A study done by (Kumaraguru et al., 2009) also showed that a higher percentage of participants who can identify phishing emails come from the users categorised as a trained user. In addition to that, (Yang et al., 2017) also found that

training embedded in e-mails with text and graphic notes about phishing is more effective than traditional security notification. This is because users need new updates about threat frequently to discuss and share information about the threats and security while attending the training with their peers, which will improve their awareness level and protection against security attacks.

Organisations should enhance the information delivery system for their employees and encourage them to use this system as a channel to warn them about any possible attacks. This includes facilitating the system with the reporting function from users. With this function, those detectors who address any attack cues in the first place may report to IT support. This helps the IT support to protect the network and build more robust protection without increasing the security cost. Based on our experiment, none of the participants reported the attack to IT support. Some of them said, i) they did not know the channel to report, ii) they were afraid that they are wrong because they are not an expert, and iii) they did not think they should involve other departments. Besides that, they did not have a strong relationship with the security department. There is strong evidence of the importance of the relationship between employees in any department with the security department. We also suggest the organisation highlight the importance of reliable consultation services that everyone can access anytime in the organisation.

Organisations should take the opportunity to work with detectors. Users who are able to detect or discover phishing emails should know the pathway to report an event to the relevant authorities. The authorities then should be responsible for issuing warnings to other users. Early detection does not only reduce the response time. It saves much money from spendings on the recovery process, such as resources damage, staff psychology treatment, IT expert hire, and client trust loss.

The most significant impact to the organisation is the “loss of client’s trust”. Lost of trust in the organization threatens handling capability not only jeopardizes the reputation but may impact their revenue.

## **7.5 Summary**

We concluded that detection behaviour is comprised of three phases where each phase produces a different impact on users. The users’ behaviour is the action from specific characteristics that differentiate between victims and detectors. Awareness of these relationships can help the organisation to increase its protective strategies. The findings from the studies supported our developed research model by explaining users’ detection behaviour . Furthermore, the study was able to identify the weaknesses in detecting phishing emails and suggest ways to improve strategies and security tools in future for organisation and developers.

## **Chapter 8 Conclusion**

Chapter 1 of this thesis presents the research problem under investigation. Chapter 2 presented a critical review of the literature and identified the gaps in knowledge about the topic. The causal model that was developed to guide the investigation was described in Chapter 3. The design and methodology used to test the model were explained in Chapter 4, while Chapter 5 and 6 discussed the analysis and results from the quantitative and qualitative data, respectively. The results and the implications for addressing phishing emails strategies were discussed in the following chapter, Chapter 7. The chapter is first presenting the summary of the findings concerning each of the research questions. The recommendations for best practices and future research direction are highlighted in this chapter (Section 7.4). Finally, the summary of the main practical contributions of the thesis, suggestion to organisation and user, and the discussion of the study's limitations was concluded in Chapter 8.

Our main findings can be summarised as, a) Users' detection behaviour has three main phases called susceptibility, confirmation and response; b) Users' characteristics have a significant impact on detection behaviour; c) Personal factors such as background and managing email impacts users' ability to detect phishing emails; and d) There is no single solution to the phishing email problem for a single type of victim. Therefore, the strategies need to target specific vulnerabilities and weaknesses.



## **8.1 Academic Contributions**

The main academic contributions of our research are:

1. Developed a model that is able to examine the entire process of users' detection behaviour and identify the weaknesses in their behaviour.
2. Used quantitative data to identify the impact of users' characteristics on the detection of phishing emails. The impact can be classified as a) the impact of trust, manage and openness on users' susceptibility and b) the impact of personality traits on users' response.
3. Used qualitative method to identify additional factors that affect different phases in the model.
4. Identified the categories of victims by using the interview with victims approach in Study Three.
5. Demonstrate the impact of users' personality and activity on users' ability to detect phishing emails.

## **8.2 Contribution to Practice**

Our main contribution is to develop practical strategies in addressing the problems related to phishing emails detection behaviour and their vulnerabilities. The related phases are susceptibility and response.

### **8.2.1 Susceptibility**

Educating users about phishing email cues to improve their ability to prevent them from becoming victims has been discussed in various studies. The ability to

spot cues can alert users on the potential dangers (Fette, Sadeh, & Tomasic, 2007b)(Dewan, Kashyap, & Kumaraguru, 2014). Our data supported this finding by identifying the two characteristics and one behaviour of users' that should be concentrated on to decrease their susceptibility (see Section 7.3). The related characteristics are Trust and Agreeableness, while the behaviour is on 'managing emails' capability. Trust in email is a major weakness in users' characteristics. Therefore, users should be trained on dealing with phishing emails that can impersonate any organisation and individual. Agreeableness is the other characteristic that increases users' susceptibility to phishing emails. The primary issue in Agreeableness and Manage is to be authoritative in control and the inability to warn users about deceptive behaviour in the first place.

#### **8.2.1.1 Trust in email.**

Users usually Trust email and have a high confidence level to use it as a modern communication medium. It is due to the features of the email systems and the email provider's ability to provide the system with the latest security services that are believed to effectively protect information. Some of the examples of service provided by email providers are:

- a. Proton Mail- is an open-source email service protected by Swiss privacy law and has end -to -end encryption.
- b. Microsoft outlook- is a browser-based email service with the operation is entirely online exchange.
- c. Zoho Mail - most secure and add free email hosting service tailor-made for the company's communication needs. It is clean and fast and offers protection against fake emails.

- d. Hubspot mail- focused on the use of existing templates according to the need. The email is easily customized by using drag and drop.
- e. Gmail- Gmail using third-party programs that synchronize email details through IMAP or POP.
- f. iCloud Mail- Provide by Apple. iCloud Mail loads automatically the HTML images.
- g. Yahoo Mail- Provide large email storage capacity to the user. This is useful for people who transfer big size of data such as image and video.

Therefore, users and organizations need to choose the email service that meets their usage needs wisely. User can not depend on and trust the service provider and the IT specialist alone. User should be trained to deal with tricks in the world of email wisely. They need to learn to control such beliefs' characteristics by obtaining certainty from various sources and not believing in one source. The ability of the internet and the existence of websites and software, either paid or free, can be used to access information and check the legitimation of email. For example, Verifalia, snov.io and the website 'verify-email.org' can help users verify the validity of emails received. It is the best way to reduce the user's probability of being susceptible to attack with extra precaution steps.

### **8.2.1.2 Agreeableness**

Agreeableness is another users' characteristics that found can increase users' vulnerability to phishing emails. Agreeableness is a personality trait that best

to described as cooperative, polite, kind, and friendly. People high in agreeableness are more trusting, affectionate, altruistic, and generally displaying more prosocial behaviours than others (P T Costa & McCrae, 1992). They tend to exaggerate the will of others over their own. If seen, it is very much related to the nature of the Trust characteristics, as stated earlier. The only difference is that the Agreeableness users' is more 'we-centric' than 'me-centric', while the Trust users' has no preference for selection.

Furthermore, agreeableness users' satisfaction can be obtained by fulfilling the desires of others. They are also less likely to say NO to others. This attitude is hazardous because it can have a harmful effect, especially on meeting hackers' needs.

Although being empathetic is a good attitude. Therefore, to ensure good attitude in agreeableness is not misused by posing a threat, this attitude needs to be addressed effectively. This is because those with this characteristic often struggle to assert their wants, needs, and preferences. They often struggle when the situation requires tough decisions.

There are several things taught in psychologist books to deal with high quality of Agreeableness person. Among the things that can be practised in the organization are:

- a. Provide training that teaches the user to always think before answering. This is to ensure that it becomes a routine and a principle in themselves by taking the time to think about all decisions rationally before taking action. Furthermore, based on research by (Williams et al., 2018) they said that Context-specific factors in emails are also likely to impact employee susceptibility in the organization.

- b. All matters given to them must be in writing or via email. High agreeableness employees often say 'yes' without thinking about the task given. In fact they also easily forget what answers they give. Giving a request in writing will allow them to think of their answer. Therefore, all warnings and instructions for the correct action to manage email threats should be given reminders by memo or email from time to time.

With both actions above, it is not impossible can reduce user susceptibility to attack. This is very important because, based on the latest statistics from (Mimecast, 2021); 52% of ransomware victims paid threat actors ransom demands.

### **8.2.1.3 Managing Email**

Our study found that weakness in managing email is another factor that causing the user to be vulnerable to email. Email management is often taken less serious by users because they often think everything will be handled by the email service provider or the email software tools purchased or subscribed by the organization. However, according to the same statistic report ( Mimecast,2021),79% of companies still lack security preparedness. Therefore, relying on this tool only does not guarantee the user's safety, especially with various new types of emails borne today.

One of the best measures is to provide consistent helpdesk services and training to users and employees on handling email more efficiently and securely. For example, as a service provider, it is necessary to provide easily accessible assistance services for all levels of users. An employer needs to provide training to employees through a physical or a practical and complete user manual according to the features

of email services owned by the company. This is because each company may use different tools. Continuous knowledge and updates about the current system and threats are necessary to guarantee the effectiveness of email services and reduce mismanaging of the email features.

## **8.2.2 Response**

They reply to phishing emails because they want to do it. This is believed to be because of some of the personality traits present in user that motivate them to respond (see Section 7.3). The attitude that we identified that influence users to become ignorance to cues is Trust and Openness. Often this attitude can produce negative consequences following their actions.

### **8.2.2.1 Trust**

Similar to the discussion of trust in section 8.111. The trust attitude exists due to users' dependence on the effectiveness of email applications and their organization. The attitude that fully trusts other things and neglects self-responsibility makes users and employees susceptible to threats.

### **8.2.2.2 Openness**

Openness attitude is good in terms of social interaction. According to (DeYoung, Weisberg, De Young, & Hirsh, 2011), openness is best explained by:

“Openness/Intellect reflects imagination, creativity, intellectual curiosity, and appreciation of esthetic experiences. Broadly, Openness/Intellect relates to the ability and interest in attending to and processing complex stimuli.”

People who have high openness tend to seek new things and experiences. Openness to experience also tends to be correlated to another psychological trait known as absorption, which involves the ability to become immersed in imagination or fantasy. This construct may also be linked to hypnotic susceptibility or the tendency to be hypnotizable (Y. Zhang et al., 2017). Despite the benefits of having openness attitude, there is also a downside of the attitude such as:

- a. The attitude of love for something interesting makes them easy to get involved in risky behaviour. They tend to challenge themselves without thinking about the effect of their action.
- b. People who are high in openness tend to be more informed about sexual relationships, have a more open attitude toward sex, and want to have more sexual experiences (Meltzer & McNulty, 2016). The possibility of people with this trait becoming bait of phishing using sex attractive modus is very high.

### **8.3 Types of Victims**

Based on our findings, there is no single type of victims. Therefore, we categorised the victims into three categories: naïve victims, doubtful victims, and risk-taking victims. We discussed each type of weaknesses in Section 7.4.

To summarize, naïve victims have almost no suspicions about an attack. These victims are vulnerable and will respond to the email directly. Raising awareness and knowledge about phishing emails and security tools is believed to be the only way to help develop safe behaviour and reduce the chances of responding to

phishing. Naive victims fall prey to phishing emails because they have a high level of susceptibility in the first phase.

Unlike naïve victims, doubtful victims have sufficient awareness of phishing emails, but they fail to confirm their suspicions or are high in a trust personality trait. This happens typically in the second phase of detection behaviour. They cannot seek confirmation for their suspicious feelings and are prone to trust the minimal information given in an email. Their level of protection would be increased by providing them with enough technical support and information to answer their suspicions. This confirmation can produce an immediate response to work with their trust personality trait.

Risk-taking victims have less secure behaviour by responding to phishing. This personality engages them in dangerous behaviour. The personality is not only able to harm themselves but also others. People with risk-taking behaviour are likely to ignore any warnings and are more selfish. Their high openness to new experience trait may cause a higher potential loss. In addition, these victims do not attach high importance to protecting private information and lack of integrity sense for their organisation. We discussed the potential strategies for organisational and individual to protect against attack in the next section.



## 8.4 Propose Strategies and Techniques

In an organization, the management is responsible for ensuring that employees can carry out a given workload and does not neglect the organisation's security against cyber threats with their actions. At the same time, individual or public email users', they still need to increase their self-awareness about cyber threats. Cyber threats, especially phishing email, are not focusing on attacking business email only. They also targeted public email account users with various other goals rather than business email compromise.

Hackers strategies to lure public email user and making them victims is still a success today. This can be seen by the number of cases or incidents of users fell to phishing email is still high (MyCert, 2020). According to the same report, the number of reported cases increased when the Covid-19 Pandemic occurred in 2020, where most people were required to work from home. Employees are unable to rely 100% on the organization's email security system. Their devices are now in the range of potential insecure environment.

The public is now very panicked with the Covid-19 situation that has hit. This can make them vulnerable to the probability of a new form of attack by hackers. It is because hackers like to use current issues to make a profit. For example, creating fake pandemic funds for pandemic victims, creating spear phishing links to the deceptive pandemic information websites. Therefore, in the current situation, whether we are the public or employee of an organisation, the responsibility to protect our confidential information is in the user itself—users' need to equip themselves with knowledge as much as possible. With enough knowledge, user can reduce their chances to become vulnerable to attack.

### 8.4.1 Training

In the face of these phishing attacks, employees have become the frontline of cybersecurity. Reducing their vulnerability to phishing emails has therefore become a critical challenge for companies. The International Organization for Standardization/International Electrotechnical Commission information security standard ISO 27001 Clause A.7.2.2 requires every organization to provide adequate training and knowledge to an employee. A study done by (Singh, Aggarwal, Rajivan, & Gonzalez, 2019) found that giving phishing email training to users can increase their confidence in dealing with a phishing email. While, (Tschakert & Ngamsuriyaroj, 2019) results show that awareness training can increase user confidence and reduce false-negative click. They also suggest that proper practical training by using various learning techniques such as video games, tutorials, and simulations will help different user preferences.

Besides the common awareness training, there are several additional measures in addition to those described in section 7.4.3. Organizations may consider doing different types of training.

- i. Training employees to be able to spot phishing emails.

User preference in learning is vital to make sure they are willing to learn and not struggle to learn. This is also to ensure the effectiveness of the lesson, which can contribute to behaviour change as required. As discussed in section 7.3.2, the inability to detect phishing cues is one of the main contributors to becoming victims.

To ensure the effectiveness of training, various methods have been done. For instance, training using phishing email simulations, one to

one staff training and even computer-based training (Tschakert & Ngamsuriyaroj, 2019) . However, according to (Proofpoint, 2020) the effectiveness of the training provided is still not showing the ability in reducing the number of victim to date. Something that we might overlook in training is ‘knowing the training participants’.

So the best way is not by training users at random but by identifying those users. Users need to be categorized into different categories to suits the training with users. For example, categories user by;

a. Knowledge

The main reason for awareness training is to equip users with appropriate knowledge about information security. Knowing a person's existing level of knowledge before they follow the training can prepare the instructor to see things that the user does not yet know. This is to ensure that no information is misrepresented to the user at all level.

The user's experience with email phishing is also important in order to know whether the user has ever been a victim or not. If the user has been a victim before, the cognitive level plays an important role in avoiding being a victim for a second time. It is different from those who have never been exposed to phishing. They need more varieties sample of phishing emails in their training session.

b. Personality

Knowing the personality of the user is one of the best ways to categorize the training. This is because the training content and the trainer choice can be adjusted according to the participants' characteristics. For example, those with an Openness personality need to be trained to be smart, not hasty and careless in making decisions ( as discussed in 8.2.2.2). At the same time, trainers to extroverts user should be wise in re-directing them to the training topic. Extrovert user must be giving a chance to be delightfully surprised by new and unexpected conversations with others. The trainer is suggested to speak with their native language and learn how to white lie because it is hard for an extrovert to accept others views.

Identify user personality using the big five personalities is also part of the objectives in this study. We want to see the relationship between users' personality/attitude and their actions to phishing emails in order to provide appropriate training. Another study that is also looking at the importance of understanding employee attitude to provide better planning was done by (Ashenden, 2018). Therefore, we believed that effective training is the best socio-technical aid against threats rather than using technology defence capabilities entirely support by (Osatuyi et al., 2018)(Ashenden & Lawrence, 2016).

- ii. Embed Cybersecurity awareness as culture.

All key personnel in the organisation must make cybersecurity issue an agenda for everyday tasks. It will make an employee understand the importance of preventing threats. The activities such as a) continuously create awareness bulletin, memo and messages b) create cyber awareness posters and advertisement that give information about the impact of the attack to an employee in organization and public; .c) organize the cyber awareness day where experts in this field can have a dialogue with people and provide the latest information. Indirectly, it will teach people to make awareness to threats as a culture of their lives and strengthen the human firewall either at work or outside the workplace.

#### **8.4.2 Reward**

Everyone loves to get a reward. A reward is given to show our appreciation for all the good that has been done. Rewards are not necessarily in the form of valuables gift but can also be in the form of certificates of appreciation and acknowledgement. Moreover, Positive and public acknowledgement will help spread good behaviour in user.

A reward is an alternative for the authorities, management in the organization, or the government to tackle user willingness to report any cyber threats event. It can also help obtain useful information about the attacks and create suitable types of system defence, which is usually challenging due to a lack of data. Therefore, a Cybersecurity Defence agency for every country must provide a platform for

reporting the event. For example, Cybersecurity Malaysia has created a ‘cyber999 line’ to help users detect, interpret, and report the incident to the authorities.

### **8.4.3 Disciplinary Measures**

Disciplinary action varies between organizations and countries. It depends on the policy and the act used. Disciplinary action is seen as a rough action against the individual, and it is advised to be the final action taken after the failure of all other efforts. In certain circumstances, employee disciplinary measures may be appropriate, especially for those who fail to follow cybersecurity precaution for more than one time. However, care must be given to the penalty given. The penalty must be tailored to the mistake made. This is to ensure that it does not cause a significant decrease in productivity due to emotional disturbance, which may also cause a long term effect.

Employer or authority may come out with different stages of warning and penalties to the offender. This is to see how effective those penalties to them. For example, the employee can be transferred to a less risky division (not handling important data) against his negligent actions for their repeated misconduct. This ensures that no major risks occur while awaiting changes in employee behaviour on the safety training provided.

As public users, the authorities often give warnings through social media, TV and radio regarding the law action that can be taken against their cyber misconduct. For example, the Communications and Media act in Malaysia, violating the consumer code of practice to cause problems to the public, can be prosecuted for up to RM10K. In Singapore, consumer negligence, whether intentional or not resulting in loss of company assets, can be fined not more than \$ 5 k and imprisoned not

exceeding ten years under the Computer Misuse Act. In the United Kingdom, however, employees generally need to be warned in advance that failing to comply with the employer's cybersecurity measures may have disciplinary consequences up to and including termination of employment.

Employment law is different between a country according to the culture and beliefs. It also needs to be revised from time to time based on its suitability with the users, technology and even cultural development in that particular country. The effectiveness of penalties and actions taken to prevent from becoming victim to the cyber threat should also constantly be reviewed by an authority.

In conclusion, users can increase their protection against email threats in many ways. Yet, it still ended with their willingness and desire to learn and strive to change their attitude to become more responsible person. The attitude to not relying on technology alone must exist in them. This is because every action taken is depending on the user decision. Psychologists often state that a person's personality cannot be changed. However, according to recent research by (Bleidorn et al., 2019)(Krueger et al., 2018), 'through effective intervention, personality traits can be changed' by training to a better direction.

## **8.5 Limitations of Study**

Our research on phishing emails tried to imitate the behaviour of real phishing emails and design incorporated features that are commonly used in most phishing emails (see Section 4.3.4). However, in real life, users are exposed to more types of phishing emails than we tested. Even though we were unable to include all

these features in our design, the main design features in our research are most commonly used in phishing emails now and will continually be used.

The second limitation of the study is the age of participants (18 and above) for the MARA group but no limitation in the Public group. In real life, phishing emails can reach any user as long as they have an email account. Younger users are believed to be vulnerable to phishing due to less knowledge and experience and frequent Internet usage compared to older people. Even though our study was unable to show the relation of experience and age in email use with the response to phishing, a previous study (Sheng et al., 2010) found that people within the ages of 18-25 were more likely to fall for phishing than people in other group age categories. The author also speculated that this is due to a few reasons; a) a lower level of education, b) less experience of using the Internet, c) less exposure to training materials, and d) less aversion to risk. Therefore, there is not enough evidence to support the theory that requires us to discard age from further study.

The third limitation is that the study only used the approved email account given by the MARA organisation with restriction (see appendix C). The attached tracking source code in the email was also with limited functionality (capture click and open email). This is due to corporate policy and privacy terms to corporate domain users. However, we managed to track the click to indicate the users have been deceived and hence warrant identification as victims. The different ways to identify the victims between the MARA and public users were also limitations in our study. However, the result of construct reliability from the survey overcame the validation of the result.



## References

- Aburrous, Maher, M. A. Hossain, Keshav Dahal, and Fadi Thabtah. 2010a. "Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies." *Cognitive Computation*.
- Aburrous, Maher, M. A. Hossain, Keshav Dahal, and Fadi Thabtah. 2010b. "Predicting Phishing Websites Using Classification Mining Techniques with Experimental Case Studies." in *ITNG2010 - 7th International Conference on Information Technology: New Generations*.
- Acquisti, Alfssandro and Jens Grossklags. 2005. "Privacy and Rationality in Individual Decision Making." *IEEE Security and Privacy*.
- Ajzen, Icek. 1991. "Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes. The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50(2):179–211.
- Akbar, Nurul. 2014. "Analyzing Persuasion Principles in Phishing Emails." (August):105.
- Ali Hussein Alkahtani, Ismael Abu-Jarad, Mohamed Sulaiman & Davoud Nikbin. 2011. "The Impact of Personality and Leadership Styles on Leading Change Capability of Malaysian Managers." *Australian Journal of Business and Management Research* 1(2):70–99.
- Almomani, Ammar, B. B. Gupta, Samer Atawneh, A. Meulenberg, and Eman Almomani. 2013. "A Survey of Phishing Email Filtering Techniques." *IEEE Communications Surveys and Tutorials*.
- Alowibdi, Jalal S., Ugo A. Buy, Philip S. Yu, and Leon Stenneth. 2014. "Detecting Deception in Online Social Networks." in *ASONAM 2014 - Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*.
- Alseadoon, Ibrahim, Taizan Chan, Ernest Foo, and Juan Gonzalez Nieto. 2012. "Who Is More Susceptible to Phishing Emails?: A Saudi Arabian Study." *23rd Australasian Conference on Information Systems (Trusteer 2009)*:1–11.
- Alsharnouby, Mohamed, Furkan Alaca, and Sonia Chiasson. 2015. "Why Phishing

- Still Works: User Strategies for Combating Phishing Attacks.” *International Journal of Human Computer Studies*.
- Anandpara, Vivek, Andrew Dingman, Debin Liu, Heather Roinestad, and Markus Jakobsson. 2007. “Phishing IQ Tests Measure Fear, Not Ability.”
- Anderson, D. Eric, Bella M. DePaulo, Matthew E. Ansfield, Jennifer J. Tickle, and Emily Green. 1999. “Beliefs about Cues to Deception: Mindless Stereotypes or Untapped Wisdom?” *Journal of Nonverbal Behavior*.
- Andy Field. 2009. “Discovering Statistics Using SPSS Statistics.” *SAGE Publications*.
- Aniket, Bhadane and B. Mane Sunil. 2018. “State Of Research On Phishing And Recend Trends Of Attacks.” *I-Manager’s Journal on Computer Science*.
- Arachchilage, N. a G. and M. Cole. 2011. “Design a Mobile Game for Home Computer Users to Prevent from ‘Phishing Attacks.’” *International Conference on Information Society, i-Society 2011*.
- Babbie, Earl. 2001. *The Practice of Social Research (9th Ed.)*.
- Bachmann, Duane, John Elfrink, and Gary Vazzana. 1996. “Tracking the Progress of E-Mail vs. Snail-Mail.” *Marketing Research*.
- Balakrishnan, Vimala, Shahzaib Khan, Terence Fernandez, and Hamid R. Arabnia. 2019. “Cyberbullying Detection on Twitter Using Big Five and Dark Triad Features.” *Personality and Individual Differences*.
- Bandura, Albert. 1986. *Social Foundations of Thought and Action: A Social Cognitive Theory*.
- Baoshan, Ge and Yu Dongming. 2009. “Social Capital and Cognitive Bias: An Empirical Study of China.” *Proceedings - 2009 IITA International Conference on Control, Automation and Systems Engineering, CASE 2009 266–70*.
- Basnet, Ram B. 2014. “Learning To Detect Phishing URLs.” *International Journal of Research in Engineering and Technology*.
- Baumgartner, Hans and Christian Homburg. 1996. “Applications of Structural Equation Modeling in Marketing and Consumer Research: A Review.” *International Journal of Research in Marketing*.
- Bechara, Antoine, Antonio R. Damasio, Hanna Damasio, and Steven W. Anderson. 1994. “Insensitivity to Future Consequences Following Damage to Human

Prefrontal Cortex.” *Cognition*.

- Bekkering, Ernst, D. Ph, and Dan Hutchison. 2009. “A Follow-up Study of Detecting Phishing Emails A Follow-up Study of Detecting Phishing Emails.” (June).
- Bernama. 2013. “BorneoPost Online.” *Borneo Post*.
- Bhattacharjee and Sanford. 2006. “Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model.” *MIS Quarterly*.
- Bissell K, LaSalle RM, Cin PD (2019). 2019. “2019 Cost of Cybercrime Study | 9th Annual | Accenture.” *Accenture’s Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection*. Retrieved April 2, 2021 (<https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>).
- Bond, Charles F., Adnan Omar, Adnan Mahmoud, and Richard Neal Bonser. 1990. “Lie Detection across Cultures.” *Journal of Nonverbal Behavior*.
- Boorman, James, Yanhua Liu, Yixin Zhang, Yu Bai, Siyi Yao, Mengxue Wang, and Li Tai. 2014. “Implications of Social Media Networks on Information Security Risks.” 1–8.
- Boyd, Danah M. and Nicole B. Ellison. 2007. “Social Network Sites: Definition, History, and Scholarship.” *Journal of Computer-Mediated Communication* 13(1):210–30.
- Boyd, Danah M. and Nicole B. Ellison. 2010. “Social Network Sites: Definition, History, and Scholarship.” *IEEE Engineering Management Review*.
- Braun, Virginia and Victoria Clarke. 2006. “Qualitative Research in Psychology Using Thematic Analysis in Psychology Using Thematic Analysis in Psychology.” *Qualitative Research in Psychology*.
- Brody, Richard G., William B. Brizzee, and Lewis Cano. 2012. “Flying under the Radar: Social Engineering.” *International Journal of Accounting and Information Management*.
- Burger, John D., John Henderson, George Kim, and Guido Zarrella. 2011. “Discriminating Gender on Twitter.” in *EMNLP*.
- Burgoon, Judee K., David B. Buller, Laura K. Guerrero, Walid A. Afifi, and Clyde M. Feldman. 1996. “Interpersonal Deception: XII. Information Management Dimensions Underlying Deceptive and Truthful Messages.” *Communication*

*Monographs.*

- Burns, Mary B., Alexandra Durcikova, and Jeffrey L. Jenkins. 2012. "On Not Falling for Phish: Examining Multiple Stages of Protective Behavior of Information Systems End-Users." in *International Conference on Information Systems, ICIS 2012*.
- Camp, L. Jean. 2007. "Security and Usability: The Gap in Real-World Online Banking." *IEEE Technology and Society Magazine*.
- Cao, Jinwei, Paul Benjamin Lowry, and Paul Benjamin Lowry. 2015. "A Systematic Review of Social Networks Research in Information Systems: Building a Foundation for Exciting Future Research." *Communications of Association for Information Systems* 36(37):727–58.
- Caputo, Deanna D., Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. 2014. "Going Spear Phishing: Exploring Embedded Training and Awareness." *IEEE Security and Privacy*.
- Carletta, J. 1996. "Assessing Agreement on Classification Tasks: The Kappa Statistic." *Computational Linguistics*.
- Carlson, John R. 1999. "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions Author ( s ): John R . Carlson and Robert W . Zmud Source : The Academy of Management Journal , Vol . 42 , No . 2 ( Apr . , 1999 ), Pp . 153-170 Published by : Academy of Ma." 42(2):153–70.
- Carter, Lorraine. 2010. "How to Conduct Surveys: A Step-by-Step Guide." *Canadian Journal of University Continuing Education*.
- Castiglione, Aniello, Roberto De Prisco, and Alfredo De Santis. 2009. "Do You Trust Your Phone?" in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.
- Castillo, Carlos, Marcelo Mendoza, and Barbara Poblete. 2011. "Information Credibility on Twitter." in *Proceedings of the 20th international conference on World wide web - WWW '11*.
- Chandrasekaran, M., K. Narayanan, and S. Upadhyaya. 2006. "Phishing E-Mail Detection Based on Structural Properties." *NYS Cyber Security Conference*.
- Cheng, Z., J. Caverlee, and K. Lee. 2010. "You Are Where You Tweet: A Content-Based Approach to Geo-Locating Twitter Users." in *Proceedings of the 19th ACM International Conference on Information and Knowledge Management*.

- Chiaburu, Dan S., In Sue Oh, Christopher M. Berry, Ning Li, and Richard G. Gardner. 2011. "The Five-Factor Model of Personality Traits and Organizational Citizenship Behaviors: A Meta-Analysis." *Journal of Applied Psychology*.
- Chitrey, Anubhav, Dharmendra Singh, and Vrijendra Singh. 2012a. "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model." *International Journal of Information and Network Security (IJINS)*.
- Chitrey, Anubhav, Dharmendra Singh, and Vrijendra Singh. 2012b. "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model." *International Journal of Information and Network Security (IJINS)*.
- Chomsiri, Thawatchai. 2007. "HTTPS Hacking Protection." in *Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW'07*.
- Chu, Zi, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. 2012. "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?" *IEEE Transactions on Dependable and Secure Computing*.
- Conti, Mauro, Radha Poovendran, and Marco Secchiero. 2012. "FakeBook: Detecting Fake Profiles in on-Line Social Networks." in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*.
- Cook, Debra L., Vijay K. Gurbani, and Michael Daniluk. 2008. "Phishwish: A Stateless Phishing Filter Using Minimal Rules." in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.
- Coronges, Kathryn, Ronald Dodge, Cort Mukina, Zachary Radwick, Joseph Shevchik, and Ericka Rovira. 2012. "The Influences of Social Networks on Phishing Vulnerability." in *Proceedings of the Annual Hawaii International Conference on System Sciences*.
- Costa Jr., Paul T., Antonio Terracciano, and Robert R. McCrae. 2001. "Gender Differences in Personality Traits across Cultures: Robust and Surprising Findings." *Journal of Personality and Social Psychology* 81(2):322–31.
- Costa, P. T. and R. R. McCrae. 1992. "Professional Manual: Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-

- FFI)." *Odessa FL Psychological Assessment Resources* 3:101.
- Couper, M. P., J. Blair, and T. Triplett. 1999. "A Comparison of Mail and E-Mail for a Survey of Employees in U.S. Statistical Agencies." *Journal of Official Statistics*.
- Cresswell, J. W., V. L. Plano-Clark, M. L. Gutmann, and W. E. Hanson. 2003. "Advanced Mixed Methods Research Designs." *Handbook of Mixed Methods in Social and Behavioral Research*.
- Cyveillance. 2015. "The Cost of Phishing : Understanding the True Cost Dynamics Behind Phishing Attacks." *October*.
- Darlington, Y. and D. Scott. 2002. "Qualitative Research in Practice. Stories from the Field 2nd Edition." *Journal of Orthopaedic Nursing*.
- Darwish, Ali, Ahmed El Zarka, and Fadi Aloul. 2012. "Toward Understanding Phishing Victims' Profile." in *2012 International Conference on Computer Systems and Industrial Informatics, ICCSII 2012*.
- Davis, F. D., R. P. Bagozzi, and P. R. Warshaw. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science* 35(8):982–1003.
- Davis, Fred D. 1989. "Perceived Usefulness , Perceived Ease Of Use , And User Acceptance." *MIS Quarterly* 13(3):319–39.
- Davis, Fred D., Richard P. Bagozzi, and Paul R. Warshaw. 1992. "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace." *Journal of Applied Social Psychology* 22(14):1111–32.
- Denise, M., B. Sim, and S. Ronald. 1998. "Not so Different after All : A Cross-Discipline View of Trust."
- Dewan, Prateek, Anand Kashyap, and Ponnurangam Kumaraguru. 2014. "Analyzing Social and Stylometric Features to Identify Spear Phishing Emails." in *eCrime Researchers Summit, eCrime*.
- Dhamija, Rachna, J. D. Tygar, and Marti Hearst. 2006. "Why Phishing Works." in *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*.
- Dillard, James and Michael Pfau. 2002. "The Persuasion Handbook: Developments in Theory and Practice."

- Dillon, Andrew. 2001. *User Acceptance of Information Technology*.
- Dimension Research. 2011. *The Risk Of Social Engineering On Information Security : A Survey of IT Professionals*.
- Dong, Xun, John A. Clark, and Jeremy Jacob. 2008. "Modelling User-Phishing Interaction." in *2008 Conference on Human System Interaction, HSI 2008*.
- Douglas, Mary. 1978. "Cultural Bias." *Royal Anthropological Institute*.
- Dow, Malcom McLaren. 1988. "Measuring Culture: A Paradigm for the Analysis of Social Organization." *American Ethnologist* 15(2):402–3.
- Downs, Julie S., Mandy Holbrook, and Lorrie Faith Cranor. 2007. "Behavioral Response to Phishing Risk." in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit on - eCrime '07*.
- Emm, David. 2006. "Phishing Update, and How to Avoid Getting Hooked." *Network Security*.
- Eriksson, Päivi and Anne Kovalainen. 2011. *Qualitative Methods in Business Research*.
- Fette, Ian, Norman Sadeh, and Anthony Tomasic. 2007a. "Learning to Detect Phishing Emails." in *Proceedings of the 16th international conference on World Wide Web - WWW '07*.
- Fette, Ian, Norman Sadeh, and Anthony Tomasic. 2007b. "Learning to Detect Phishing Emails." in *16th International World Wide Web Conference, WWW2007*.
- Field, Andy. 2013. *Discovering Statistics Using IBM SPSS Statistics*.
- Field, Andy P. 2018. *Discovering Statistics Using IBM SPSS Statistics: 5th Edition*.
- Finn, Peter and Markus Jakobsson. 2007. "Designing Ethical Phishing Experiments." *IEEE Technology and Society Magazine*.
- Fire, Michael, Roy Goldschmidt, and Yuval Elovici. 2014a. "Online Social Networks: Threats and Solutions." *IEEE Communications Surveys and Tutorials*.
- Fire, Michael, Roy Goldschmidt, and Yuval Elovici. 2014b. "Online Social Networks: Threats and Solutions." *IEEE Communications Surveys and Tutorials*.
- Flores, Waldo Rocha, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. 2015.

- “Investigating Personal Determinants of Phishing and the Effect of National Culture.” *Information and Computer Security*.
- Fornell, Claes and David F. Larcker. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.” *Journal of Marketing Research*.
- Francis Galton, F. R. S. 1893. “Hereditary Genius: An Inquiry into Its Laws and Consequences.” *Science*.
- Furner, Christopher P. and Joey F. George. 2009. “Making It Hard to Lie: Cultural Determinants of Media Choice for Deception.” in *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*.
- Gao, Hongyu, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y. Zhao. 2010. “Detecting and Characterizing Social Spam Campaigns.” in *Proceedings of the 10th annual conference on Internet measurement - IMC '10*.
- Garfinkel, Simson L., David Margrave, Jeffrey I. Schiller, Erik Nordlander, and Robert C. Miller. 2005. “How to Make Secure Email Easier to Use.” in *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*.
- Görling, Stefan. 2006. “The Myth of User Education.” *Virus Bulletin Conference*.
- Gosling, Samuel D., Peter J. Rentfrow, and William B. Swann. 2003. “A Very Brief Measure of the Big-Five Personality Domains.” *Journal of Research in Personality*.
- Grazioli, Stefano. 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*.
- Grazioli, Stefano and Sirkka L. Jarvenpaa. 2000. “Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers.” *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*.
- Grazioli, Stefano and Alex Wang. 2001. “Looking Without Seeing : Understanding Unsophisticated Consumers ’ Success and Failure To Detect Internet Deception.” *ICIS 2001 Proceeding*.
- Gudgeon, Andrew C., A. L. Comrey, and H. B. Lee. 1994. “A First Course in Factor Analysis.” *The Statistician*.



- Gupta, B. B., Nalin A. G. Arachchilage, and Kostas E. Psannis. 2017. "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions." *Telecommunication Systems* 1–32.
- Gupta, B. B., Aakanksha Tewari, Ankit Kumar Jain, and Dharma P. Agrawal. 2017. "Fighting against Phishing Attacks: State of the Art and Future Challenges." *Neural Computing and Applications*.
- Gupta, Surbhi, Abhishek Singhal, and Akanksha Kapoor. 2017. "A Literature Survey on Social Engineering Attacks: Phishing Attack." in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*.
- Hadnagy, Christopher. 2010. "Social Engineering: The Art of Human Hacking." *The Art of Human Hacking*.
- Hair, J. F., W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham. 2010. *Multivariate Data Analysis*.
- Hansche, Susan. 2001. "Designing a Security Awareness Program: Part I." *Information Systems Security* 9(6):14.
- Hanson, William E., John W. Creswell, Vicki L. Plano Clark, Kelly S. Petska, and J. David Creswell. 2005. "Mixed Methods Research Designs in Counseling Psychology." *Journal of Counseling Psychology*.
- Henseler, Jörg. 2017. "Bridging Design and Behavioral Research With Variance-Based Structural Equation Modeling." *Journal of Advertising*.
- Herley, Cormac. 2009. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." in *NSPW '09 Proceedings of the New Security Paradigms Workshop*.
- Herzberg, Amir. 2009. "Why Johnny Can't Surf (Safely)? Attacks and Defenses for Web Users." *Computers and Security*.
- Higgins, Edward Tory and Arie W. Kruglanski, eds. 1996. *Social Psychology: Handbook of Basic Principles*. New York, NY, US: Guilford Press.
- Hong, Jason I. 2009. "A Hybrid Phish Detection Approach by Identity Discovery and Keywords Retrieval." 571–80.
- Hovland, Carl. I., Irving. L. Janis, and Harold. H. Kelly. 1953. "Communication and Persuasion: Psychological Studies of Opinion Change." *American Sociological*

*Review.*

- Huber, Markus, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa. 2009. "Towards Automating Social Engineering Using Social Networking Sites." *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009* 3:117–24.
- Humphreys, Lee, Phillipa Gill, and Balachander Krishnamurthy. 2010. "How Much Is Too Much? Privacy Issues on Twitter." in *ICA 2010*.
- Hutcheson, Graeme and N. Sofroniou. 1999. *The Multivariate Social Scientist*.
- Iahad, A. and Ab Rahim. 2012. "A Comparative Study of Acceptance and Use of ICT among University Academic Staff of ADSU and LASU: Nigeria." 2(1):103–15.
- Ibrahim, Nanzakiahmegat and Chesu Mustaffa. 2016. "Relationship between Message Strategy by Development Agent of Majlis Amanah Rakyat (Mara) with Participation in Training and Adoption Innovation." *Jurnal Komunikasi: Malaysian Journal of Communication*.
- Iqbal, Farkhund, Hamad Binsalleeh, Benjamin C. M. Fung, and Mourad Debbabi. 2010. "Mining Writeprints from Anonymous E-Mails for Forensic Investigation." *Digital Investigation* 7(1–2):56–64.
- Iqbal, Farkhund, Liaquat a. Khan, Benjamin C. M. Fung, and Mourad Debbabi. 2010. "E-Mail Authorship Verification for Forensic Investigation." *Proceedings of the 2010 ACM Symposium on Applied Computing - SAC '10* 1591.
- Irani, Danesh, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu. 2011. "Reverse Social Engineering Attacks in Online Social Networks." in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.
- Iuga, Cristian, Jason R. C. Nurse, and Arnau Erola. 2016. "Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks." *Human-Centric Computing and Information Sciences*.
- Jackson, Thomas W., Anthony Burgess, and Janet Edwards. 2006. "A Simple Approach to Improving Email Communication." *Communications of the ACM*.
- Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. "Social Phishing." *Communications of the ACM*.

- Jakobsson, Markus. 2007. "The Human Factor in Phishing." *Privacy Security of Consumer Information* 1–19.
- Jampen, Daniel, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. "Don't Click: Towards an Effective Anti - Phishing Training . A Comparative Literature Review." *Human-Centric Computing and Information Sciences*.
- Jin, Lei, Hassan Takabi, and James B. D. Joshi. 2011. "Towards Active Detection of Identity Clone Attacks on Online Social Networks." in *Proceedings of the first ACM conference on Data and application security and privacy - CODASPY '11*.
- John, Op P. and S. Srivastava. 1999. "The Big Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives." *Handbook of Personality: Theory and ...*
- Johnson, Paul E., Stefano Grazioli, and Karim Jamal. 1993. "Fraud Detection: Intentionality and Deception in Cognition." *Accounting, Organizations and Society* 18(5):467–88.
- Johnson, Paul E., Stefano Grazioli, Karim Jamal, and Imran A. Zualkernan. 1992. "Success and Failure in Expert Reasoning." *Organizational Behavior and Human Decision Processes*.
- Johnson, Richard D., George M. Marakas, and Jonathan W. Palmer. 2006. "Differential Social Attributions toward Computing Technology: An Empirical Investigation." *International Journal of Human-Computer Studies* 64(5):446–60.
- Karakasiliotis, A., S. M. Furnell, and M. Papadaki. 2006. "Assessing End-User Awareness of Social Engineering and Phishing." in *7th Australian Information Warfare and Security Conference*.
- Khayyambashi, Mohammad Reza and Fatemeh Salehi Rizi. 2013. "An Approach for Detecting Profile Cloning in Online Social Networks." in *2013 7th International Conference on e-Commerce in Developing Countries: With Focus on e-Security, ECDC 2013*.
- Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. 2013. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys and Tutorials*.
- Kim, Dan J., Donald L. Ferrin, and H. Raghav Rao. 2008. "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents." *Decision Support Systems*.
- Kim, Young Gab, Sanghyun Cho, Jun Sub Lee, Min Soo Lee, In Ho Kim, and Sung

- Hoon Kim. 2008. "Method for Evaluating the Security Risk of a Website against Phishing Attacks." in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.
- Kleinginna, Paul R. and Anne M. Kleinginna. 1981. "A Categorized List of Emotion Definitions, with Suggestions for a Consensual Definition." *Motivation and Emotion*.
- Knight, William. 2004. "Goin' Phishing?" *Infosecurity Today*.
- Kontaxis, Georgios, Iasonas Polakis, Sotiris Ioannidis, and Evangelos P. Markatos. 2011. "Detecting Social Network Profile Cloning." in *2011 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011*.
- Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. "Advanced Social Engineering Attacks." *Journal of Information Security and Applications*.
- Kruger, H. A. and W. D. Kearney. 2006. "A Prototype for Assessing Information Security Awareness." *Computers and Security* 25(4):289–96.
- Kumaraguru, Ponnurangam. 2009. "Phishguru: A System for Educating Users about Semantic Attacks." *Dissertation Abstracts International: Section B: The Sciences and Engineering*.
- Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. "School of Phish: A Real-World Evaluation of Anti-Phishing Training Categories and Subject Descriptors." P. 12 in *Symposium on Usable Privacy and Security (SOUPS)*.
- Kumaraguru, Ponnurangam, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System." *Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems*.
- Kumaraguru, Ponnurangam, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2007. "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer." in *ACM International Conference Proceeding Series*.
- Kumaraguru, Ponnurangam, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor,

- and Jason Hong. 2010. "Teaching Johnny Not to Fall for Phish." in *ACM Transactions on Internet Technology*.
- Kusrini, Elisa, Subagyo, and Nur Aini Masruroh. 2017. "Applying Triangulation Method to Strengthen Validity of Integrated Balanced Scorecard's Performance Measurement Model for Supply Chain's Actors and Regulators." *Advances in Intelligent Systems and Computing* 487:461–66.
- Kvedar, Derek, Michael Nettis, and Steven P Fulton. 2010. "The Use of Formal Social Engineering Techniques To Identify Weaknesses During a Computer Vulnerability Competition." *Journal of Computing Sciences in Colleges*.
- Lampert, Andrew. 2010. "Detecting Emails Containing Requests for Action." (June):984–92.
- Lance Spitzner. 2010. "How to Build an Effective Information Security Awareness Program - Information Security Magazine." *Techtarget*. Retrieved (<https://searchsecurity.techtarget.com/magazineContent/How-to-build-an-effective-information-security-awareness-program>).
- Landers, Richard N. and John W. Lounsbury. 2006. "An Investigation of Big Five and Narrow Personality Traits in Relation to Internet Usage." *Computers in Human Behavior* 22(2):283–93.
- Lean, Ooh Kim, Suhaiza Zailani, T. Ramayah, and Yudi Fernando. 2009. "Factors Influencing Intention to Use E-Government Services among Citizens in Malaysia." *International Journal of Information Management* 29(6):458–75.
- Li, T. Y. and Yongdong Wu. 2003. "Trust on Web Browser: Attack vs. Defense." *Applied Cryptography and Network Security* 241–253.
- Liang, Huigang and Yajiong Xue. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems*.
- Liu, Wendy and Derek Ruths. 2013. "What's in a Name? Using First Names as Features for Gender Inference in Twitter." *Proceedings of the 2013 AAAI Spring Symposium: Analyzing Microtext*.
- Louho, R., M. Kallioja, and P. Oittinen. 2006. "Factors Affecting the Use of Hybrid Media Applications." *Graphic Arts in Finland* 35(3):11–21.
- Lume, V. O. 2018. *Microsoft Security Intelligence Report*.

- Maldonado, Sebastián and Gaston L'Huillier. 2013. "SVM-Based Feature Selection and Classification for Email Filtering." Pp. 135–48 in *Pattern Recognition - Applications and Methods*, edited by P. Latorre Carmona, J. S. Sánchez, and A. L. N. Fred. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Mannan, Mohammad and Paul C. van Oorschot. 2008. "Privacy-Enhanced Sharing of Personal Content on the Web." *Proceeding of the 17th International Conference on World Wide Web - WWW '08* 487.
- Mao, Huina, Xin Shuai, and Apu Kapadia. 2011. "Loose Tweets: An Analysis of Privacy Leaks on Twitter." in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society - WPES '11*.
- Marett, Kent, David P. Biro, and Monti L. Knode. 2010. "Self-Efficacy, Training Effectiveness, and Deception Detection: A Longitudinal Study of Lie Detection Training."
- Maslow, Abraham. 1943. "A Theory of Human Motivation A Theory of Human Motivation." *Psychological Review*.
- Maslow, Abraham H. 1954. "Motivation and Personality." *Journal of Consulting Psychology*.
- Maslow, Abraham H. 1969. "The Farther Reaches of Human Nature." *Journal of Transpersonal Psychology*.
- McCord, M. and M. Chuah. 2011. "Spam Detection on Twitter Using Traditional Classifiers." in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.
- McGrath, D. K. and Minaxi Gupta. 2008. "Behind Phishing: An Examination of Phisher Modi Operandi." *Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET) 4*.
- McIlwraith, A. 2006. "Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness." 2006.
- McKnight, H., C. Kacmar, and V. Choudhury. 2003. "Whoops... Did I Use the Wrong Concept to Predict e-Commerce Trust? Modeling the Risk-Related Effects of Trust versus Distrust Concepts." in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, HICSS 2003*.
- Medlin, Christopher, Subroto Roy, Theong Ham Chai, and T. Ham Chai. 1999. "World Wide Web versus Mail Surveys: A Comparison and Report." *Paper*

*Presentation at ANZMAC99 ....*

- Miles, M.B & Huberman, A. .. 1994. *An Expanded Sourcebook: Qualitative Data Analysis (2nd Edition)*.
- Miranda, Shaila M. and Carol S. Saunders. 2003. "The Social Construction of Meaning: An Alternative Perspective on Information Sharing." *Information Systems Research*.
- Moore, Tyler and Richard Clayton. 2007. "An Empirical Analysis of the Current State of Phishing Attack and Defence." *Workshop on the Economics of Information Security*.
- Morgan, Paul. 1979. "Memorabilia." *Notes and Queries* 26(5):387–88.
- Neufeld, Derrick J., Linying Dong, and Chris Higgins. 2007. "Charismatic Leadership and User Acceptance of Information Technology." *European Journal of Information Systems* 16(4):494–510.
- Ng, Boon Yuen, Atreyi Kankanhalli, and Yunjie (Calvin) Xu. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective." *Decision Support Systems*.
- Nguyen, Huu Hieu and Duc Thai Nguyen. 2016. "Machine Learning Based Phishing Web Sites Detection." in *Lecture Notes in Electrical Engineering*.
- Nicholas Ismail. 2018. *Why Employees Are a Businesses Weakest Link - and How to Remedy That*.
- Novak, Thomas P., Donna L. Hoffman, and Yiu Fai Yung. 2000. "Measuring the Customer Experience in Online Environments: A Structural Modeling Approach." *Marketing Science*.
- Oh, Yunsang and Takashi Obi. 2012. "Evaluation of Field Phishing Study Setup Method." *International Journal of Information & Network Security (IJINS)*.
- Oppliger, Rolf, Ralf Hauser, and David Basin. 2008. "SSL/TLS Session-Aware User Authentication Revisited." *Computers and Security*.
- Pallant, Julie. 2011. *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS*.
- Papers, Federalist and E. Anderxon. 2006. "A Framework for Authorship Identification of Online Message: Writing-Style Features and Classification Techniques." *Journal Of The American Society for Information Science* (57(3)).

- Park, Gregory, H. Andrew Schwartz, Johannes C. Eichstaedt, Margaret L. Kern, Michal Kosinski, David J. Stillwell, Lyle H. Ungar, and Martin E. P. Seligman. 2015. "Automatic Personality Assessment through Social Media Language." *Journal of Personality and Social Psychology*.
- Parrish Jr., J. L., J. L. Bailey, and J. F. Courtney. 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks." *Southwest Decision Sciences Institute (SWDSI) Annual Meeting* 285–96.
- de Paula, Rogério, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David F. Redmiles, Jie Ren, Jennifer A. Rode, and Roberto Silva Filho. 2005. "In the Eye of the Beholder: A Visualization-Based Approach to Information System Security." *International Journal of Human-Computer Studies* 63(1–2):5–24.
- Pennacchiotti, Marco and Ana-Maria Popescu. 2011. "A Machine Learning Approach to Twitter User Classification." in *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media (ICWSM)*.
- Perloff, Richard M. 1993. *Audience and Behavior*.
- Pervin, Lawrence A. and Oliver P. John. 1999. *Handbook of Personality: Theory and Research*. Elsevier.
- Petty, Richard E. and John T. Cacioppo. 1986. "The Elaboration Likelihood Model of Persuasion." *Advances in Experimental Social Psychology*.
- Pfeiffer, Thomas, Heike Theuerling, and Michaela Kauer. 2013a. "Click Me If You Can! How Do Users Decide Whether to Follow a Call to Action in an Online Message?" in *International Conference on Human Aspects of Information Security, Privacy, and Trust*.
- Pfeiffer, Thomas, Heike Theuerling, and Michaela Kauer. 2013b. "Click Me If You Can! BT - Human Aspects of Information Security, Privacy, and Trust." Pp. 155–66 in, edited by L. Marinos and I. Askoxylakis. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Polakis, I., G. Kontaxis, and S. Antonatos. 2010. "Using Social Networks to Harvest Email Addresses." in *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*.
- Position, Enisa and Paper No. 2007. "Security Issues and Recommendations for Online Social Networks." *ENISA*.
- Purkait, Swapan. 2012. "Phishing Counter Measures and Their Effectiveness -



- Literature Review.” *Information Management and Computer Security*.
- Radicati, S. and Q. Hoang. 2017. “Email Statistics Report, 2017-2021.” *Email Statistics Report, 2017-2021 - Executive Summary* 44(0):4.
- Radicati, Sara, Principal Analyst, and Justin Levenstein. 2013. “Email Statistics Report , 2013-2017.” 44(0):2013–17.
- Rahman, Md Sazzadur, Ting-Kai Huang, Harsha V Madhyastha, Michalis Faloustos, Sazzadur Rahman, Ting-Kai Huang, Harsha V Madhyastha, and Michalis Faloutsos. 2012. “Efficient and Scalable Socware Detection in Online Social Networks Socware.” *Proceedings of the 21st USENIX Conference on Security Symposium*.
- Rao, Delip, Michael Paul, Clay Fink, David Yarowsky, Timothy Oates, and Glen Coppersmith. 2011. “Hierarchical Bayesian Models for Latent Attribute Detection in Social Media.” in *The Fifth International AAAI Conference on Weblogs and Social Media*.
- Rao, Delip, David Yarowsky, Abhishek Shreevats, and Manaswi Gupta. 2010. “Classifying Latent User Attributes in Twitter.” in *Proceedings of the 2nd international workshop on Search and mining user-generated contents - SMUC '10*.
- Rashtian, Hootan, Yazan Boshmaf, Pooya Jaferian, and Konstantin Beznosov. 2014. “To Befriend Or Not? A Model of Friend Request Acceptance on Facebook.” in *Proceedings of the Tenth Symposium On Usable Privacy and Security*.
- Raykov, Tenko and George A. Marcoulides. 2019. “Confirmatory Factor Analysis.” in *A First Course in Structural Equation Modeling*.
- Recker, Jan. 2013a. *Scientific Research in Information Systems: A Beginner’s Guide*.
- Recker, Jan. 2013b. “Scientific Research in Information Systems.” in *Scientific Research in Information Systems*.
- Reeder, Rob and Sunny Consolvo. 2015. “‘... No One Can Hack My Mind’: Comparing Expert and Non-Expert Security Practices.” *Symposium on Usable Privacy and Security*.
- Rhee, Hyeun Suk, Cheongtag Kim, and Young U. Ryu. 2009. “Self-Efficacy in Information Security: Its Influence on End Users’ Information Security Practice Behavior.” *Computers and Security*.

- Robert H. Gass, Fullerton and John S. Seiter. 2015. *Persuasion*. 5th ed. Routledge, 2015.
- Robert McMillan. 2009. "Researcher Make Wormy Twitter Attack."
- Rogers, Everett M. 1995. *Diffusion of Innovations*.
- Rosseel, Yves. 2012. "Lavaan: An R Package for Structural Equation Modeling. Journal of Statistical Software." *Journal of Statistical Software*.
- Rosseel, Yves. 2012. "Lavaan: An R Package for Structural Equation Modeling." *Journal of Statistical Software*.
- Rousseau, Denise M., Sim B. Sitkin, Ronald S. Burt, and Colin Camerer. 1998. "Not so Different after All: A Cross-Discipline View of Trust." *Academy of Management Review*.
- Schneider, Gary, Jessica Evans, and Katherine T. Pinard. 2009. *The Internet - Illustrated*.
- Schneier, B. 2000. "Semantic Network Attacks." *Communications for the ACM*.
- Schram, Jon. 2019. "Your Password May Be Vulnerable to Credential Stuffing: Here's How to Protect Your Company." *Kansas City Business Journal*.
- Seiter, John S. and Robert H. Gass. 2007. "A Rationale for Studying Persuasion."
- Sekaran, U. 2003. *Research and Markets: Research Methods for Business - A Skill Building Approach*.
- Shariff, Shafiza Mohd and Xiuzhen Zhang. 2014. "A Survey on Deceptions in Online Social Networks." *2014 International Conference on Computer and Information Sciences, ICCOINS 2014 - A Conference of World Engineering, Science and Technology Congress, ESTCON 2014 - Proceedings* (January).
- Sharma, Kunal. 2010. "An Anatomy of Phishing Messages as Deceiving Persuasion: A Categorical Content and Semantic Network Study." *EDPACS*.
- Shaw, R. S., Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. 2009. "The Impact of Information Richness on Information Security Awareness Training Effectiveness." *Computers & Education*.
- Sheng, Steve, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 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 '10.

- Sheng, Steve and Bryant Magnien. 2007. "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish." *In Proceedings of SOUPS 2007*.
- Silverman, David. 2006. "Interpreting Qualitative Data: Methods for Analyzing Talk, Text and Interaction - David Silverman - Google Books." 2.
- Silverman, David. 2011. "Chapter 3: Data Analysis." *Interpreting Qualitative Data : A Guide to the Principles of Qualitative Research*.
- Solomon, David J. 2001. "Conducting Web-Based Surveys." *Practical Assessment, Research and Evaluation*.
- Srivastava, Sanjay, Oliver P. John, Samuel D. Gosling, and Jeff Potter. 2003. "Development of Personality in Early and Middle Adulthood: Set Like Plaster or Persistent Change?" *Journal of Personality and Social Psychology*.
- Stebila, Douglas. 2010. "Reinforcing Bad Behaviour: The Misuse of Security Indicators on Popular Websites." *Proceedings of the 22nd Conference of the Computer- ....*
- Stembert, Nathalie, Arne Padmos, Mortaza S. Bargh, Sunil Choenni, and Frans Jansen. 2015. "A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence." Pp. 113–20 in *2015 European Intelligence and Security Informatics Conference*. IEEE.
- Stevens, James. 1992. *Applied Multivariate Statistics for the Social Sciences, 2nd Ed.* Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc.
- Stiff, James B., Hyun J. Kim, and Closepet N. Ramesh. 1992. "Truth Biases and Aroused Suspicion in Relational Deception." *Communication Research*.
- Stringhini, Gianluca;Christopher Kruegel;Giovanni Vigna. 2010. "Detecting Spammers on Social Networks." (b):1–16.
- Stringhini, Gianluca, Christopher Kruegel, and Giovanni Vigna. 2010. "Detecting Spammers on Social Networks[1] G. Stringhini, C. Kruegel, and G. Vigna, 'Detecting Spammers on Social Networks,' Proc. 26th Annu. Comput. Secur. Appl. Conf. - ACSAC '10, p. 1, 2010." *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10* 1.
- Tashakkori, A. and C. Teddlie. 2003. "Handbook of Mixed Methods in Social &

Behavioral Research.” *Sage Publication*.

Tembe, Rucha, Kyung Wha Hong, Emerson Murphy-Hill, Christopher B. Mayhorn, and Christopher M. Kelley. 2013. “American and Indian Conceptualizations of Phishing.” in *Workshop on Socio-Technical Aspects in Security and Trust, STAST*.

Thompson, Bruce. 2004. *Exploratory and Confirmatory Factor Analysis: Understanding Concepts and Applications*.

Thompson, Ronald L., Christopher A. Higgins, and Jane M. Howell. 1991. “Personal Computing: Toward a Conceptual Model of Utilization.” *MIS Quarterly* 15(1):125.

Thompson, Samuel. 2013. “Helping the Hacker? Library Information, Security, and Social Engineering.” *Information Technology and Libraries*.

Thornburgh, Tim. 2005. “Social Engineering : The ‘ Dark Art .’” in *Proceedings of the 1st annual conference on Information security curriculum development*.

Torabi, Sadegh and Konstantin Beznosov. 2013. “Privacy Aspects of Health Related Information Sharing in Online Social Networks.” ... *2013 USENIX Workshop on Health Information* ....

Trenholm, Sarah. 1989. *No Title*.

Tschakert, Kai Florian and Sudsangan Ngamsuriyaraj. 2019. “Effectiveness of and User Preferences for Security Awareness Training Methodologies.” *Heliyon*.

Twitchell, Douglas P. 2006. “Social Engineering in Information Assurance Curricula.” *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*.

Vacca, John R., Markus Jakobsson, and Alex Tsow. 2013. “Identity Theft.” Pp. e41–60 in *Computer and Information Security Handbook*.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. “User Acceptance of Information Technology: Toward a Unified View.” *Source: MIS Quarterly* 27(3):425–78.

Venkatesh, Viswanath, James Thong, and Xin Xu. 2012. “Consumer Acceptance and User of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology.” *MIS Quarterly* 36(1):157–78.

Vishwanath, Arun. 2015. “Diffusion of Deception in Social Media: Social Contagion

- Effects and Its Antecedents.” *Information Systems Frontiers*.
- Vishwanath, Arun, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. 2011. “Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model.” *Decision Support Systems* 51(3):576–86.
- Wagner, Claudia, Silvia Mitter, Christian Körner, and Markus Strohmaier. 2012. “When Social Bots Attack: Modeling Susceptibility of Users in Online Social Networks.” in *CEUR Workshop Proceedings*.
- Wang, Jingguo, Rui Chen, Tejaswini Herath, and H. Raghav Rao. 2009. “An Exploration of the Design Features of Phishing Attacks.” *Information Assurance, Security and Privacy Services*.
- Whittaker, Steve and Candace Sidner. 1996. “Email Overload: Exploring Personal Information Management of Email.” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Common Ground* 35:276–83.
- Whitten, A. and J. D. Tygar. 1999. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” *Proceedings of the 8th USENIX Security Symposium*.
- Williams, Emma J., Joanne Hinds, and Adam N. Joinson. 2018. “Exploring Susceptibility to Phishing in the Workplace.” *International Journal of Human Computer Studies* 120(June 2017):1–13.
- Witte, Kim. 1992. “Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model.” *Communication Monographs*.
- Workman, Michael. 2008. “A Test of Interventions for Security Threats from Social Engineering.” *Information Management and Computer Security*.
- Wright, Ryan, Suranjan Chakraborty, Asli Basoglu, and Kent Marett. 2010a. “Where Did They Go Right? Understanding the Deception in Phishing Communications.” *Group Decision and Negotiation* 19(4):391–416.
- Wright, Ryan, Suranjan Chakraborty, Asli Basoglu, and Kent Marett. 2010b. “Where Did They Go Right? Understanding the Deception in Phishing Communications.” *Group Decision and Negotiation*.
- Wu, Min, Robert C. Miller, and Greg Little. 2006. “Web Wallet: Preventing Phishing Attacks by Revealing User Intentions.” in *Symposium On Usable Privacy and Security*.

- Yang, Weining, Aiping Xiong, Jing Chen, Robert W. Proctor, and Ninghui Li. 2017. "Use of Phishing Training to Improve Security Warning Compliance." 52–61.
- Zamal, Faiyaz Al, Wendy Liu, and Derek Ruths. 2012. "Homophily and Latent Attribute Inference: Inferring Latent Attributes of Twitter Users from Neighbors." in *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media*.
- Zhang, Qi, Lu Cheng, and Raouf Boutaba. 2010. "Cloud Computing: State-of-the-Art and Research Challenges." *Journal of Internet Services and Applications*.
- Zinoviev, Dmitry and Vy Duong. 2009. "Toward Understanding Friendship in Online Social Networks." *The International Journal of Technology, Knowledge, and Society: Annual Review*.

# Appendices

## Appendix A: Survey Question

### Demography

In what year were you born?

Please indicate your gender

- Male
- Female
- other

How long have you been using email?

- Less than a year
- 1-2 years
- 2-4 years
- 5-9 years
- More than 10 years

### Email Usage

The Following questions ask about the number of emails for various facets of your email use. Please pick the response that best estimates your usage.



Please estimate how many emails are currently in your inbox.

- 50-100
- 101 -500
- More than 500

How frequently important emails do you receive each day . (Important here means that you need to respond urgently).

- none
- Little
- Some
- A Lot

How many emails do you respond to each day.

- 1-4
- 5-10
- more than 10

In average ,how many emails do you send each day?

- none
- 1-4
- 5-10
- more than 10

### **Feeling towards email**

**The following will tell us about you feelings towards your email usage.Please choose that best represents your agreement with the statement.**

Rank the following uses of email to indicate their importance to you (1 is most important and 4 is least important).

	1	2	3	4
On-line Verification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Work communication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social networking notification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online shopping and promotion updates.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Email Practices

The following questions ask about your current email practices. Please provide the answer that best represents your practice.

What email service do you use most frequently?

- Gmail
- Company email
- Yahoo
- Others

How many active email account do you have?

- 1 only
- 2 - 4
- 5 or more

Do you check your email everyday?

- Yes
- No

### Uses And Gratification

Could you please provide your email address?

- Yes
- No

Which of the following describes your work situation?

- Unemployed
- Professional
- Student
- General worker
- Other

**For the following questions, please rate you level of agreement**

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I use email to keep up-to-date with work activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use email for my social network activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found email is a good way to maintain relationship	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email is very important to my daily life	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I look professional when using email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use email to pass the time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I manage to control incoming email myself	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have no problem to tell others my email address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
My email use is effective	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found email is easy to use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I always choose email as an option for communication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am easy to trust conversation made by email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I always monitor my incoming email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I only response email from known sender	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I delete email from unknown sender	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Computer use

Approximately how many hours a day do you spend using a computer?

- less than 1
- more than 1 and less than 5
- more than 5

Rank the task below in terms of your priority in using the internet.

Information seeking and searching

Electronic mail

Social networking sites

Online Shopping

Online Game

How important is having internet access to you?

- not at all
- moderately
- very

Do you update your antivirus manually?

- No
- Yes, If so how often?

How much confidence do you have in your antivirus software?

- None
- some
- a lot

---

Do you scan downloaded files for viruses?

- Always
- Sometimes
- Never

Please choose the corresponding number in each statement which best describes the degree to which a statement is true for you:

I see my self as:

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
Extroverted,enthusiastic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Critical, quarrelsome	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dependable, self-deciplined	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anxious, easily upset	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Open to new experiences, complex	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reserved, quiet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sympathetic, warm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disorganized, careless	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Calm,emotionally stable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Conventional, uncreative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

**Please read the short paragraph to answer this question:**

**Dear participant, please pretend that you received the next four email .**

**The question is what will be your action to each of the email.**

### Email 1

• Hello! People ✱

---

• **mc** <waterprufull@yahoo.com> 11/19/14 at 9:44 AM ✱  
To: m\_cruch@yahoo.com

Hello!  
My name is miss Marcy,i saw your profile at (www.facebook.com)i'm sorry if i am embarrassing you, please i will like you to write to me with my private Email (m\_cruch@yahoo.com)i have something important to tell you

[Reply](#), [Reply All](#) or [Forward](#) | [More](#)

Email 2



Warning Notification

Dear PayPal Member ,

It has come to our attention that your PayPal<sup>®</sup> account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records before August 09, 2007.

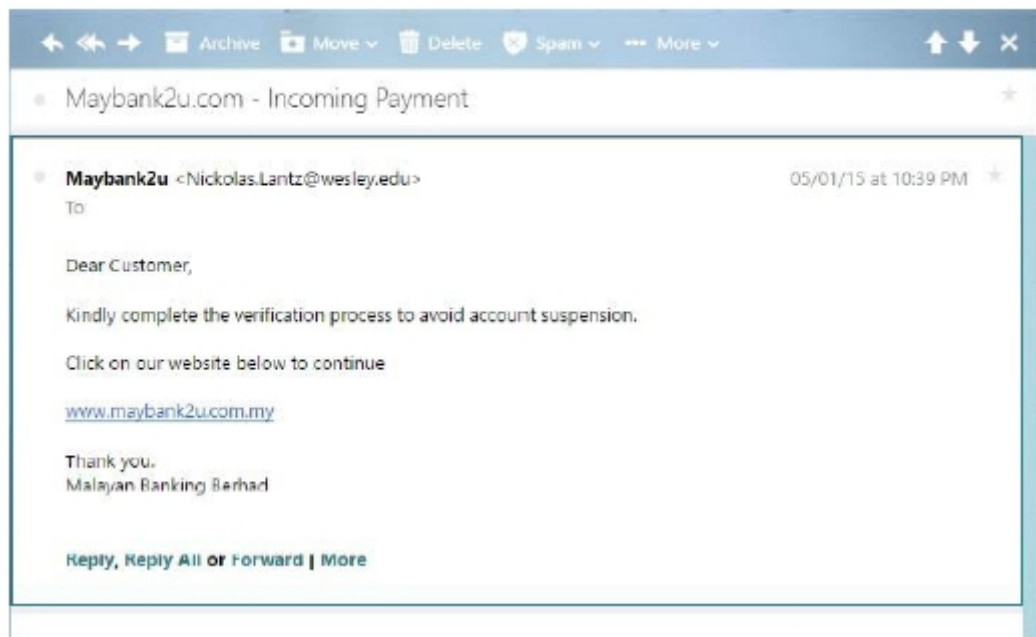
Once you have updated your account records, your PayPal<sup>®</sup> account activity will not be interrupted and will continue as normal.

[Click here to update your PayPal account information](#)

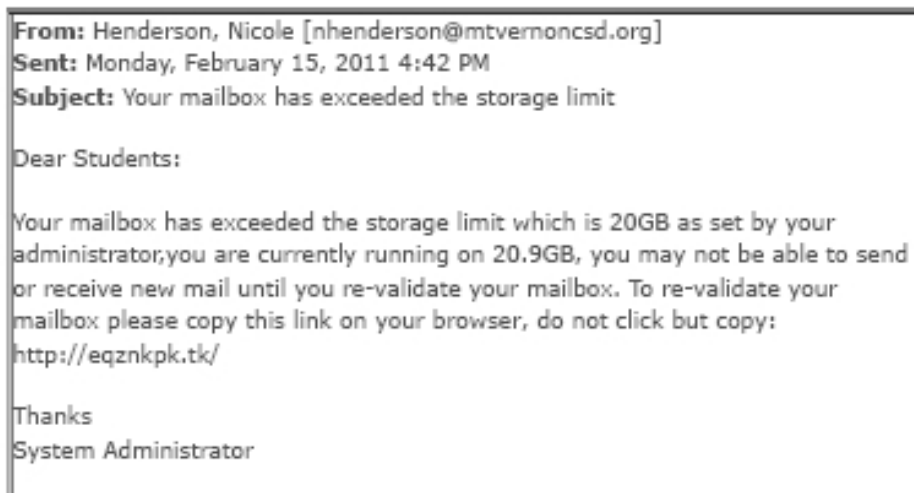
Copyright © 1999-2007 PayPal. All rights reserved.  
Information about FDIC pass-through insurance



### Email 3



### Email 4




Please rate your answer for email 1- email 4:

1. *Definitely will delete or ignore the email*
2. *Most likely will delete or ignore the email*
3. *Maybe will delete or ignore the email*
4. *I don't know*
5. *Maybe will respond*
6. *Most likely will respond*
7. *Definitely will respond*

	1	2	3	4	5	6	7
Email 1: Hello	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email 2: Paypal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email 3: Maybank2U	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email 4: System Maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Appendix B : Interview Question

<b>RESEARCH TEAM</b>		
Principle Researcher:	Zalina Ayob Doctor of Computer Science Student	
Principle Supervisor:	Dr.George Weir Lecturer Computer and information Science University Of Strathclyde ,UK	
Associate Researcher:	Pn. Siti Hawa Ahmad Lecturer Computer Science MARA Professional College, Malaysia	
<b>DESCRIPTION</b>		
<p>This Project is being undertaken as part of doctorate computer science for Zalina Ayob. The purpose of this interview is to identify the socio-psychological factors that influence email users to fall victims for phishing email, and find the relationship between each factor and users' demographics such as age, gender, educational level, relationship status, and personality type. You are invited to participate in this project because you are ( respond/ignore) to our phishing email experiment. The research team requests your assistance because your input is valuable in helping to develop a better understanding on how email users can fall under (victims/detector) categories for phishing email tricks and attacks.</p>		
<b>PARTICIPATION</b>		
<p>Your interview will be recorded in audio. The interview will take approximately about 30- 45 minute of your time. Interview can be performed by phone or face to face only.</p>		
<b>RISKS</b>		
<p>There are no significant potential risks associated with this research project. However the interview may cause participants to experience some level of anxiety. Also, some anxiety may arise from a realization that the participants are vulnerable. However, participations are entirely voluntary and participants are not obliged to answer any questions they find objectionable and they have the right to stop the interview at any time without any penalty. No information collected will be reported to anyone who is authority over them and participants.</p>		
<b>PRIVACY AND CONFIDNTALITY</b>		
<p>All comments and responses will be treated confidentially. Your name is not required in any of the responses. However, any information obtained in connection with this research that can identify you will remain confidential. It will only be disclosed with your permission, subject to legal requirements. Any data collected as part of this project will be stored in non-identifiable form and securely as University Of Strathclyde of research data policy. We plan to publicly present and publish the results of this research as journal articles and conference proceedings. However, information will only be provided in a form that does not identify you. The interview will be audio recorded and the transcriptions will remove any identifying details. Only the researcher will have access to the audio tape. The audio tape will be destroyed at the conclusion of the project. The transcription of the interview will be sent to you before data analysis to be revised and where necessary rectified by you. It is not possible for you to participate without being audio recorded.</p>		
<b>CONSENT TO PARTICIPATE</b>		
<p>We would like to ask you to sign a written consent form (enclosed) to confirm your agreement to participate.</p>		
<b>QUESTIONS/ FURTHER INFORMATION ABOUT THE PROJECT</b>		
<p>If have any questions or require further information please contact one of the research team members below.</p>		

**CONTACT INFORMATION**

Zalina Ayob  
(Main Interviewer)  
0182264301  
zalina.ayob@mara.gov.my

Siti Hawa Abdullah  
(2<sup>nd</sup> Interviewer)  
01162031170  
s.hawa@mara.gov.my

Telephone: 0141 548 3707  
Email: ethics@strath.ac.uk

*Thank you for helping with this research project. Please keep this sheet for your information.*

**QUESTIONS:**

1. Have you heard about phishing emails?
2. How do you identify phishing email?
3. What did you do when you opened the phishing email? why?
4. Have you checked the link in phishing email? what did you found?
5. Have you checked the reply address in the phishing email? What did you found?
6. What did you do when you suspected the phishing email?
7. Why did you respond to the phishing email? (for victims)
8. What did you do when you discover the phishing email? (for detectors)
9. What is your reaction if someone accesses your account?
10. .How important is your account to you?

**(PRINT NAME)****Signature of Participant:****Date:**

## Appendix C: Ethical Consent



Participant Information Sheet for Security and Email use Survey

**Name of department:** School Of Information Science

**Title of the study:** Exploring user awareness of network security threats

ZalinaAyob

Postal Address:

LT12.13

Computer and Information Sciences Livingstone Tower

26 Richmond St GLASGOW G1 1XH

**Application ID:** 183

**Status:** Approved

**Title of research:**

Exploring user awareness of network security threats

**Summary of research:**

This study aims to shed light on end-user awareness of network security issues and seeks to gauge user's own impressions of such awareness with a view to exploring how such perception may affect the end-user's network behaviour

**How will participants be recruited?**

Recruitment

-Indirect contact with the participant

-Participants will be identified by the student researcher or person in authority.

-The recruitment by student researchers will be via:

-Directory or Database in the approval domain.

-Direct Contact with the Participant

**The recruitment will be via:**

Email  
Personal contact

**How will consent be demonstrated?**

An information sheet has been prepared which gives participants full details of the survey. It will be made clear to participants in the information sheet that

Anonymity and confidentiality will be maintained.  
The study will not affect activity and their running system productivity.  
No harm will affect participants in terms of psychology or emotion.

**What will the participants be told about the conduct of the research?**

Participants will be informed that they will be asked to give their permission to be included in the study. Thereafter, they will receive survey email and a request to complete a short on-line questionnaire that addresses aspects of computer experience and security awareness.

**What will participants be expected to do?**

Participants must complete a consent form to confirm their willingness to take part in this study. Participation in this research is on a volunteer basis and no payment will be made. The research is expected to answer specific research questions on perceived risks in network security.

**How will data be stored?**

The researcher will abide by the provisions of the Data Protection Act and the University Data Protection Policy there for;  
Data and results obtained from the research will only be used in the way(s) for which consent has been given.

**Data will be:**

Fairly and lawfully processed  
Processed for limited purposes  
Adequate, relevant and not excessive  
Accurate  
Not kept longer than necessary  
Processed in accordance with the participant's rights  
Secure  
Not transferred to settings without adequate protection.

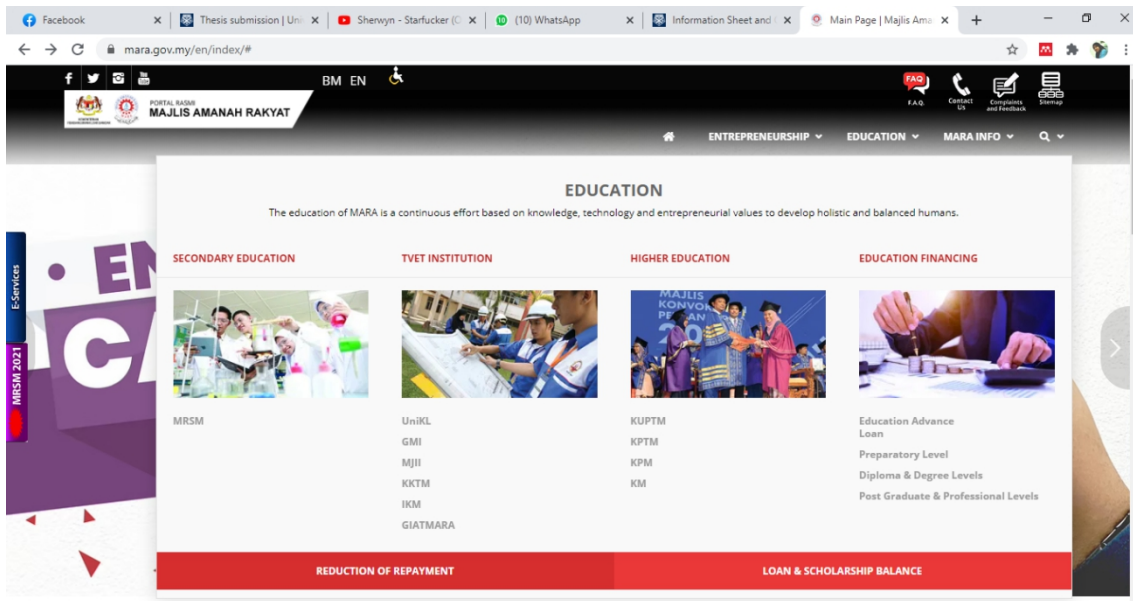
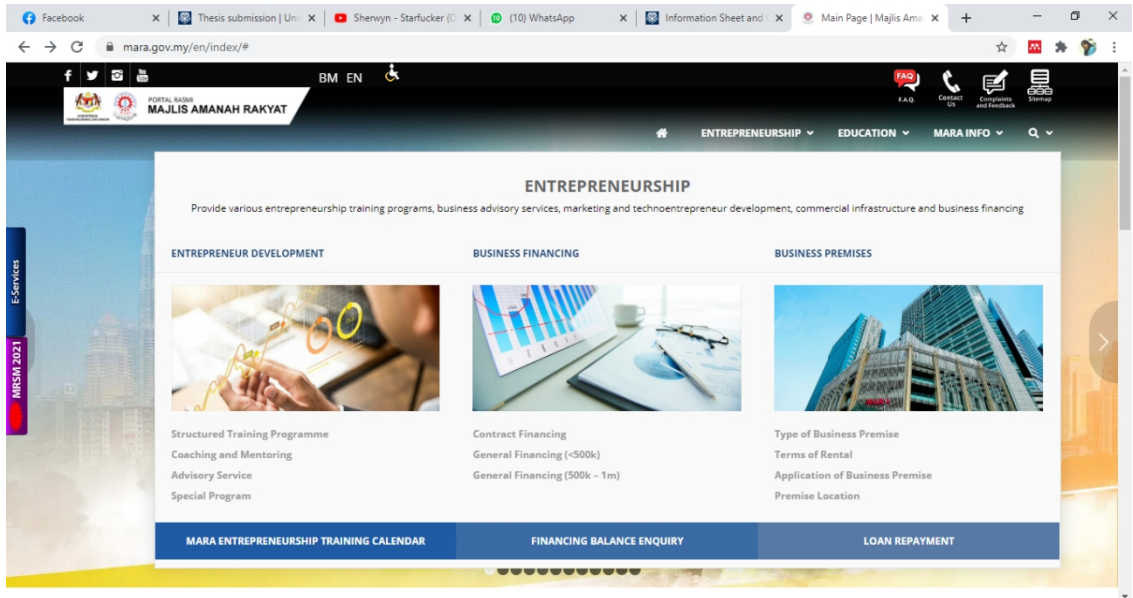
**How will data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.)** The data will be collected and analysed based upon the research focus. Only anonymised, relevant and allowable/ non-confidential data be disclosed in the research dissertation. The data will also be compared to other secondary sources such as related articles, journals or books. This comparison will support judgments on the reliability of the collected data. The data will also be the basis for comparative study with similar overseas/ international data.

**How and when will data be disposed of?**

The student researcher will have access to data generated in the study. In addition the research supervisor of may see the data, in order to guide the student in the associated analysis. In working with the collated data, all information that could identify individual participants will be removed. Data will be stored for a maximum of one year after the conclusion of the researcher's present degree course. All data will be stored in a secure PGR database that can only be accessed by the authenticated student researcher.

# Appendix D: MARA Profile

## a) MARA Website (www.mara.gov.my)






Appendix E: Sample latest phishing email attack to MARA inbox

**Fw: Payment Advice**

amratulnisa binti ahmad <amratulnisa.ahmad@mara.gov.my>  
Mon 28-Sep-20 3:29 PM  
To: Zalina binti Ayob <zalina.ayob@mara.gov.my>

---

**From:** Rozaina binti. Jamaludin <rozainaj@mara.gov.my>  
**Sent:** Friday, September 18, 2020 7:32 AM  
**To:** KPM Beranang <kpmberanang@mara.gov.my>  
**Subject:** Payment Advice

 Microsoft

Remittance Advice - Kpmberanang 09172020.pdf 22.8 KB

[View Attachments](#)

mara.gov.my uses OneDrive to share documents securely.

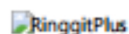
Last Chance To Get RM450 Cash With A New Citibank Credit Card!

Diana from RinggitPlus <can@ringgitplus.com>

Fri 11-Sep-20 12:04 PM

To: Zalina binti Ayob <zalina.ayob@mara.gov.my>

If this e-mail is not displayed properly, click here.



Dear Zalina Binti Ayob,

We're mid way through September and RM450 is waiting to be yours! Apply for Citibank Credit Card, get approved and RM450 is yours.

Just Apply, Approve & Spend\* when you apply for a Citibank Credit Card with us.

Valid for ALL approved applicants!

\*T&Cs Apply.

**How to Get RM450:**

1. Interact with our chatbot after clicking the link below and starting the conversation
2. Provide pictures of your IC for credit score checking on WhatsApp
3. Complete the card application process on WhatsApp and get approved by the bank

All approved applicants from 9 September 2020 (1pm) to 14 September 2020 (6pm) will receive RM450 cash, upon fulfillment of spend requirement.

**APPLY QUICKLY**

You are receiving this email because you have subscribed to RinggitPlus newsletter.  
If you prefer not to receive our future newsletter you can [unsubscribe](#).

Address: Level 25, Vertical Corporate Tower B, Avenue 10, No. 8, Jalan Kerinchi, Bangsar South, 59200 Kuala Lumpur, Malaysia

Terms of Use | Privacy Policy  
Copyright 2020 © Jirnexu Sdn Bhd. All rights reserved.

**PERINGATAN - notifikasi emel spam**

Admin Mara <admin@mara.gov.my>

Tue 01-Sep-20 12:30 PM

To: All User <alluser@mara.gov.my>

Assalamualaikum & Salam Sejahtera,

YBhg. Datuk/Dato'/Datin/Tuan/Puan,

**MAKLUMAN**

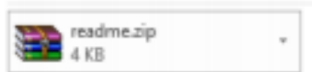
Notifikasi seperti emel di bawah adalah dirujuk.

Berikutan insiden penyebaran notifikasi emel yang mengandungi lampiran seperti paparan dibawah, mohon kerjasama semua pengguna untuk **menghapuskan (delete) emel yang telah diterima tanpa membuka emel berkenaan**. Pengguna juga diingatkan untuk tidak membuka / klik pada lampiran (attachment) yang terdapat dalam emel tersebut. Insiden ini dikategorikan sebagai *spam email*. Walaubagaimanapun, setakat semakan pihak BTM, emel tersebut tidak memberi kesan kepada inbox pengguna dan pihak BTM telah menyenarai hitam emel tersebut.

Diingatkan juga, sekiranya YBhg. Datuk/Dato'/Datin/Tuan/Puan ada menerima sebarang emel dari penghantar yang tidak dikenali atau subjek emel yang tidak jelas, hapuskan (*delete*) emel tersebut dengan segera. Sebarang pertanyaan berkaitan perkara di atas, sila hubungi Helpdesk MARA di talian 03-2613 2323 / 03-2613 2322.

Sekian, harap maklum.

b/p : Pengarah  
Bahagian Teknologi Maklumat (BTM)  
MARA



**DISCLAIMER**

*This e-mail ( including any attachments ) may contain confidential information and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, you are hereby notified that any dealing, review, distribution, printing, copying or use of this e-mails strictly prohibited. If you have received this e-mail in error, please notify the sender or MARA immediately and delete the original message. Opinions, conclusions and other information in this e-mail that do not relate to the official business of MARA and/or its subsidiaries shall be understood as neither given nor endorsed by MARA and/or its subsidiaries and neither MARA nor its subsidiaries accepts responsibility for the same. All liability arising from or in connection with this computer viruses and/or corrupted e-mails is excluded to the fullest extent permitted by law.*

Fw: Mara.gov.my\_Notification:(Wednesday, September 16, 2020)

amratulnisa binti ahmad <amratulnisa.ahmad@mara.gov.my>

Mon 28-Sep-20 3:28 PM

To: Zalina binti. Ayob <zalina.ayob@mara.gov.my>

---

From: Surainizan binti. Mohamed Sufian <surainizan@mara.gov.my>

Sent: Wednesday, September 16, 2020 9:03 AM

To: amratulnisa binti ahmad <amratulnisa.ahmad@mara.gov.my>

Subject: Mara.gov.my\_Notification:(Wednesday, September 16, 2020)

## OFFICE 365

Hello Amratulnisa.ahmad,

Your amratulnisa.ahmad@mara.gov.my password is set to Expire today,

Wednesday, September 16, 2020 at 1:03:33 AM

You can change your password or continue using same password below

[Keep Same Password](#)

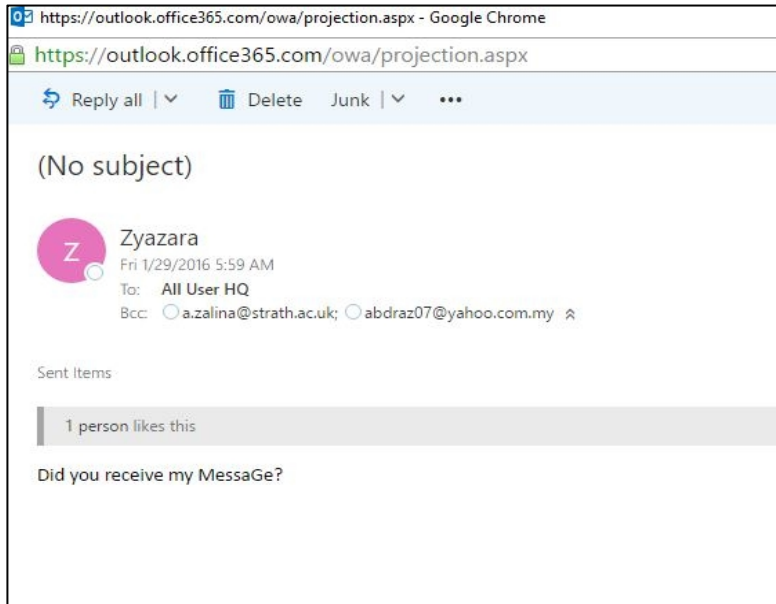
Mara.gov.my Support

### DISCLAIMER

*This e-mail ( including any attachments ) may contain confidential information and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, you are hereby notified that any dealing, review, distribution, printing, copying or use of this e-mails strictly prohibited. If you have received this e-mail in error, please notify the sender or **MARA** immediately and delete the original message. Opinions, conclusions and other information in this e-mail that do not relate to the official business of **MARA** and/or its subsidiaries shall be understood as neither given nor endorsed by **MARA** and/or its subsidiaries and neither **MARA** nor its subsidiaries accepts responsibility for the same. All liability arising from or in connection with this computer*

## Appendix F :Email Experiment

### Experiment 1



### Result

#### **Email Features:**

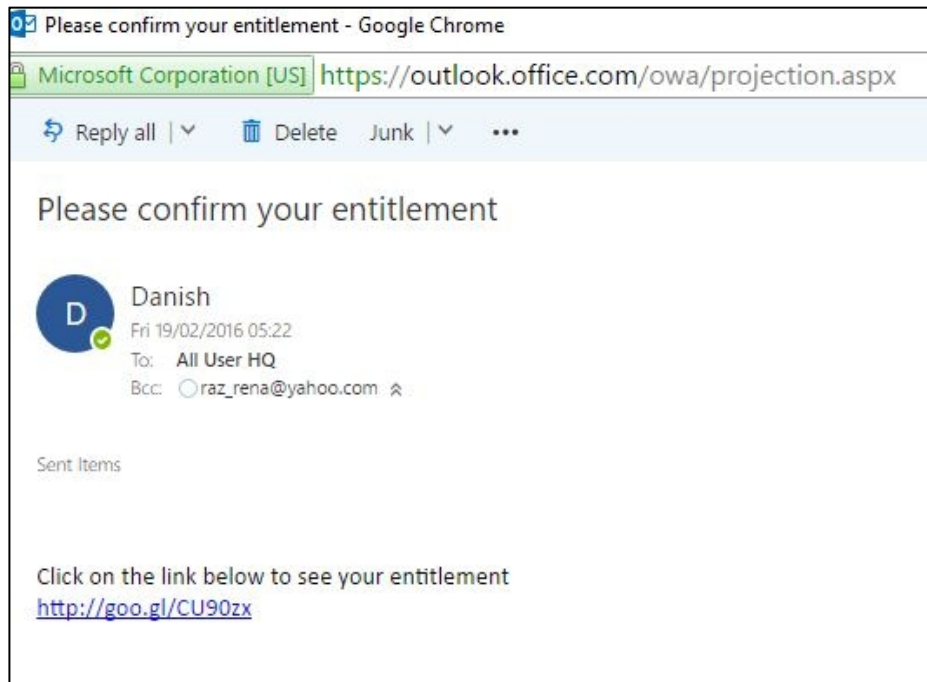
Sender email: *zyazara@mara.gov.my*  
Recipient email domain: *@mara.gov.my*  
Status: *known sender*  
Service: *Outlook*  
Subject: *none*  
Link: *none*  
Attachment: *None*  
Content: *Did you get my messaGe?*

Quantity: *~3000 users*  
Tracking duration: *7a.m – 7 p.m-malaysia*

#### **Results:**

Email opened: *1850*  
Reply message: *10*

## Experiment 2



## Result

### Email Features:

Sender email: *danish@mara.gov.my*

Recipient email domain: *@mara.gov.my*

Status: *known sender*

Service: *Outlook*

Subject: *Please confirm your entitlement*

Link: *yes*

Attachment: *None*

Content: *Click on the link below to see your entitlement*

<http://goo.gl/CU90zx>

Quantity: *~3000 users*

Tracking duration: *7a.m – 7 p.m-malaysia*

### Results:

Email opened: *803*

Reply message: *0*

Link click: *149*

## Experiment 3:



## Result

### Email Features:

Sender email: *worldprospect2u@gmail.com*

Recipient email domain: *Variety*

Status: *unknown sender*

Service: *google mail*

Subject: *Your future prospect*

Link: *no*

Attachment: *None*

Content: *Hello,*

*My name Jack Hooke, I saw your profile at facebook. I don't want to embarrass you, so please respond to my email as I have something important to tell you regarding your future prospect.*

*Regard*

*JH*

Quantity: 70 users

Tracking duration: unlimited

Results:

Email opened: not track

Reply message: 0