A MODEL TO IDENTIFY FACTORS INFLUENCING INDIVIDUAL PHISHING SUSCEPTIBILITY AMONG E-MAIL USERS

ALLEN ANAK PETER DIMAN

ASIA e UNIVERSITY
2023

A MODEL TO IDENTIFY FACTORS INFLUENCING INDIVIDUAL PHISHING SUSCEPTIBILITY AMONG E-MAIL USERS

ALLEN ANAK PETER DIMAN

A Thesis Submitted to Asia e University in
Fulfilment of the Requirements for the
Degree of Doctor of Philosophy

August 2023

ABSTRACT

E-mail phishing is a serious problem for the human society as well as for the organisations. Previous studies have identified that an individual's personality characteristics were among the key contributors to the problem. As such, this study has applied a combination of the Big-Five Personality Traits Theory, the Protection Motivation Theory, and Cialdini's Principle of Persuasion as its research model. The structural Equation Modelling (SEM) technique was used to measure hypothetical, direct, and mediated relationships between the constructs of the study. Data collection using survey questionnaires was collected from 403 respondents who use e-mails as part of their daily tasks. This study's findings revealed a relationship between individuals' personality traits and how they perceive themselves in appraising phishing threats and associated coping strategies. The study also found that individual levels of appraisal concerning the threat of phishing and coping strategies can affect their likelihood of becoming a phishing victim. Finally, the study discovered that the relationships between an individual's personality traits and an individual's phishing susceptibility can be further explained through the mediating effect of threat and coping appraisal. The primary contribution of this study lies in its novel approach of utilising the Protection Motivation Theory to explain the factors that render certain characteristics of individuals more vulnerable to phishing attacks as a result of their unique personality traits.

Keywords: Coping appraisal, personality traits, persuasion, phishing, phishing susceptibility, protection motivation theory, threat appraisal

APPROVAL

This is to certify that this thesis conforms to acceptable standards of scholarly presentation and is fully adequate, in quality and scope, for the fulfilment of the requirements for the degree of Doctor of Philosophy

The student has been supervised by: **Professor Dr. Titik Khawa Abdul Rahman.**

The thesis has been examined and endorsed by:

Associate Professor Dr. Wan Fatimah Wan Ahmad
Universiti Teknologi Petronas
Examiner 1

Associate Professor Dr. Nasiroh Binti Omar
Universiti Teknologi Mara
Examiner 2

This thesis was submitted to Asia e University and is accepted as fulfilment of the requirements for the degree of Doctor of Philosophy.

Professor Dr. Siow Heng Loke
Asia e University
Chairman, Examination Committee
22nd August 2023

DECLARATION

I hereby declare that the thesis submitted in fulfilment of the PhD degree is my own work and that all contributions from any other persons or sources are properly and duly cited. I further declare that the material has not been submitted either in whole or in part, for a degree at this or any other university. In making this declaration, I understand and acknowledge any breaches in this declaration constitute academic misconduct, which may result in my expulsion from the programme and/or exclusion from the award of the degree.

Name: Allen Anak Peter Diman

Signature of Candidate: **Date**: 22 August 2023

ACKNOWLEDGEMENTS

Praise be to God, the greatest of all, who enables me to conduct and complete my PhD research through His guidance and mercy. Special thanks also to Professor Dr. Titik Khawa Abdul Rahman who has provided me with unwavering support, guidance, and encouragement from the beginning of my PhD voyage to the conclusion of my research. I would also like to thank Asia e University (AeU) for providing me with the opportunity and support throughout my PhD journey. My sincere appreciation also extends to those who participated in the survey. Finally, I am grateful to my parents, who have always supported me and my growth. To my devoted wife, Veronica Lugah, who has always been there for me, and to my cherished children, Ryan Alistair and Alex Zechariah, for their fortitude and motivation throughout the journey of completing this PhD study.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

LIST OF ABBREVIATION

AVE	Average Variance Extracted
COVID-19	Corona Virus Disease of 2019
CR	Composite Reliability
HTMT	Heterotrait-Monotrait
IBM	International Business Machine
PLS	Partial Least Square
PMT	Protection Motivation Theory
SEM	Structural Equation Modelling
SPSS	Statistical Product and Service Solutions
TTAT	Technology Threat Avoidance Theory
USD	United States Dollars
VAF	Variance Accounted For

CHAPTER 1

INTRODUCTION

1.0 Introduction

This chapter provides the foundation as well as the direction of the study. The chapter begins with the background on the subject area that was undertaken in this study. This is followed by a problem statement that identifies the gap in the literature which is required to be addressed and the arguments on why it is vital to conduct research on the topic of individual susceptibility to phishing attacks are covered. Subsequently, based on the problem statement, the study's research objectives and research questions were derived which were used to guide the researcher throughout this study. Next, the scope of the study was presented which forms the boundary within which the study was conducted. Justification for conducting the study and why the study is significant to the area of information security were thoroughly discussed. Next, the chapter discussed the contribution of the study to the body of knowledge from the perspective of theoretical, practical, and methodological contributions. The definitions of key terms which are essentially the common key terms that the current researcher used in this study were provided. Finally, the organisation of the thesis provides the readers with a brief description of the contents of each chapter in this thesis followed by the chapter summary.

1.1 Background of the Study

Phishing is a serious and costly threat to both individuals and organisations (Burns et al., 2019; Kleitman et al., 2018). The consequences as a result of being a phishing victim include financial losses, an effect on the individual's or organisation's reputation, loss of confidential data, and an effect on the organisation's competitiveness (Armin et al., 2016; Bose & Leung, 2014; Cross & Gillett, 2020;

Jampen et al., 2020; Smith et al., 2019). Various reports indicate that phishing incidents have been on the rise year after year (Gupta et al., 2017). According to data collected by the cyber security firm AAG IT Services, phishing incidents have cost American business victims more than United States Dollars (USD) 2.7 billion in 2022 alone, and between 2020 and 2021, the reported cybercrime which includes phishing has increased 168% in the Asia-Pacific region (Griffiths, 2023).

In addition, the site has also presented some interesting facts related to phishing incidents. It stated that nearly 82% of all security breaches that occurred in organisations globally were due to the human element of which 35% of such breaches were the result of phishing via e-mail (Griffiths, 2023). Griffiths (2023) also noted a 74% increase in phishing e-mails sent per second in 2022 and that almost 100% of social attacks in the Public Administration sector in the USA involved phishing methods. Moreover, according to the author, security strategies such as firewalls, secure e-mail gateways, and proxy servers, are no longer capable of stopping phishing threats from occurring, mainly because cybercriminals have increasingly launched these phishing attacks from trusted servers and business or personal messaging applications.

Malaysia has also not sparred from being the target of cyber criminals using the tactic of phishing. Based on the information presented by Muharram et al. (2022) on average 31 cybersecurity incidents such as phishing take place in Malaysia daily. Moreover, Muharram et al. (2022) also stated that in 2019 alone, CyberSecurity Malaysia reported that the country lost RM539 million from the 13,000 reported cybercrime cases. This number according to the authors has since increased to 17,000 in 2020 and for 2021, there were more than 20,000 reported cases resulting in losses amounting to RM560 million. In 2022, the daily newspaper, Bernama quoted by the

New Straits Times stated that almost RM600 million were reported lost due to the same phenomenon (Bernama, 2023). For the year 2023 up to June, based on the latest statistical figures provided by CyberSecurity Malaysia which are available online, it was reported that approximately 13,500 cybercrime cases were reported to have occurred during the period (CyberSecurity Malaysia, 2023). If this trend continues, it is expected that cybercrime in Malaysia in 2023 will surpass the previously recorded cases in 2020, 2021 and 2022.

On another note, the same daily newspaper, The New Straits Times which quoted the Commercial Crime Investigation Department (CCID) of the Royal Malaysian Police, stated that Malaysians lost roughly Ringgit Malaysia (RM) 2.23 billion from phishing incidents during years from 2017 to June 2021 (Basyir, 2021). Another interesting finding is that a report on the Cyber Risk Index (CRI) for the second half of 2021 revealed that 87% of the organisations in Malaysia (either public or private) has suffered one or more cyber-attacks in the preceding 12 months period (Muharram et al., 2022).

In addition to financial losses, phishing incidents have also caused organisations to suffer significant damage to their reputation and loss in competitiveness. According to the online portal, Cyber Security Hub, in 2021, it was reported that Facebook suffered data leaks totalling 533 million of its users that use its application. As a result, Facebook had to pay a USD 5 billion fine to the Federal Trade Commission (Morgan, 2022). Similarly, a tech-giant company, Google has also reported 52.5 million personal data leaks as a result of a data security breach in 2018 (Heiligenstein, 2023). In Malaysia, the recent data leaks involved 13 million of its citizens comprising 3.5 million Astro customers, 1.8 million Maybank banking users, and 7.2 million Election Commission of Malaysia (EC) personal data has led the

Ministry of Malaysian Communications and Digital to request the CyberSecurity Malaysia to investigate the incidents (Nair & Ross, 2023).

Digging deeper into the topic, a report by an accounting firm, Deloitte, stated that roughly 91% of incidents involving data breaches started with the unsuspected victim receiving a phishing e-mail requesting the recipient to either click on the link or the given attachment (Deloitte, 2020). The same report also highlighted that 32% or one-third of all successful information security breaches in organisations involved the use of phishing techniques. This shows that phishing technique is popular among cybercriminals and is also a highly effective unlawful technique to gain access to restricted data. Moreover, a study conducted by Carroll et al. (2022), found that in general, it is difficult for ordinary people to detect modern phishing e-mail attacks and that the majority of them lack confidence, are worried, and are often dissatisfied with the current technologies available to protect them against phishing e-mails.

Organisations' defence strategies against phishing attacks are usually centred on either using technological barriers as a means to prevent the phishing message from entering their information system or by educating the users on how to identify the suspicious message, therefore preventing them from replying to the message or to click on the attachment (Jain & Gupta, 2021). However, neither technological means nor education can provide truly effective protection against phishing attacks (Aldawood & Skinner, 2019; Bullee & Junger, 2020; Caputo et al., 2014; Dalal et al., 2021; Furnell et al., 2019; Gavett et al., 2017; Goel et al., 2017; Gordon et al., 2019; Heartfield & Loukas, 2016; Purkait, 2012; Sumner et al., 2021; Tschakert & Ngamsuriyaroj, 2019). Similarly, the existence and implementation of information security policies and processes within an organisation have also been unable to form an effective barrier against phishing attacks (Gupta et al., 2016; Ifinedo, 2019; Mansfield-Devine, 2018;

Siponen et al., 2014; Vance et al., 2013). This phenomenon according to Ifinedo (2019) and Vance et al. (2013) was due to certain types of individuals who were found not following the rules as laid down in the organisation's policy and processes. This according to both authors, is one of the reasons that contribute to the frequent occurrence of phishing incidents.

Therefore, it is not surprising, that despite the continuous effort by various government and private agencies through various media to educate the public on the danger of phishing, the effort seems to be unfruitful as evidenced by the frequent occurrence of reported phishing incidents in the local news. Moreover, the tactics used by cybercriminals have always changed and in most cases seems to be ahead of the organisations' and individuals' strategies for protection against phishing attempt (Bhardwaj et al., 2020; Binks, 2019; Das et al., 2022; Mansfield-Devine, 2018; Tambe Ebot, 2019; Vayansky & Kumar, 2018). As such, because of the continuous phenomenon and the mitigations being put in place also seem to be ineffective, several researchers in the field of information security believe that humans are the weakest link in the fight against phishing attacks (Aldawood & Skinner, 2018; Anawar et al., 2019, Ani et al., 2019; Asbaş, & Tuzlukaya, 2022; Darwish et al., 2012; Goel & Jain, 2018; Lebek et al., 2013; Mohebzada et al., 2012; Yang et al., 2022, Yan et al., 2018; Zhang et al., 2021).

1.2 Problem Statement

According to Abroshan et al. (2021) and Pantic and Husain (2018), individuals become susceptible to e-mail phishing attacks because they genuinely believe that such e-mails are legit. In most cases, victims are usually tempted to either click on the attachment or respond to such e-mail (Atkins & Huang, 2013; Jones et al., 2019; Qabajeh et al., 2018). To attract the attention of the potential victims to carry out such actions, the senders of the e-mails commonly called ‘phishers’, would employ the tactics of persuasion as their strategy to achieve the objective (Bayl-Smith et al., 2021; Ferreira & Teles, 2019; Koddebusch, 2022; Lin et al., 2019). In this sense, Bayl-Smith et al. (2021) and Ferreira and Teles (2019) further elaborate that based on the analysis of several phishing e-mails, the persuasion technique used by phishers can be grouped according to the Principle of Persuasion previously conceptualised by Cialdini (Cialdini, 2007). It consists of six different techniques which are authority, commitment, liking, reciprocity, scarcity, and social proof (Ferreira & Teles, 2019).

To understand, the reason why certain individuals are prone to get attracted to the persuasion techniques mentioned above, past researchers have tried to conceptualise different relationships that could be used to understand the phenomenon. These include looking from the perspective of demographic factors (such as age and gender) (Baki & Verma, 2023; Bullee et al., 2017b; Butavicius et al., 2022; Chou & Sun, 2017; Das et al., 2022; Farooq et al., 2015; Gillam & Waite 2021; Greitzer et al., 2021; Iuga et al., 2016; Li et al., 2020; McGill & Thompson 2021; Oliveira et al., 2019; Rastenis et al., 2019; Sun et al., 2016; Taib et al., 2019; Whitty, 2019), level of technical knowledge (Baki and Verma, 2023; Orunsolu et al., 2018; Parker & Flowerday, 2020; Rocha Flores et al., 2015), e-mail habits (Vishwanath, 2015; Vishwanath et al., 2016), the effectiveness of phishing awareness training (Amankwa et al., 2014; Arachchilage & Love, 2014; Carella et al., 2017; Gavett et al., 2017; Jensen et al., 2017; Weaver et al., 2021) and individual characteristics or personality traits (Anawar et al., 2019; Barman & Conlan, 2021; Eftimie et al., 2022; Frauenstein & Flowerday 2020; Ge et al., 2021; Hong et al., 2013; Lawson et al., 2020; Yang et al., 2022).

However, among the several factors mentioned above, it seems that the main determinant that can link different individuals with different types of persuasion techniques is their unique characteristics or personality traits. This evidence is not only limited to phishing studies but also has been proved in other non-information security studies. This includes the general study of human behaviour (Oyibo et al., 2017; Oyibo et al., 2018; Wall et al., 2019), social media advertising (Winter et al., 2021), and healthcare (Nofal et al., 2020). This shows that in general, relationships exist between individual personality traits and persuasion techniques. In other words, individuals become susceptible to certain types of persuasion tactics as a result of their inherent characteristics (Lawson et al., 2017).

Despite acknowledging that individuals' personality traits do have a role in influencing the individual decision to either reply or to click the attachment related to suspicious e-mails, previous studies on the issue have not been able to provide reasons why such relationships exist. Although several previous studies such as those conducted by Frauenstein and Flowerday (2020), Hamoud et al. (2022), Harrison et al. (2015), Musuva et al. (2019), Parker and Flowerday (2020) and Vishwanath et al. (2011) did attempt to explain the phenomenon by incorporating the individual information processing characteristics as the intervening variables between the variable of interest (e.g., personality traits) and an individual's phishing susceptibility, the findings of the study are still inconclusive. As an example, in a study by Frauenstein and Flowerday (2020), the findings revealed that information processing theory can only be used to explain a few of the five personality traits' relationships with persuasion techniques.

This situation presents a gap that needs to be investigated to further our understanding of the relationships between the two variables. This is significant as the inability to address the gap sufficiently will lead to individuals and organisations being unable to put forth the necessary barriers to mitigate phishing threats. Therefore, any further research needs to consider other factors or variables that can act as an intervention between the two variables. To address the above gap, this study has adopted the Protection Motivation Theory (PMT) as a mediator to be tested in relationships between personality traits and individual susceptibility to phishing as a result of the persuasion technique. The decision to adopt the PMT as the mediator was based on previous studies in other disciplines that have looked at PMT as an intervention between personality traits and construct of interest. This includes the field of health science (Pilch et al., 2021), marketing (Ioannou et al., 2021), mobile app information systems (Chennamaneni & Gupta, 2022), and prison system (Leszko et al., 2020). The findings from these studies have been encouraging in the sense that the researchers have been able to use PMT as an additional factor to explain those relationships.

Separately, PMT has also been used extensively in studies related to information security. In this sense, the majority of the studies involved utilising PMT as the independent variable of the phishing issue being studied. For example, studies by Verkijika (2018) used PMT as an independent variable to study the understanding of smartphone security behaviours, and Lau et al. (2020) used PMT as the independent variable to examine mobile device users’ information security behaviour. On the other hand, one example of a study that used PMT as the mediator is De Kimpe et al. (2021) who utilise PMT to study the relationship between perceived knowledge about online risk and trust in internet safety as independent variables and intention to take a protective measure which is the dependent variable. However, to the knowledge of the current researcher, none of the studies reviewed so far involves incorporating the PMT simultaneously in direct relationships or as the mediator between personality traits and persuasion techniques in the context of an individual’s phishing susceptibility. As such, there is a need to conduct further studies that examine both relationships to establish the role of PMT in an individual’s phishing susceptibility.

In phishing research, PMT is typically used to connect people’s motivation to their perceptions of phishing threats (Jansen & Van Schaik, 2019; Sommestad et al., 2015; Verkijika, 2019) and security measures (Bayl-Smith et al., 2021; Van Bavel et al., 2019; Thomas, 2018), including how effective those measures are at preventing phishing. Users’ beliefs about their security are a driving factor in determining how vulnerable they will be to phishing attacks. This may seem like an obvious point, but research has shown that people’s perceptions of phishing threats and security measures vary greatly depending on their unique qualities or personality factors (Lau et al., 2020). As a result, no two people will likely have the same perspective on the gravity of phishing risks or the same set of responses. This is supported by research from various academic fields. For instance, Pilch et al. (2021) observed that individuals with the trait of agreeableness had a greater likelihood of believing they could effectively manage the threat posed by COVID-19 and thereby avoid becoming infected with the virus. Neurotic people, on the other hand, often mistakenly believe that they are the ones acting in opposition to others who exhibit agreeableness (Pilch et al., 2021).

The other aspect that needs to be considered is the effect of cultural differences on the perspective of the relationships between personality traits, PMT, and susceptibility to phishing through persuasion. This is significant because, except for the recent study by Sulaiman et al. (2022), all of the other studies conducted involving all or any of the three variables are done in a different culture than in Malaysia, for example in Australia (Bayl-Smith et al., 2021), New Zealand (Shahbaznezhad et al.,