

2021

## **An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breaches**

Nisha Jatin Patel

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)



Part of the [Computer Engineering Commons](#), and the [Computer Sciences Commons](#)

### **Share Feedback About This Item**

---

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

An Empirical Assessment of Users' Information Security Protection Behavior  
towards Social Engineering Breaches

by

Nisha Patel

A dissertation submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in  
Information Systems

College of Computing and Engineering  
Nova Southeastern University

2021

We hereby certify that this dissertation, submitted by Nisha Patel conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



\_\_\_\_\_  
Ling Wang, Ph.D.  
Chairperson of Dissertation Committee

9/7/21

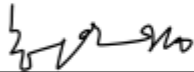
\_\_\_\_\_  
Date



\_\_\_\_\_  
Wei Li, Ph.D.  
Dissertation Committee Member

9/7/21

\_\_\_\_\_  
Date



\_\_\_\_\_  
Inkyoung Hur, Ph.D.  
Dissertation Committee Member

9/7/21

\_\_\_\_\_  
Date

Approved:



\_\_\_\_\_  
Meline Kevorkian, Ed.D.  
Dean, College of Computing and Engineering

9/7/21

\_\_\_\_\_  
Date

College of Computing and Engineering  
Nova Southeastern University

2021

An Abstract of a Dissertation Submitted to Nova Southeastern  
University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

## An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breach

by  
Nisha Patel  
September 2021

User behavior is one of the most significant information security risks. Information Security is all about being aware of who and what to trust and behaving accordingly. Due to technology becoming an integral part of nearly everything in people's daily lives, the organization's need for protection from security threats has continuously increased. Social engineering is the act of tricking a user into revealing information or taking action. One of the riskiest aspects of social engineering is that it depends mainly upon user errors and is not necessarily a technology shortcoming. User behavior should be one of the first apprehensions when it comes to social engineering. Unfortunately, there are few specific studies to understand factors that affect users' information security protection behavior towards social engineering breaches.

The focus of the information security literature is shifting from technology to user behavior in recent times. SETA (Security Education Training Awareness) program aids organizations in teaching their users about information security issues and expectations to prevent information security breaches. Information security policies depict the rules and regulations that everyone must follow utilizing an organization's information technology resources. This research study used Protection Motivation Theory (PMT) combined with the SETA program and security policies to determine factors that affect users' information security protection behavior towards social engineering breaches. This research study was an empirical and quantitative study to congregate data utilizing a web survey and PLS-SEM (Partial Least Squares Structural Equation Modeling) technique. As a result, the research study supported all three hypotheses associated with fear, including a positive impact of perceived severity on fear, perceived vulnerability on fear, and fear on protection motivation. Moreover, the research study substantiated the positive impact of perceived severity, perceived vulnerability, and response efficacy on protection motivation. Furthermore, the research study also confirmed the positive impact of protection motivation and the SETA program on protection behavior.

The findings of this research study derived that, unswerving with the literature, social engineering has arisen as one of the biggest threats in information security. This research study explored factors impacting users' information security protection behavior towards social engineering breaches. Support of all hypotheses for fear appeal is a substantial

contribution in view of a lesser-researched fear appeal in preceding research using PMT. This research study provided the groundwork for encouraging and nurturing users' information security protection behavior to prevent social engineering breaches. Finally, this research study contributes to the increasing phenomenon of social engineering in practice and future research.

## **Acknowledgments**

Above all, I would like to convey thanks to my two wonderful sons for filling my life with joy and laughter. Countless thanks to my husband for his unwavering love. I wish to express my gratitude to my mother and father for their unconditional support. I am grateful to my brother, sister-in-law, niece, and nephew for their unfaltering care.

I wish to thank all the teachers and mentors who inspired me with this journey. I found the nugget of information I was seeking from them.

My utmost appreciation and thankfulness to my committee members, Dr. Inkyoung Hur, and Dr. Wei Li, for taking the time to review my effort and believing in me with their continuous support. The support Dr. Hur and Dr. Li provided has been nothing short of amazing.

Ultimately, I would like to thank my advisor, Dr. Ling Wang, for her endurance and thoughtfulness. Her constant communication, guidance, and sustenance are encouraging and invaluable to me. She continually stood by me and led me to realize my potential. It has been a distinct honor to collaborate with her.

# Table of Contents

**Abstract** iii  
**Acknowledgments** v  
**List of Tables** ix  
**List of Figures** xi

## Chapters

### **1. Introduction 1**

Background 1  
    Information Security 1  
    Social Engineering 1  
    Protection Behavior 3  
Problem Statement 3  
Dissertation Goal 5  
Research Model 7  
Research Question 11  
Hypotheses 11  
Relevance and Significance 19  
Barriers and Issues 19  
Assumptions, Limitations, and Delimitations 20  
    Assumptions 20  
    Limitations 20  
    Delimitations 21  
Definition of Terms 21  
List of Acronyms 23  
Summary 24

### **2. Review of the Literature 25**

Introduction 25  
Information Security 25  
Social Engineering 26  
SETA Program 29  
Security Policies 30  
Protection Motivation Theory (PMT) 30  
    Perceived Severity 32  
    Perceived Vulnerability 32  
    Fear 32  
    Maladaptive Rewards 33  
    Response Efficacy 33  
    Self-efficacy 34  
    Response Cost 34  
    Protection Motivation 35  
    Protection Behavior 35

Utilization PMT and Information Systems Literature 36  
Gaps in PMT and Information Systems Literature 38  
Summary 39

### **3. Methodology 41**

Introduction 41  
Research Design Overview 41  
Research Methodology 42  
    Human Ethical Attention 42  
    Delphi Method Study 42  
    Data Collection 43  
Instrument Development and Validation 43  
    Instrument Reliability and Validity 44  
    Internal Consistency Reliability 44  
    Construct Validity and Content Validity 44  
    Convergent Validity 44  
    Discriminant Validity 45  
Sample 45  
    Sampling Type 45  
    Sampling Recruitment 45  
    Sampling Size 46  
    Descriptive Statistics 46  
Data Analysis 47  
    Pre-analysis Screening 47  
    Common Method Bias 48  
    Partial Least Squares Structural Equation Modeling 48  
Formats for Presenting Results 49  
Resource Requirements 49  
Summary 49

### **4. Results 51**

Introduction 51  
Survey Validation and Delphi Study 51  
Data Collection 52  
Data Screening 53  
    Mahalanobis Distance 53  
    Normality Test 54  
Demographics 55  
Data Analysis 57  
Measurement Model 57  
    Convergent Validity and Outer Loadings 57  
    Construct Reliability and Validity 60  
    Discriminant Validity 61  
    Model Fit 66  
Structural Model 67  
    Collinearity 67



Path Coefficients 68  
Hypothesis Summary 70  
Total Effects 73  
Coefficient of Determination 74  
Effect Size 75  
Predictive Relevance 76  
Important-Performance Map Analysis 77  
PLS Predict 77  
Summary 78

## **5. Discussion, Limitations, Implications, Recommendations, and Conclusion 80**

Introduction 80  
Discussion 80  
    Influences on Fear 81  
    Influences on Protection Motivation 82  
    Influences on Protection Behavior 85  
    Support for the Research Model 86  
    Support for the Research Question 87  
Limitations 87  
Implications 88  
    Contributions to Theory 88  
    Contributions to Practice 89  
Recommendations 90  
Conclusion and Thesis Summary 91

## **Appendices**

A. Summary of Measurement Items 94  
B. Summary of Reliability Evidence 100  
C. IRB Approval 101  
D. Participant Email Message 102  
E. Participant Survey 103  
F. Mahalanobis Distance and Stem & Leaf Plot 118  
G. Return of Mahalanobis Distance and Stem & Leaf Plot after removal of 5 extreme values 122  
H. Normality and Scatter Plot 126  
I. Additional Comments 129

## **References 133**

## **List of Tables**

### **Tables**

1. Summary of Constructs used 18
2. Participants Demographic and Background Questions 47
3. Participants Gender Demographics 55
4. Participants Age Demographics 55
5. Participants Education Demographics 56
6. Participants Social Engineering Breach Exposure Demographics 56
7. Initial Outer Loadings 58
8. Final Outer Loadings 59
9. Construct Reliability and Validity 60
10. Cross-Loadings of Threat Appraisal Items 62
11. Cross-Loadings of Coping Appraisal Items 63
12. Cross-Loadings of Protection Items 64
13. Fornell-Larcker Criterion 65
14. Heterotrait-Monotrait Ratio (HTMT) 66
15. Model Fit 67
16. Collinearity Statistics (VIF) 68
17. Path Coefficients 69
18. Hypothesis Summary 73
19. Total Effects 74
20. R Square 75

21. f Square 76

22. Q Square 76

23. PLS Predict Assessment 78

## **List of Figures**

### **Figures**

1. Proposed Research Model 11
2. Final Research Model 70
3. Important-Performance Map Analysis (IPMA) 77

# Chapter 1

## Introduction

### Background

#### *Information Security*

Society, organizations, and governments have become increasingly reliant on information technology (D'Arcy & Hovav, 2008; Guo, Yuan, Archer, & Connelly, 2011; Siponen & Vance, 2014). Moreover, information security breaches, a murkier side of information technology, are tough to identify, impeach, and become more sophisticated due to technology advancements (D'Arcy, Herath, & Shoss, 2014; Hovav & D'Arcy, 2012; Ifinedo, 2014). As the attacking techniques are getting more automated, hacking tools are increasingly available free of charge, and besides, skills required to perform attacks are becoming lesser significant (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Dhillon & Backhouse, 2001; Straub & Welke, 1998).

#### *Social Engineering*

Scholars have defined social engineering as "the psychological manipulation of people in order to gain access to a system for which the attacker is not authorized" (Bhakta & Harris, 2015, p. 424). Social engineering is a technique used to manipulate users steered by a cybercriminal to access confidential information or executing an action to enable a cyberattack (Alazri, 2015; Osuagwu & Chukwudebe, 2015). Social engineering (SE) is a crucial area of information security. Social Engineering manipulates people to compromise information security (Brody, Brizzee, & Cano, 2012; Malfaz & Salichs, 2011; Tetri & Vuorinen, 2013). Users are considered the weakest link in information security (Butler, 2007;

Dinev & Hu, 2007; Warkentin & Willison, 2009). Social engineering attackers begin with the target or their associate obtaining specific physical and emotional attributes of a person (Heartfield & Loukas, 2015; Mansfield-Devine, 2016; Meguerdichian, Koushanfar, Qu, & Potkonjak, 2001). Social engineers target people who have access to systems or other people, persuading them into revealing confidential information or influencing them to carry out steps for the attacks (Brody et al., 2012; Bullée, Montoya, Pieters, Junger, & Hartel, 2015; Heartfield & Loukas, 2015).

Information security attacks and information misuse result in significant financial losses to users, businesses, government, and organizations (D'Arcy, Hovav, & Galletta, 2009; Herath & Rao 2009a; Saleem, 1996). Social engineering has emerged as a severe threat due to a shortage of visibility about information collected by social engineering attacks combined with an exponential increase of risk associated with social engineering (Acquisti, Brandimarte, & Loewenstein, 2015; Mitnick & Simon, 2002; Tetri & Vuorinen, 2013). A social engineering attacker can use the most prominent instrument of manipulating people into giving organizational information (Loch, Carr, & Warkentin, 1992; McCoy, Park, Shi, & Jakobsson, 2016; Tetri & Vuorinen, 2013).

It is possible to execute social engineering on a large scale, and multinational companies and government organizations are victims of these attacks (Bélanger & Crossler, 2011; McCoy et al., 2016). Accordingly, organizations design and implement SETA (Security Education Training Awareness) program and security policies for security awareness training, ongoing communication of security policies, reminders for changing passwords, spreading mindfulness of penalties involved in security misuse, and prompt response

cognizance in case of a social engineering breach (Chen, Ramamurthy, & Wen, 2012; Straub & Welke, 1998).

### *Protection Behavior*

Every time users interact with technology, there is a possibility of a user error (Boss et al., 2009; Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Ng, Kankanhalli, & Xu, 2009).

However, what is thought-provoking is that every user could fall for a social engineering attack (Cram, Proudfoot, & D'Arcy, 2017; Herath & Rao, 2009b; Straub, 1990).

Notwithstanding all technological advances in information security, user behavior plays an important part, as most users do not comprehend how to safeguard critical information and digital assets (Komatsu, Takagi, & Takemura, 2013; Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Straub & Welke, 1998). Nonetheless, information security technology alone is not sufficient to mitigate information security risks; protection behavior remains a central aspect in information security and should not be underestimated (Cram, Proudfoot, & D'Arcy, 2017; Dhillon & Backhouse, 2001; Straub & Welke, 1998).

### **Problem Statement**

Social engineering attacks defraud executives out of the organization's money and results in substantial financial losses for a significant number of organizations (Brody et al., 2012; Zweighaft, 2017). Therefore, this study addressed the research problem by identifying factors impacting users' information security protection behavior towards social engineering breaches. This research study was built on previous research by Hong and Thong (2013) and Wolff (2016), who recommended that social engineering risks, threats, features, actions, and responses need significant attention. There is an increasing need to protect organizations from ongoing threats and prevent social engineering attacks (Bélanger & Crossler, 2011;

Bullée et al., 2015). At the same time, social engineering breaches continue to increase in complexity and impact (Bullée et al., 2015; Johnston & Warkentin, 2010).

Social engineering breaches can be disastrous for an organization's brand image and reputation in the industry (Goode, Hoehle, Venkatesh, & Brown, 2017). Bélanger and Crossler (2011) cautioned that organizational resources are reactive to social engineering breaches rather than proactive. Even though many social engineering risks result in financial losses, organizations are under-secured, the social engineering problem has remained under-researched and unresolved (Jakobsson, 2016; Willison & Warkentin, 2013). Thus, there is an imperative need to comprehend and examine countermeasures and means to prevent social engineering risks (Hu, Dinev, Hart, & Cooke, 2012).

Social engineers manipulate users into giving information (Krombholz, Hobel, Huber, & Weippl, 2015; Tetri & Vuorinen, 2013). Users' usage and a violation of security policies can breach security (Benson, Saridakis, & Tennakoon, 2015). Internal user behavior was the cause of 34% of security breaches (McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017). Technical actions alone are insufficient to safeguard an organization's information security (InfoSec); there is a more significant emphasis required on the human aspects of InfoSec (McCormac et al., 2017). While users are among the leading causes of security breaches, insider threats are not easy to avoid and prevent (Wang, Gupta, & Rao, 2015). Algarni, Xu, and Chan (2017), Bullée et al. (2015), as well as Heartfield and Loukas (2015) recommended that users' information security protection behavior towards social engineering breaches need additional attention and research.

Despite what the prior research studies have explored and resolved, social engineering is still a significant problem (Algarni et al., 2017; Kaushalya, Randeniya, & Liyanage, 2018).



Numerous studies focused on various aspects of social engineering. Nevertheless, most of these studies have not engrossed in users' behavioral responses to the imposed social engineering attacks. There was a discrepancy in the existing research on users' beliefs and perceptions that impact their behavioral responses to social engineering attacks. Previous studies had not explored factors that influence users' information security protection behavior towards social engineering breaches.

Therefore, it appeared that additional investigation on factors that affect users' information security protection behavior towards social engineering breaches was necessary (Algarni et al., 2017; Kaushalya et al., 2018). Boss, Galletta, Lowry, Moody, and Polak (2015) proposed using fear appeals in the PMT to motivate users and deter information security breaches.

There was a solid need for further exploration and research on well-formulated SETA program and well-aligned security policies for the overall IS (information systems) strategy to keep organizational information assets and resources safe from dire attacks (D'Arcy & Hovav, 2007; Kankanhalli, Teo, Tan, & Wei, 2003; Lee, Lee, & Yoo, 2004). There was no published research to determine the effects of perceived severity, perceived vulnerability, fear, maladaptive rewards, response efficacy, self-efficacy, perceived response costs, SETA program, security policies, and protection motivation on users' information security protection behavior to prevent social engineering breaches using PMT.

### **Dissertation Goal**

This research study's main goal was to perform an empirical verification of the factors contributing to users' information security protection behavior. This research study developed a model that entails the full nomology of Protection Motivation Theory (PMT) combined with the SETA program and security policies to test the hypotheses on the constructs.

Additionally, this research study developed an integrated SETA program and security policies model under the umbrella of PMT theory full nomology (D'Arcy & Herath, 2011). It assisted in cumulative theory-building initiatives to improve the information security arena and prevent social engineering breaches (Herath & Rao, 2009b).

Initially discovered by Rogers (1975), PMT has become a gold standard for health-related behavior research, discovery, and exploration. PMT was originally established to elucidate the impacts of fear appeals on health motivation and behaviors (Rogers, 1975). PMT shows how individuals are inspired to respond to dangerous situations, named fear appeals (Boss et al., 2015). PMT describes that individuals use a cognitive process combining threat and coping appraisals to interpret and respond to dangerous situations (Boss et al., 2015).

PMT was adapted to understand what motivates individuals to adopt security policies (Johnston, Warkentin, & Siponen, 2015) and espouse authentication services (Yang, Zhang, & Lanting, 2017). PMT has been utilized to exhibit online privacy protection behavior (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009) and employ anti-malware software (Johnston & Warkentin, 2010; Lee & Larsen, 2009).

There are various enhancements and extensions implemented in the information security field over time. PMT has core nomology and full nomology. The PMT core nomology is the same as the full nomology, except that core nomology does not include the two constructs, fear and maladaptive rewards (Boss et al., 2015). Boss et al. (2015) found that "typically, ISec studies omit core PMT concepts or fear-appeal manipulations without explanation" (p. 9). Boss et al. (2015) argued that the misrepresentation of the PMT presents a substantial issue for information security researchers as such:

Our careful review of the foundation for PMT identified three opportunities for improving ISec PMT research. First, extant ISec studies do not use the full nomology of PMT constructs. Second, only one study uses fear-appeal manipulations, even though these are a core element of PMT, and virtually no ISec study models or measures fear. Third, whereas these studies have made excellent progress in predicting security intentions, none of them have addressed actual security behaviors (p. 2).

This research study, therefore, utilized the full nomology of PMT to develop its research model. It was worthwhile to further investigate the PMT in combination with the SETA program and security policies in the context of social engineering.

### **Research Model**

PMT is a valuable groundwork for explaining how individuals use a cognitive method to decide security behavior to respond to insecure conditions (Boss et al., 2015). It offers a comprehensive understanding of why individuals may not execute recommended protective behaviors against social engineering threats (Herath & Rao, 2009b). This understanding improves educational, training, and awareness resources to respond to social engineering breaches (Lee, Larose, & Rifon, 2008). Although the information security domain utilized PMT widely, there was an additional need for empirical research studies performed in social engineering (Lee & Larsen, 2009; Tetri & Vuorinen, 2013). This research model utilized PMT in social engineering (Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013).

Although the extant research studies in the information security area used many PMT concepts, most of them did not use the full nomology of PMT (Boss et al., 2015). In the information security literature, researchers have incorporated PMT by utilizing fragments of it

(Johnston & Warkentin, 2010). Extant research studies omitted constructs from the full nomology of PMT (Liang & Xue, 2010). Previous research studies omitted constructs such as response costs and maladaptive rewards, missing out on utilizing the benefit of full nomology of PMT (Alashoor, Han, & Joseph, 2017). This research study utilized the full nomology of PMT to incorporate comprehensive analysis and understand the impact of every construct (Floyd, Prentice-Dunn, & Rogers, 2000).

PMT is logically suitable for information security research where fear inspires users to exhibit protection behaviors (Milne, Sheeran, & Orbell, 2000). Fear provocation happens as a retort to circumstances adjudicated as unsafe and protective behavior is exhibited to prevent it (Rogers 1975). PMT includes fear and provides information about users' ability to cope with the threat in a productive way (Floyd et al., 2000). Neglecting fear from the information security research study utilizing PMT could weaken the results; hence, this study included fear in the research model (Boss et al., 2015).

Many information security research utilizing PMT used protection motivation as the research model's dependent construct (Boss et al., 2015). PMT can predict both protection motivation and protection behavior, as reinforced by Sommestad, Karlzén, and Hallberg (2015). Extant research studies utilizing PMT in the health area have addressed actual behaviors in addition to intentions (Milne et al., 2000). Actual behaviors and intentions need to be studied for social engineering because behaviors also need to be improved and not just intentions (Boss et al., 2015). This research study went beyond protection motivation and incorporated the relationship between protection motivation and protection behavior to prevent social engineering breaches (Floyd et al., 2000).

To carry out security policy and increase protection behaviors of users, organizations implement a comprehensive SETA program (D'Arcy & Herath, 2011; Johnston et al., 2015). Nurturing a security culture that inspires robust and well-aligned SETA program and security policies should help reduce information misuse and increase protection behavior in the workplace (D'Arcy & Hovav, 2007; Herath & Rao 2009b). Therefore, this research model analyzed the impacts of SETA program and security policies on protection behavior to prevent security engineering breaches.

The cognitive mediating method comprises of two distinct processes: the threat appraisal process (perceptions of how endangered an individual feels) (Liang & Xue, 2009) and the coping appraisal process (perceptions of the recommended coping response to the danger) (Floyd et al., 2000). This research study made use of PMT (Maddux & Rogers, 1983; Rogers, 1975), which propositions that an individual's perceived vulnerability and the severity will influence the level of fear experienced.

Fear and rewards will influence the execution of behaviors to protect against danger. These factors make the threat appraisal component of the model. Furthermore, response efficacy, self-efficacy, and response costs will influence an individual's protection motivation to perform protection behaviors. These factors make the coping appraisal component of the model. The anticipated paybacks of not executing protection behaviors against social engineering threats and the expected costs to be experienced by executing protection behaviors may negatively influence users' protection motivation.

Threat appraisal in this research model includes fear appeal (how individuals respond to unsafe circumstances) (Milne et al., 2000), maladaptive rewards (paybacks from not exhibiting the protection behavior) (Slovic & Peters, 2006), perceived severity (individual

judging the scale of the danger) (Maddux & Rogers, 1983), and perceived vulnerability (individual deciding own susceptibility to the danger) (Liang & Xue, 2010). The coping appraisal includes response efficacy (the individual's belief in the perceived effectiveness of the protective action) (Anderson & Agarwal, 2010), response cost (perceived cost to the individual in exhibiting the protection behavior) (Rogers, 1975), and self-efficacy (the individual's belief in own capability to exhibit the protection behavior) (Herath & Rao, 2009b).

The research model included eleven constructs that determine the users' information security protection behavior towards social engineering breaches. Four of these constructs, perceived severity, perceived vulnerability, fear, and maladaptive rewards, made up the user's threat appraisal. Response efficacy, self-efficacy, and response costs made up the user's coping appraisal. This research model went beyond the nomological model of the PMT by introducing vital precursors SETA program and security policies. The SETA program and security policies were two additional constructs utilized in addition to PMT constructs.

Figure 1 shows the proposed research model.

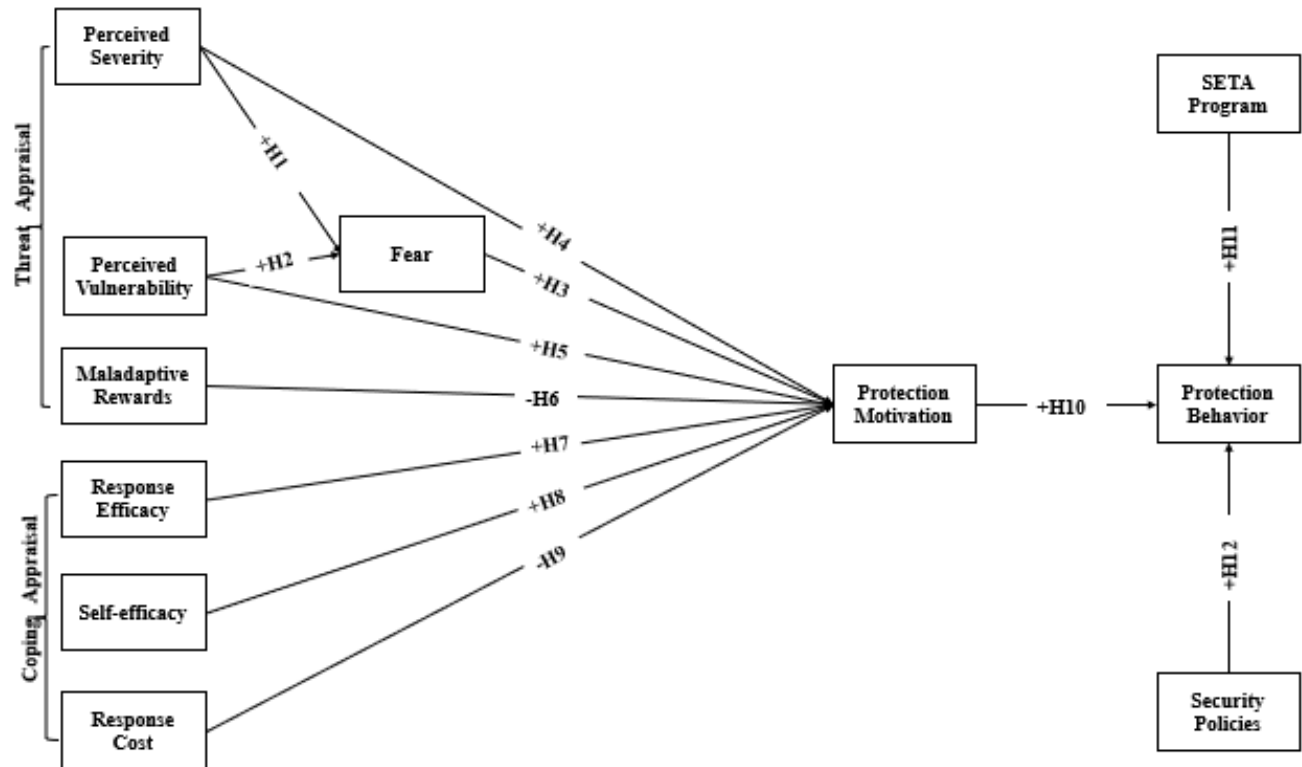


Figure 1: Proposed Research Model

## Research Question

This research study addressed the following main research question:

*RQ: What are the factors influencing the users' information security protection behavior towards social engineering breaches?*

## Hypotheses

In this research study, perceived severity signified the brutality of the social engineering breach and the possible losses caused by the organization's breach. PMT accentuates the impacts created by persuasive communications to influence people's behavior in a determined manner (Rogers, 1975). Similarly, the scope of PMT includes factors that influence motivation that, in turn, affect behavior (Rogers, 1975). In this research study, a social engineering breach is considered the users' perceived threat. The PMT suggested that perceived severity directly affects fear (Rogers, 1975). The higher the threat's perception to

be more serious, the higher the fear appeal for the danger (Maddux & Rogers, 1983). Correspondingly, the more severe the threat to a user is, the more fear the user would entuse (Milne et al., 2000). Boss et al. (2015) noted that there is a positive relationship between perceived severity and fear. Therefore, hitherto background and the positive association between perceived severity and fear resulted in the following hypothesis:

***H1: Perceived severity is positively associated with fear.***

In this research study, perceived vulnerability signified users' assessment of whether their organization was susceptible to social engineering breaches without following security measures. The PMT suggested that perceived vulnerability directly impacted fear (Floyd et al., 2000; Marett, McNab, & Harris, 2011). The higher the perception of threat likely to happen, the higher the users' emotional response towards the threat (Floyd et al., 2000). Boss et al. (2015) noted a positive relationship between perceived vulnerability and fear. Consequently, the background up until now and the positive association between perceived vulnerability and fear gave rise to the following hypothesis:

***H2: Perceived vulnerability is positively associated with fear.***

Fear is a negative emotion that rises from diagnosing threats in social engineering breaches (Rogers, 1975). The more significant the threat, the more probable users would be motivated to protect themselves from a social engineering breach (Milne et al., 2000). Raising fear can result in a user taking additional protection actions (Rogers, 1975). Consequently, if users feel that the negative consequences of a given security threat are severe and likely to occur, they would be more motivated to perform suggested protection behaviors.



Users who emphasize controlling dangers of information security risk are more motivated to mitigate the origin of the danger. Fear becomes a motivator based on positive coping responses (Burns, Posey, Roberts, & Lowry, 2017). Burns et al. (2017) and Posey, Roberts, and Lowry (2015) noted a positive relationship between fear and protection motivation. So, hitherto background and the positive association between fear and protection motivation brought about the following hypothesis:

***H3: Fear is positively associated with protection motivation.***

In this research study, perceived severity is social engineering breach's apparent impact. According to the PMT, the higher the user's belief that social engineering breaches will cause danger, the user is more motivated to adhere to information security compliance (Rogers, 1975). Past research demonstrated that perceived severity positively influences users' security measures (Dang-Pham & Pittayachawan, 2015). Similarly, when a user faced a condition that induces fear, the user may find that espousing the necessary measure will resolve the situation (Boss et al., 2015). These results are reliable with other research studies that demonstrated security concerns positively influence security attitudes, positively affecting motivation to follow security measures (Anderson & Agarwal, 2010). Vance, Siponen, and Pahnla (2012) noted a positive relationship between perceived severity and protection motivation. Accordingly, the background up until now and the positive association between perceived severity and protection motivation led to the following hypothesis:

***H4: Perceived severity is positively associated with protection motivation.***

In this research study, perceived vulnerability is the likelihood that an unwanted breach will occur without following security measures. PMT states that the higher the perception of a threat, the more the users will adapt to the desired behavior. Perceived vulnerability is a

users' belief in their chance of undergoing a threat. Posey et al. (2015) noted a positive relationship between perceived vulnerability and protection motivation. Subsequently, the context up until now and the positive association between perceived vulnerability and the protection motivation directed to the following hypothesis:

***H5: Perceived vulnerability is positively associated with protection motivation.***

Users exhibit maladaptive responses when they believe that failing to adapt outweighs the adaptation (Burns et al., 2017). Saving time is often considered a maladaptive reward in prior information security compliance research (Vance et al., 2012). Youn (2009) substantiated that the higher the maladaptive rewards lower the protection motivation. Both Burns et al. (2017) and Boss et al. (2015) noted a negative relationship between maladaptive rewards and protection motivation. So, hitherto background and the negative association between perceived maladaptive rewards and protection motivation brought about the following hypothesis:

***H6: Maladaptive rewards are negatively associated with protection motivation.***

In this research study, response efficacy signified users' confidence that specific behaviors would allow them to prevent social engineering breaches. Users' perceptions of an anticipated response's efficacy motivate them to exhibit desired behavior (Bandura, 1977). Jayanti and Burns (1998) discovered outcome benefits to play a substantial part in the motivation to perform the expected actions. Therefore, if users distinguish that a recommended security measure is easy to exhibit but expects the results of using such measure to be inefficient, they may not perform security measures (Compeau & Higgins, 1995).

Kumar, Park, and Subramaniam (2008) found that response efficacy positively correlates with executives' motivation to adopt security countermeasures. Johnston and Warkentin (2010) noted a positive relationship between response efficacy and protection motivation. Consequently, hitherto background and the positive association between response efficacy and protection motivation brought about the following hypothesis:

***H7: Response efficacy is positively associated with protection motivation.***

In this research study, self-efficacy referred to users' belief that they can efficaciously fulfill information security policies, preventing social engineering breaches. Bandura (1977) initially perceived the notion of self-efficacy. Self-efficacy underscores users' judgment of their capabilities to adhere to information security policies (Bandura, 1977). Likewise, self-efficacy was positively related to motivation for behaviors (Bandura, Adams, Hardy, & Howells, 1980). Self-efficacy beliefs result in protection motivation towards information security policies (Boss et al., 2015). Johnston and Warkentin (2010) noted that there is a positive relationship between self-efficacy and protection motivation. Thus, background up until now and the positive association between self-efficacy and protection motivation directed the following hypothesis:

***H8: Self-efficacy is positively associated with protection motivation.***

PMT theorizes that as the response cost increases, the prospect of exhibiting the adaptive coping response decreases. Prior IS research has found support in this matter. Kumar et al. (2008) validated that the executive's security compliance motivation lowered when response cost increased. In this research study, response cost included the inconvenience incurred in complying with information security policies to prevent social engineering breaches.

Furthermore, response cost is associated with apprehensions about how much it would cost to perform the recommended protection response (Milne et al., 2000).

Response cost includes financial costs, the cognitive effort associated with a protective countermeasure, the time required to implement the protection behaviors, expense, inconvenience, difficulty, side effects, lost business, or opportunity cost (Burns et al., 2017). The higher the response cost, the less motivated a user is to perform a behavior to protect from social engineering breaches (Burns et al., 2017). Vance et al. (2012) noted a negative relationship between response cost and protection motivation. So, hitherto context and the negative association between response efficacy and protection motivation led to the following hypothesis:

***H9: Response cost is negatively associated with protection motivation.***

Venkatesh, Morris, Davis, and Davis (2003) noted that intentions are good predictors for the actual behavior, which, in the context of this research study, is users' information security protection behavior to prevent social engineering breaches. The intention to follow information security procedures leads to compliance with information security (Fishbein & Ajzen, 1975). In addition, users' intention to exhibit the behavior of their interest determines their actual behavior (Dinev & Hu, 2007). Intentions may capture the motivation that stimulus a behavior, showing how hard users will perform a specific behavior (Ajzen, 1991). Therefore, context up until now and the positive association between protection motivation and protection behavior gave rise to the following hypothesis:

***H10: Protection motivation is positively associated with protection behavior.***

The SETA program strengthens adequate security guidelines and accentuates a breach's potential significances to improve users' information security protection behavior (D'Arcy et

al., 2009; Posey et al., 2015). In addition, the greater the SETA program, the more motivated a user is to perform a behavior to protect from social engineering breaches (D'Arcy & Hovav, 2007; Posey et al., 2015; Puhakainen & Siponen, 2010). Subsequently, hitherto background and the positive association between SETA program and protection motivation resulted in the following hypothesis:

***H11: SETA program is positively associated with protection behavior.***

Security policies cover rules, procedures, and guidelines for the appropriate and inappropriate usage of information assets, resources, and systems, as well as penalties for improper usage (D'Arcy et al., 2009; Kankanhalli et al., 2003). Furthermore, security policies provide rules to the users regarding what to do and what not to do (D'Arcy & Herath, 2011; Moody, Siponen, & Pahlila, 2018; Straub & Welke, 1998). Due to its detailed guidelines, a more advanced security policy results in higher user protection behavior (D'Arcy et al., 2009; Lee et al., 2004). Therefore, the greater the security policies, the more protection behavior users will exhibit toward social engineering breaches (D'Arcy & Hovav, 2007; Herath & Rao 2009b). Accordingly, background up until now and the positive association between security policies and protection motivation brought about the following hypothesis:

***H12: Security policies are positively associated with protection behavior.***

Table 1 demonstrated the constructs of the hypotheses of this research study.

Table 1

*Summary of Constructs used*

Constructs	Definition	References
Perceived severity	How serious the users believe that the social engineering breach would be to themselves	Boss et al., 2015; Floyd et al., 2000
Perceived vulnerability	How personally susceptible a user feels to the apparent social engineering threat	Boss et al., 2015; Floyd et al., 2000
Fear	A negative emotion representing a response that arises from recognizing social engineering danger	Boss et al., 2015; Posey et al., 2015
Maladaptive rewards	Purposefully avoiding a danger-control response in response to social engineering fear appeal and choosing a behavior that is not protective against the social engineering danger raised in the fear appeal	Boss et al., 2015; Burns et al., 2017
Response efficacy	The belief that the adaptive response will work and taking the protection action will help protect the self or others from social engineering breach	Boss et al., 2015; Johnston & Warkentin, 2010
Self-efficacy	The perceived ability of the individual to carry out the adaptive response for social engineering breach	Boss et al., 2015; Johnston & Warkentin, 2010
Response Cost	Any costs associated with taking the adaptive coping response for social engineering breach	Boss et al., 2015; Vance et al., 2012
SETA Program	SETA (Security Education Training Awareness) program aims to reduce the organization's security risk and increase the ability to prevent social engineering breaches	Posey et al., 2015
Security Policies	Security policies provide comprehensive direction to users regarding acceptable use of organizational information assets and resources	D'Arcy & Hovav, 2007
Protection Motivation	One's intentions to protect oneself from the social engineering breach	Boss et al., 2015; Johnston & Warkentin, 2010; Vance et al., 2012
Protection Behavior	Purposefully choosing a danger-control response in response to a social engineering threat and choosing a behavior that protects against the social engineering breach	Boss et al., 2015; Dinev & Hu, 2007; Venkatesh et al., 2003

## **Relevance and Significance**

Technology on its own is inadequate in the arena of information security, and researchers have started focusing on the human side of security (Goel, Williams, & Dincelli, 2017; Liang & Xue, 2010; Wang, Li, & Rao, 2016). "Knowledge about user security behaviors is far from complete" (Warkentin & Willison, 2009, p. 395). Understanding the factors that influence users' information security protection behavior to prevent social engineering breaches is vital for any organization (Abraham & Chengalur-Smith, 2010; Kaushalya et al., 2018; Krombholz et al., 2015).

Algarni et al. (2017) and Tetri and Vuorinen (2013) recognized the lack of research involving social engineering and the need to understand crucial factors influencing users' information security protection behavior to prevent social engineering breaches. Therefore, a complete and comprehensive overview was necessary to uncover factors influencing users' protection motivation and behavior to prevent social engineering breaches (Bullée et al., 2015).

## **Barriers and Issues**

One of the barriers that might be possible for the survey questionnaire was that participants might have been hesitant to provide undesirable responses in terms of information security policies and standards. Information security expectations are prevalent in most organizations, resulting in this research study's probable under-reporting of unwanted behavior. Consequently, participants of this research study might have felt the possibility of their employer finding their opinions about information security-related items. Therefore, to mitigate this barrier, the survey questionnaire did not seek personal or employment details that might have resulted in participant identification.

This research's primary contribution is by incorporating the SETA program and security policies into the PMT full nomology research model to perform an empirical assessment of users' information security protection behavior to prevent social engineering breaches. Social engineering should be explored further in future research to provide additional insight into this vital topic. There could be additional constructs that may provide other perceptions into the information security behavior of individual users to prevent social engineering breaches.

Another barrier of this research study is the thought process for PMT itself. PMT is grounded mainly on fear. It assumes that individuals retort to fear by protecting themselves. There could be other factors in play that impacts users' behavior which PMT does not consider. Future research should study users who fail in securely conducting themselves and explore the reasons behind it.

### **Assumptions, Limitations, and Delimitations**

#### *Assumptions*

Assumptions included that the participants would be comfortable sharing their honest opinion while answering the survey. Similarly, participants provided precise answers to the survey questions, a crucial element regarding a sensitive topic like their organizations' information security (Sekaran & Bougie, 2013).

#### *Limitations*

Limitations impact the research results, and researchers cannot control the limitations (Creswell, 2005). The Hawthorne effect describes the pre-disposition in which participants change their answers because they are observed (Olson, Verley, Santos, & Salas, 2004). The participants may have been influenced by the fact that they could have been monitored for



their organizational behavior and responded with the information closer to the desired behaviors (Hagen & Albechtsen, 2009).

### *Delimitations*

Delimitation refers to explaining the boundaries set and the study's scope (Leedy & Ormrod, 2013). A delimitation of this research study was that all the samples belonged to only one country, the United States of America (U.S.A.). The results of this research study might have differed in the other countries.

### **Definition of Terms**

The following section shows vital terms and their related definitions in the context of this research study.

**Information security** – Protects information from a comprehensive array of threats to safeguard business continuity, curtail business risk, and capitalize on business opportunities and return investments (ISO/IEC, 2005).

**Information system risk** – Any financial loss or disruption of confidentiality, integrity, and availability (CIA) of information systems caused by a malicious cyber-attack (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016; Rees, Deane, Rakes, & Baker, 2011).

**Social engineering** – A practice of using people skills and persuasion techniques to attain unauthorized information is called social engineering (Jakobsson, 2016).

**SETA program** – A formal process to increase awareness and motivation through ongoing training and education, remind users about the security guidelines to protect from the security breach, and make users aware of the consequences of information misuse (D'Arcy et al., 2009).

**Security policy** – "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" (Bulgurcu, Cavusoglu, & Benbasat, 2010, p. 526-527).

**Protection motivation theory** – A theory to elucidate how individuals change their attitudes and actions, cope with the situation, and make decisions when facing danger (Rogers, 1975).

**Threat appraisal** – An element of PMT to evaluate the perceived threat level in a specific situation (Floyd et al., 2000).

**Coping appraisal** – An element of PMT that evaluates several factors that are likely to warrant an individual to engage in a suggested preventive response (Floyd et al., 2000).

**Perceived severity** – A degree to which a user perceives that adverse results, including physical and psychological damage caused by a social engineering breach, will be severe (Liang & Xue, 2010).

**Perceived vulnerability** – A perception of the probability of experiencing adverse results from a social engineering breach (Workman, Bommer, & Straub, 2008).

**Maladaptive rewards** – An expected benefit to be gained for not exhibiting protection behavior of complying with information security measures to prevent social engineering breaches (Boss et al., 2015).

**Response efficacy** – A user's belief that an adaptive response (a recommended behavior) will help mitigate social engineering breaches (Workman et al., 2008; Yoon, Hwang, & Kim, 2012).

**Self-efficacy** – User's beliefs in their ability to perform adaptive response against a social engineering breach (Yoon et al., 2012).

**Response costs** – Users' perceived downsides for indulging in protection behavior (Posey et al., 2015).

**Fear** – A user's negative emotional response to danger (Boss et al., 2015; Johnston et al., 2015).

**Protection motivation** – An intention to execute protection behaviors against security breaches (Floyd et al., 2000).

**Protection behavior** – An actual execution of protective behaviors against security breaches (Floyd et al., 2000).

**PLS-SEM** – A structural equation modeling technique develops exploratory research theories to comprehend multifaceted cause-effect relationship models with latent variables (Hair, Risher, Sarstedt, & Ringle, 2019).

### **List of Acronyms**

The following section comprises acronyms utilized throughout this research study.

**IT** – Information Technology

**SE** – Social Engineering

**CIA** – Confidentiality, Integrity, and Availability

**SETA** – Security Education Training Awareness

**PMT** – Protection Motivation Theory

**PS** – Perceived Severity

**PV** – Perceived Vulnerability

**FE** – Fear

**MR** – Maladaptive Rewards

**RE** – Response Efficacy

**SE** – Self-efficacy

**RC** – Response Cost

**ST** – SETA Program

**SP** – Security Policies

**PM** – Protection Motivation

**PB** – Protection Behavior

**PLS-SEM** – Partial Least Squares Structural Equation Modeling

**IRB** – Institutional Review Board

### **Summary**

Chapter one of this research study included background, problem statement, dissertation goal, research model, research question, and hypotheses. It contained relevance and significance, barriers and issues, assumptions, limitations, delimitations, the definition of terms, and a list of acronyms. Chapter one set the tone of this research study by stating the main problem, framework, and significance. Chapter two of this research study contains a literature review to help as the groundwork and reasoning for the research problem, research questions, hypotheses, and methodology. It delivers information about the current state of research on the selected topic. Likewise, it synthesizes prior research, integrates the literature's critical details, and detects potential gaps and disagreements.

## **Chapter 2**

### **Review of the Literature**

#### **Introduction**

This chapter contains an analysis of the literature regarding the research question raised by this research study (Paré, Trudel, Jaana, & Kitsiou, 2015). In addition, it synthesizes research about information security and social engineering, and it commences with a brief overview of information security, social engineering, the SETA program, and security policies. A subsequent discussion about protection motivation theory and its constructs perceived severity, perceived vulnerability, fear, maladaptive rewards, response efficacy, self-efficacy, response cost, protection motivation, and protection behavior follows. Finally, this chapter includes the gaps in PMT and information systems literature.

#### **Information Security**

Warkentin and Willison (2009) stated that the most significant threats are insider threats from organizational users who are 'trusted agents.' Despite the technology solutions, understanding why users fall for information security breaches and expose personally identifiable information (PII) needed much research attention (Dinev & Hart, 2006; Liang & Xue, 2010; Wang et al., 2016). Therefore, an emerging research stream on the human standpoint of information security emphasized user protection behaviors and the factors that motivate users to exhibit the protection behavior (Bulgurcu et al., 2010; Goel et al., 2017; Liang & Xue, 2010).

Irrespective of the right technology implemented to protect organizational information assets, users frequently exhibited undesirable security behaviors like mishandling passwords,

clicking on dangerous links, and accessing unprotected networks (Das & Khan, 2016; Jensen, Dinger, Wright, & Thatcher, 2017; Menard, Bott, & Crossler, 2017). In other words, social engineering breaches are often not the result of technology failure, but because users ignore or override security measures (Bravo-Lillo, Cranor, Downs, & Komanduri, 2011; Menard et al., 2017). The reasons for this problem were uncertain and necessitated additional research. Therefore, the research study described in this thesis investigated why users do not perform protection behaviors against social engineering breaches.

### **Social Engineering**

Social engineering breaches remained an ongoing risk that allows hackers to evade security measures and pose a significant risk (Bulgurcu et al., 2010; Dinev & Hu, 2007; Goel et al., 2017). For example, Heartfield and Loukas (2015) researched semantic attacks, one of the many social engineering attacks. Junger, Montoya, and Overink (2017) measured disclosure by asking sensitive information subjecting to increase social engineering risk. Furthermore, Algarni et al. (2017) explored Facebook users' susceptibility to social engineering victimization.

Moreover, Krishnamurthy and Wills (2009) found insufficient existing information security and privacy protection techniques. Mouton, Leenen, and Venter (2016) combined social engineering attack templates with real-world examples. In addition, Bullée et al. (2015) found that increasing awareness about the countermeasures associated with social engineering demonstrated a substantial helpful effect on neutralizing the attack.

Organizations and institutions suffer from social engineering attacks (Abraham & Chengalur-Smith, 2010; Myyry, Siponen, Pahlila, Vartiainen, & Vance, 2009). As technology increases in sophistication, deceitful attackers target users rather than users' technology (Safa, Von Solms, & Furnell, 2016; Xue, Liang, & Wu, 2011). The principal

danger to organizational security is not a technical glitch or inefficient system; it is a user (Algarni et al., 2017; Anderson & Agarwal, 2010, 2011). In this unprecedented era of online invention, users may spontaneously give away sensitive information without understanding security repercussions (D'Arcy & Lowry, 2019; Goel & Chengalur-Smith, 2010; Krombholz et al., 2015).

Many users overlook the warnings generated by the technology and tools to prevent social engineering breaches for various motives (Goel et al., 2017; Kirlappos & Sasse, 2012; Luga, Nurse, & Erola, 2016). As a result, social engineering traps gullible users intentionally into conveying their confidential data, thus providing open access to an organization's fundamental assets, circumventing all the layers of organizational policies and systems (Brody et al., 2012; Lai, Li, & Hsieh, 2012). Furthermore, some social engineering is involved in most information security attacks (Bullée et al., 2015; Tu, Turel, Yuan, & Archer, 2015).

Social engineering has become an ever-increasing threat impacting multinational organizations, governments, and individuals (Williams, Hinds, & Joinson, 2018). Social engineering is the most popular technique among hackers because it can break even the utmost protected systems (Krombholz et al., 2015). Also, the users themselves are the weakest part of the information security system, and it is more natural to exploit users' weaknesses than exploit technology loopholes (Liang, Xue, Pinsonneault, & Wu, 2019). Moreover, social engineers have fully automated attacks and orchestrated them on a colossal scale (Krombholz et al., 2015).

Social engineers carry attacks over various channels, including email, telephone, websites, cloud, and social networks, and can originate either by humans or technology (Krombholz et

al., 2015). There are numerous types of social engineering outbreaks like phishing, spear phishing, dumpster diving, shoulder surfing, reverse social engineering, waterhole attacks, advanced persistent threat, and baiting (Conteh & Schmick, 2016; Krombholz et al., 2015).

Phishing is a practice of trying to gather confidential information using deceptive mechanisms like e-mails, phones, text messages, and websites (Conteh & Schmick, 2016; Dodge, Carver, & Ferguson, 2007). In addition, spear phishing is a practice of targeting a specific individual, organization, or business to gather confidential information using deceptive mechanisms like e-mails, phones, text messages, and websites (Chaudhry, Chaudhry, & Rittenhouse, 2016). The difference between phishing and spear-phishing is that the phishing campaigns do not target victims individually, unlike spear phishing (Chaudhry et al., 2016). Moreover, dumpster diving retrieves information from the documents from rubbish (Krombholz et al., 2015; Tetri & Vuorinen, 2013).

Shoulder surfing is a practice of gaining information by making secret, direct observations like watching a user's keystrokes while using a computer (Tetri & Vuorinen, 2013). On the other hand, reverse social engineering is a practice where an attacker gains the victim's trust by offering help (Krombholz et al., 2015). A waterhole attack is a practice where an attacker infects the websites often visited by the target victims at the waterhole (Fan, Lwakatare, & Rong 2017). An advanced persistent threat is a practice where an attacker uses continuous and concealed methods to gain access to information, steal data, or surveil systems of the victim's organization and remain inside for a long time (Fan et al., 2017).

Baiting is a practice where an attacker exploits the victims' greediness and inquisitiveness by luring them into a trap of something like a gift kept somewhere and can be received by the victims (Conteh & Schmick, 2016; Fan et al., 2017). Known as voice phishing or phone



elicitation, vishing is a practice where an attacker uses social engineering to assess vulnerabilities and call victims to lure them into conceding confidential information (Fan et al., 2017). Pretexting is a practice where an attacker uses a fabricated scenario and a false motive to obtain confidential data using methods like namedropping, impersonation, and untruthful identity (Conteh & Schmick, 2016; Fan et al., 2017).

Tailgating, also known as piggybacking, is a practice where an attacker seeks access to the restricted area by following the victim's authorized access (Conteh & Schmick, 2016; Fan et al., 2017). Quid pro quo is a practice where an attacker presents a technical service in exchange for information; for example, the attacker mimics a vendor representative and offers to help a victim who needs technical assistance (Conteh & Schmick, 2016).

### **SETA Program**

Information security leaders implement information security measures, including security education, training, and awareness (SETA) programs to improve the security protection behavior of users (Johnston et al., 2015). Thus, SETA programs emphasize raising users' awareness of their responsibilities related to organizational information assets and resources, the penalties of misusing them, and providing training and education to build these capabilities (D'Arcy & Hovav, 2007; Johnston et al., 2015). Efficacious SETA programs should result in augmented mindfulness of protection behaviors by making users recognize security risks concerning their interactions with information resources and mitigate them by refining their acts (Herath & Rao, 2009b; Johnston et al., 2015).

Users who had better abilities to detect the social engineering breach are the ones who did better in refusing to provide access to the organizational information assets (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015; Wright & Marett, 2010). The deep-

knowledgeable users about social engineering emails and the relevant repercussions did better in responding to the emails than ill-knowledgeable (Jansson & von Solms, 2013; Parsons et al., 2015; Stajano & Wilson, 2011). Accordingly, the goal of the SETA program is to inspire users to focus increasingly on a proactive approach instead of a reactive approach (Straub & Welke, 1998; Vance et al., 2012).

### **Security Policies**

Security policies are statements of organizational goals, controls, procedures, rules, and users' responsibilities to prevent social engineering breaches (Lee & Lee, 2002). The details and complexity of security policies differ from industry to industry (D'Arcy & Hovav, 2007). Specifically, the financial services industry may have more stringent security policies than hospitality (D'Arcy & Hovav, 2007).

### **Protection Motivation Theory (PMT)**

PMT, developed in 1975 by Rogers, utilizes the cognitive process that users undergo when they experience danger and respond accordingly (Maddux & Rogers, 1983; Rogers, 1975). Furthermore, it was initially developed based on the expectancy-value theory to comprehensively understand the impact of fear appeals on attitude (Maddux & Rogers, 1983; Rogers, 1975). Moreover, PMT underwent two meta-analyses (Floyd et al., 2000; Milne et al., 2000). PMT originated in the health science and psychology field, primarily known for motivating people to practice healthy behavior (Posey et al., 2015). PMT is now widely recognized as a framework to study protection motivation against any threat (Posey et al., 2015).

PMT provides an efficient theoretical foundation for analyzing how users determine what kind of security behaviors to exhibit. At the base of PMT, there are two leading independent

appraisal processes transpiring as an effect of a fear appeal: threat appraisal and coping appraisal (Maddux & Rogers, 1983). The two kinds of coping appraisal are adaptive coping (to protect) and maladaptive coping (not to protect) (Floyd et al., 2000). PMT theorizes that threat appraisal determines factors for a user to adopt a specified coping response (Floyd et al., 2000). Posey et al. (2015) summarized threat appraisal and coping appraisal succinctly:

Threat appraisal is the process by which insiders analyze (1) their perceived vulnerability, (2) their perceived severity, and (3) potential intrinsic or extrinsic rewards for engaging in maladaptive responses. Coping appraisal is the process by which insiders evaluate (1) the efficacy of the potential adaptive responses to a threat or response efficacy; (2) their ability to successfully carry out the recommended responses, or self-efficacy; and (3) the perceived response costs associated with their engagement in the adaptive coping strategy (p. 6-7).

The threat appraisal procedure encompasses the users' perception determination about vulnerability to an information security threat (perceived vulnerability), the brutality of the threat (perceived severity), the terror of the threat (fear) (Boss et al., 2015), as well as any intrinsic or extrinsic inspiration for exhibiting an unwanted behavior (maladaptive rewards) (Vance et al., 2012). The coping appraisal procedure encompasses the users determining whether protection action is efficient at protecting from the threat (response efficacy), whether they are capable of executing the protection action (self-efficacy) and if it justifies the perceived cost of the action (response cost) (Floyd et al., 2000). Furthermore, response efficacy is the user's belief that complying with the organization's information security measures will prevent the breach (Maddux & Rogers, 1983). Moreover, self-efficacy is the

user's confidence to adhere to the organization's information security measures (Bandura, 1977).

### *Perceived Severity*

Perceived severity is a users' valuation of the severity of the significances caused by a social engineering breach (Hanus & Wu, 2016). Liang and Xue (2010) and Mohamed and Ahmad (2012) appeared to have found a positive relationship between perceived severity and protection behavior. Prior literature, such as Hanus and Wu (2016) and Youn (2005), did not associate perceived severity and protection behavior. Zahedi, Abbasi, and Chen (2015) found perceived severity as a foremost forecaster for protection motivation. In contrast, LaRose and Eastin (2004) and Lee et al. (2008) did not find a significant relationship between perceived severity and protection motivation.

### *Perceived Vulnerability*

If users perceive they are susceptible to a social engineering breach, they are more likely to follow information security measures (Workman et al., 2008). Liang and Xue (2010), Mohamed and Ahmad (2012), as well as Ng et al. (2009) appeared to have found a weak positive relationship between perceived vulnerability and protection behavior. Additionally, prior literature such as Hanus and Wu (2016) and Youn (2005) did not find any positive relation between perceived vulnerability and protection behavior.

### *Fear*

Information security scholars are seemingly attuned to utilize fear which motivates users to abide by suggested security protection behaviors (Herath & Rao, 2009a; Johnston & Warkentin, 2010). Mwangwabi, McGill, and Dixon (2018) studied fear regarding guideline usage for secure password creation. In conjunction with perceived severity and perceived vulnerability, fear has a unique and essential role in PMT (Boss et al., 2015). In addition, fear is

frequently a user's emotional response to a threat (Rosenstock, 1974; Witte, 1994). Fear may comprise anxiety, uneasiness, shock, provocation, worry, or distress (Boss et al., 2015; Rosenstock, 1966). "Fear appeals are a necessary component of a holistic security management program because threats to information assets are prevalent and must be warned against" (Johnston et al., 2015, p. 117).

### *Maladaptive Rewards*

If users perceive that the reward for not exhibiting protection motivation is higher than exhibiting it, they will be less likely to exhibit it (Vance et al., 2012). Rewards increase the likelihood of choosing the maladaptive behavior (Crossler & Bélanger, 2014; Floyd et al., 2000). Maladaptive rewards are paybacks from following protection measures and, therefore, can be perceived in the form of time-saving, cost-saving, efficiency, pleasure, or even damage (Boss et al., 2015; Floyd et al., 2000; Johnston & Warkentin, 2010).

### *Response Efficacy*

Response efficacy is the degree to which a user believes that a specific action prevents a social engineering breach (Compeau & Higgins, 1995; Jayanti & Burns, 1998; Venkatesh et al., 2003). If a user believes that a specific task will secure organizational information assets, the user will be more motivated to comply (Meso, Ding, & Xu, 2013). Response efficacy measures the user's belief in the efficacy of security measures in addition to self-efficacy (Johnston et al., 2015). The perceived efficiency of security measures positively inclined the security measure to not download unknown files and not click on unknown links to prevent social engineering breaches (Lai et al., 2012).

Response efficacy appeared to have found positively associated with authentication service (Yang et al., 2017), acceptance of spyware protection (Johnston & Warkentin, 2010), and an acceptance of security policy (Ifinedo, 2012; Lee & Larsen, 2009). Prior literature

such as Gurung, Luo, and Liao (2009), Hanus and Wu (2016), Hu and Dinev (2005), Liang and Xue (2010), as well as Yoon et al. (2012), found a positive relation between response efficacy and protection behavior. Nonetheless, Mohamed and Ahmad (2012) appeared to have found no positive connection between response efficacy and protection behavior.

### *Self-efficacy*

Self-efficacy of noticing information security breaches may reduce one's chance of being breached (Wang et al., 2016). PMT introduced self-efficacy by adopting the social cognitive theory of Bandura (1977). Furthermore, highly self-efficacious users will be more likely to exhibit protection behavior by engaging in protection actions and avoiding high-risk activities such as sharing passwords and clicking on unknown links (Hu & Dinev, 2005; Milne, Labrecque, & Cromer, 2009). Self-efficacy involved former research investigating counterfeit website detectors (Zahedi et al., 2015) and online safety protection behaviors (Lee et al., 2008). Prior literature, such as Hanus and Wu (2016) and Yoon et al. (2012), found a positive relationship between self-efficacy and protection behavior. On the other hand, Tsai, Jiang, Alhabash, LaRose, Rifon, and Cotton (2016) found a negative relation between self-efficacy and protection motivation.

### *Response Cost*

Response cost can be any delay, obstacle, side effect, or disadvantage that users believe they will incur if they exhibit protection behavior (Posey et al., 2015). The adoption of protection behavior may involve some reluctance for the users to espouse. For instance, if a user observes a high response cost for complying with the security measure, the probability of non-compliance is also high (Meso et al., 2013). Similarly, response costs decrease the likelihood of choosing adaptive behavior (Floyd et al., 2000).

Researchers have found that the perceived response cost discourages users from exhibiting protection behavior (Arachchilage & Love, 2013; Boss et al., 2015; Taneja, Vitrano, & Gengo, 2014; Zhang & McDowell, 2009). Prior literature, such as Liang and Xue (2010), and Yoon et al. (2012), found a negative relation between response cost and protection behavior. Mohamed and Ahmad (2012) and Ng et al. (2009) appeared to have found no link between response cost and protection behavior.

### *Protection Motivation*

Protection motivation intends to perform protection behaviors against a social engineering threat (Lee, Lim, Kim, Zo, & Ciganek, 2013; Sommestad et al., 2015). Technical and social-organizational aspects are central to the success of information security (Bulgurcu et al., 2010; Dinev & Hu, 2007). Subsequently, protection motivation for information security breaches has emerged as a crucial socio-technical factor (Dinev & Hu, 2007; Liang & Xue, 2010; Wang et al., 2016). The prior research for protection motivation included the intention not to disclose personal information (Beldad, van der Geest, de Jong, & Steehouder, 2012) and intention to comply with IT security policies (Crossler, Long, Loraas, & Trinkle, 2014).

### *Protection Behavior*

Protection behavior is the actual performance of protection actions against social engineering threats (Arachchilage & Love, 2014). Specifically, prior research encompassed analysis of protection behavior concerning phishing, a type of social engineering (Arachchilage & Love, 2013, 2014). Understanding users' protection behavior to prevent social engineering breaches is vital for organizations (Bulgurcu et al., 2010; Bullée et al., 2015; Chai et al., 2009). Similarly, Liang and Xue (2010) stated that research about users' information security behaviors needs much work. As per Liang and Xue (2010), "Although a few studies have

examined individual users' security behavior, the findings are largely inconsistent and sometimes contradictory" (p. 404).

### **Utilization PMT and Information Systems Literature**

PMT postulates that when users experience a threat, they undergo cognitive threat appraisal and coping appraisal processes. A user assesses threat and corresponding coping mechanisms and determines to perform adaptive or maladaptive behaviors. These adaptive behaviors intend to protect the user against danger, while maladaptive responses prevent the desired behavior.

PMT is an exceedingly pertinent theory in information security research due to the tangible threat-response pairs commonly found in information security. PMT is a well-researched theory to explore privacy concerns over social network sites (Alashoor et al., 2017; Mohamed & Ahmad, 2012), intention for antispyware software usage (Gurung et al., 2009), and online protection actions (Chen & Zahedi, 2016).

PMT has been used to research online shopping protection behavior (Milne et al., 2009), online protection behavior (Lee et al., 2008), online unsafety behavior (Chou & Chou, 2016), and secure email behavior (Ng et al., 2009). Similarly, PMT has been used to discover what motivates users to comply with security measures like data backup (Lee & Kozar, 2005; Menard, Gatlin, & Warkentin, 2014).

PMT is well-utilized to research protection behavior of securing desktops (Hanus & Wu, 2016), online safety behaviors (Tsai et al., 2016), and adoption of security behaviors (Boehmer, LaRose, Rifon, Alhabash, & Cotton, 2015). For example, Lee and Larsen (2009) used PMT to discover what motivates users to comply with security measures like anti-malware software and explored social influence. Consistently, PMT has been used to



investigate compliance with information security policies (Herath & Rao, 2009b; Ifinedo, 2012; Johnston et al., 2015; Siponen, Pahlila, & Mahmood, 2010) and unified security practices (Crossler & Bélanger, 2014).

Crossler et al. (2013) explored PMT and behavioral InfoSec areas, including insider deviant behavior versus insider misbehavior, security compliance, and data collection and measurement. Similarly, Workman et al. (2008) examined a research model to determine why users would not exhibit protection behavior and why they would choose not to protect themselves, even if they believed in the self's ability to defend.

PMT has been used to explore malware avoidance behavior (Dang-Pham & Pittayachawan, 2015), adoption of antivirus software, and strong passwords (Meso et al., 2013; Zhang & McDowell, 2009), and coping behaviors to fight identity theft (Lai et al., 2012). Additionally, PMT is well-served to discover the intention to practice safe computing at home (Anderson & Agarwal, 2010) and intentions and behaviors to use antispyware (Liang & Xue, 2010).

PMT has been used to explore protection behavior against online harassment (Lwin, Li, & Ang, 2012) and online safety behaviors (Yoon et al., 2012). For example, Johnston and Warkentin (2010) utilized PMT by studying the threat-response pair where users experienced the spyware threats and, at the same time, were given an antispyware mechanism to protect themselves. Thus, PMT has been utilized and verified as the leading theory in many studies related to information security in organizations (Boss et al., 2015; Lee & Larsen, 2009; Liang & Xue, 2010; Moody et al., 2018; Workman et al., 2008).

## **Gaps in PMT and Information Systems Literature**

Information security research routinely dropped proven PMT constructs instead of utilizing the PMT full nomology (Boss et al., 2015). Anderson and Agarwal (2010), Chou and Chou (2016), Herath and Rao (2009a), Johnston and Warkentin (2010), as well as, Kumar et al. (2008) focused on the adaptive coping response of PMT instead of including a maladaptive coping portion of PMT in their research. Adaptive behavior is the behavior that users exhibit to avert the threat from revealing itself (Chen & Zahedi, 2016). On the contrary, maladaptive coping is the users' choice not to comply with a security measure to protect from the security breach (Boss et al., 2015).

The review of the literature exposed that most of the information systems research involving PMT utilized only part of PMT instead of using the full model (Crossler & Bélanger, 2014; Ifinedo, 2012; Johnston & Warkentin, 2010; Liang & Xue, 2010; Workman et al., 2008). PMT is a cognitive process with fear appeal as the central factor determining how it impacts attitude and behavior (Milne et al., 2000; Rogers, 1975). Even though the relationship between fear and protection motivation seems so natural and fear is one of the most significant constructs of PMT, extant information security research has dropped fear construct from the PMT research model most of the time (Floyd et al. 2000; Rogers 1975). Fear is the most significant factor in the adaptive coping process of PMT. Nonetheless, much information systems research involving PMT did not include fear (Chou & Chou, 2016; Hanus & Wu, 2016; Lee & Larsen, 2009; Tsai et al., 2016; Yang et al., 2017).

Again and again, information systems research involving PMT did not include response cost (Boehmer et al., 2015; Chen & Zahedi, 2016; Johnston et al., 2015; Mohamed & Ahmad, 2012). In many instances, information systems research involving PMT did not

include perceived severity (Alashoor et al., 2017). Some information systems research involving PMT did not contain perceived vulnerability (Anderson & Agarwal, 2010). Some information systems research involving PMT did not include response efficacy (Youn, 2005). On top of that, some information systems research involving PMT did not comprise self-efficacy (Zhang & McDowell, 2009). Most of the extant research explored protection motivation and did not include behavior (Posey et al., 2015).

This literature overview highlighted predominantly significant existing gaps. It demonstrated that the effects of PMT on protection motivation and behavior to prevent social engineering breaches are still not well recognized or dependable in literature. Though PMT is well-accepted to discover new information security models (Moody et al., 2018), PMT's full research model has not been accurately used to study users' behavior to prevent social engineering breaches.

There was a lack of literature utilizing PMT combined with the SETA program and security policies to explore factors affecting users' information security protection behavior to prevent social engineering breaches. This research study was exploratory. Based on the gaps in existing literature, this research study discovered factors affecting users' information security protection behavior to prevent social engineering breaches using full PMT nomology.

## **Summary**

The multidisciplinary nature of the problem in this research study required a thorough literature review. Despite the research steered in social engineering, other studies have failed to solve the problem, and social engineering seems to be still a problem. An assessment of numerous facets of PMT resulted in delivering the groundwork for this research study. PMT

has been utilized in the information security field to study protection motivation and protection behaviors.

Previous research did not use the combination of the PMT full nomology, the SETA program, and security policies to explain social engineering protection behavior. An in-depth literature review resulted in the necessary information for an empirical assessment of users' information security protection behavior to prevent social engineering breaches leveraging protection motivation theory, the SETA program, and security policies. Chapter two concluded the literature review.

The next chapter of this research study contains information about methodology. It includes an overview of the research design to answer the research questions and test the hypotheses. It encompasses instrument development and validation, and measurement items for the constructs. Furthermore, it contains instrument reliability and validity, internal consistency reliability, construct validity, content validity, convergent validity, and discriminant validity. It comprises details of the proposed sample, sample population, and anticipated response rate. It presents a plan for data analysis, formats for demonstrating results, and resource requirements.

## **Chapter 3**

### **Methodology**

#### **Introduction**

This research study explored the role threat appraisal (perceived severity, perceived vulnerability, fear, and maladaptive rewards), coping appraisal (response efficacy, self-efficacy, and response costs), SETA program, and security policies have with the users' information security protection motivation and protection behavior to prevent social engineering breaches. Data Science is an overarching term for methodologies to gather insights from data. Quantitative analysis is the procedure of collecting and analyzing quantifiable and provable data to gain intuition. This research study is quantitative and utilized formerly established survey instruments for both the dependent and independent variables. Web survey administration provided statistical analysis input. A seven-point Likert scale measured constructs. Participant's demographics and background information were collected, followed by a validity and reliability assessment of the response data.

The Partial Least Square Structural Equation Modeling, known as PLS-SEM, is used to model and estimate the cause-effects relationship model. PLS-SEM is suitable for exploratory research by identifying the variance in the dependent variables when verifying proposed theoretical models (Hair, Hult, Ringle, & Sarstedt, 2017). Data results assisted in hypotheses validation. The data results are summarized, followed by the conclusion.

#### **Research Design Overview**

The research method was quantitative research comprised of data collection, analysis, interpretation, and presentation of the research study (Creswell & Creswell, 2018). The

research method included web-based survey research to test the research model empirically. The research study utilized the positivism research philosophy to derive measurable observations that result in statistical evaluations, ensuring that research results are observable and quantifiable.

The research study was a cross-sectional type where the study measured a cross-section of a given population at one precise instant in time. The unit of analysis was the primary entity that the intended research study was planning to analyze. Furthermore, the unit of analysis of this research study was individual users, as it was the most appropriate choice based on the research plan of the study. The research study tested all the items in the context of users' information security protection behavior towards social engineering breaches.

## **Research Methodology**

### *Human Ethical Attention*

Prior approval by the Nova Southeastern University institutional review board (IRB) was a prerequisite to conducting this research study. So, the survey of this research study went through an IRB process. The research study was not hostile, devious, daunting, or traumatic to the participants and guaranteed participants that their identity would be kept completely anonymous, and their responses will be strictly utilized only for this research study (Gall, Borg, & Gall, 1996).

### *Delphi Method Study*

A panel of three SMEs in the information security area reviewed the web-based survey questionnaire and measurement items. SMEs provided advice to attain consensus in solving the problem, evaluate the course of action, and assess the web-based survey questionnaire. The enhanced survey questionnaire encompassed SMEs' expert advice.

### *Data Collection*

Four hundred potential participants received a data collection survey. The web-based survey data presented a high-level overview of this research study, researcher contact information, and an estimated survey completion time frame. It showed details on ensuring confidentiality and anonymity of participants and assurance about using the data strictly for this research study. The participants received the urge to provide the most accurate and honest answers to the questions, and participants received thanks at the end of the survey.

### **Instrument Development and Validation**

Construct operationalization is the method of ensuring that variables are measured as impeccably as possible. This research study utilized an interval scale because it provides measurements where the difference between the values of two variables is expressive. One of the most successfully used interval scale measurements in social science is the Likert scale. The range of the seven-point Likert scale was (1 = strongly disagree; 2 = disagree; 3 = somewhat disagree; 4 = neither agree nor disagree; 5 = somewhat agree; 6 = agree; 7 = strongly agree).

Each of the measurement items incorporated in this research study was reflective (Hair et al., 2017). This research study used the pre-validated measurement items verified in the former research. One of the survey items for the variable, protection behavior, was self-developed; the rest of the survey items for all the dependent and independent variables were previously developed and validated in the prior literature (Churchill, 1979; Straub, 1989).

Appendix A showed a measurement item summary stating the complete list of all measurement items. Appendix B showed an overview of reliability evidence stating the complete list of reliability evidence. The purpose of using existing measurement items was to

understand the phenomenon in a new context of social engineering (Niederman & March, 2015). Performing research on proven measurement items further validated, provided additional insight on the existing instrument scales, and supported future research about social engineering.

#### *Instrument Reliability and Validity*

Instrument reliability safeguards that an instrument is reliable and measures dependably. Instrument validity defends that reliable results are also valid. Instrument validity and reliability both are necessary. It is not possible to achieve instrument validity without achieving instrument reliability. Instrument reliability is a prerequisite for instrument validity. The subsequent steps ensured instrument reliability and validity in this research study.

#### *Internal Consistency Reliability*

Cronbach's alpha calculation safeguarded the internal consistency reliability (Hair, Black, Babin, & Anderson, 2010). All the factors in this research study had Cronbach's alpha values well above 0.7 to ensure internal consistency reliability (Nunnally & Bernstein, 1994).

#### *Construct Validity and Content Validity*

Factor analysis performed using SmartPLS software tested construct validity. Delphi study safeguarded the construct validity, content validity and attained agreement on survey instrument measurement items over two rounds before finalization. Three subject-matter experts (SMEs) participated in the Delphi study.

#### *Convergent Validity*

Factor analysis safeguarded the convergent validity of the instrument (Fornell & Larcker, 1981). The average variance extracted (AVE) is the average variance in indicator variables



that the corresponding construct successfully clarifies. AVE is a degree of the discrepancy amount taken by a construct due to variance owing to measurement error. Hair et al. (2010) asserted that all constructs' AVE value should be more than the 0.5 minimum threshold.

#### *Discriminant Validity*

The discriminant validity ensured the most solid relationships between a reflective construct and its indicators (Hair et al., 2010). This research study safeguarded the instrument's discriminant validity by successfully fulfilling the cross-loading method (Chin, 1998).

### **Sample**

#### *Sampling Type*

The non-probability sampling approach is the approach that relies on the subjective judgment of the researcher. The purposive sampling approach is one of the types of non-probability sampling approach. The research study's purposive sampling (also called judgment, subjective, or selective sampling) approach decisively pursued specific group members. Information technology (IT) users who are not IT professionals may have different views on social engineering breaches than IT professionals. The target group for this research study did not restrict to just IT professionals; any users who use information technology were eligible for the survey. The target group in this research study was IT users.

#### *Sampling Recruitment*

The research study used emails to recruit participants. Response time was rapid, and the cost per participant was lesser without compromising the quality than other enrollment approaches (Steelman, Hammer, & Limayem, 2014). Participants were not compensated or incentivized to participate in the survey.

### *Sampling Size*

Cohen's (1992) statistical power analysis is one of the most prevalent methods in determining sampling size and an essential factor in designing experiments and testing results (Cappelleri, Darlington, & Trochim, 1994; Thomas & Juanes, 1996). Cohen's (1992) statistical power analysis utilizes the relationships among the five factors: sampling size, significance level, effect size, desired power, and estimated variance. Each of the five factors is a function of the other four for any statistical model (Cohen, 1992).

According to Cohen's (1992) statistical power analysis, any given statistical test can calculate sampling size by supplying values for the other four factors: significance level, effect size, desired power, and estimated variance. For this research study, the appropriate sampling size was at least one hundred and sixteen based on Cohen's (1992) statistical power analysis table at a statistical power of 80%, a medium effect size of .30, and a significance level of 0.05.

The plan to attain a large enough sampling size subsequently determined the total number of target participants (Cohen, 1988; Hair, Ringle, & Sarstedt, 2011). The goal was to solicit a response from at least one hundred and sixteen participants. With a 29% estimated completion rate, a web-based survey targeted four hundred participants. Only U.S.A. residents received the survey.

### *Descriptive Statistics*

The web-based survey captured participants' demographics and background information, including gender, age, education, and social engineering breach exposure (Steelman et al., 2014). Table 2 showed the participants' demographic and background information questions and corresponding scales.

Table 2

*Participants Demographics and Background Questions*

Item	Questions	Scale	Options
Gender	What is your gender?	3-point category scale	1 = Male; 2 = Female, 3 = Other
Age	What is your age range?	6-point Likert scale	1 = 18–24; 2 = 25–34; 3 = 35–44; 4 = 45–54; 5 = 55–64; 6 = Over 65 Years
Education	What is your highest education achieved?	7-point Likert scale	1 = Some School, No Degree; 2 = High School Graduate; 3 = Some College, No Degree; 4 = Associate's Degree; 5 = Bachelor's Degree; 6 = Master's Degree; 7 = Doctoral Degree
Social Engineering Breach Exposure	What is your exposure to social engineering breaches?	3-point category scale	1 = None, 2 = Some, 3 = Extensive

**Data Analysis***Pre-analysis Screening*

Reliability and validity examinations comprised preliminary statistical analysis. The reliability check encompassed Cronbach's alpha, while the validity verification involved convergent and discriminant validity (Cronbach, 1951). There were no questions where all the answers were identical. The research study checked the Mahalanobis distance in the pre-testing phase (Mahalanobis, 1936). The Mahalanobis distance is equal to the distance between two points in the multivariate arena. The Mahalanobis distance measures distance relative to the central point. The benefit of using Mahalanobis distance was to recognize and remove multivariate outliers in the pre-testing phase.

### *Common Method Bias*

Common method bias (CMB, also known as common method variance, CMV) are the variations created by the measuring method rather than constructs the measures are supposed to measure (Schaller, Patil, & Malhotra, 2014). The questions on the web-based survey were unambiguous, and the web-based survey requested the participants to answer the questions with honesty and sincerity to reduce common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Podsakoff, MacKenzie, & Podsakoff, 2012).

### *Partial Least Squares Structural Equation Modeling*

The data was analyzed and interpreted using Structural Equation Modeling, considering the research question and PMT (Gefen, Rigdon, & Straub, 2011). PLS-SEM is a Structural Equation Modeling (SEM), a vigorous technique that permits assessing intricate cause-effect relationship models involving latent variables (Hair et al., 2019). The partial Least Squares Structural Equation Modeling (PLS-SEM) method verified the research model.

The PLS-SEM comprises two sub-models. The two sub-models are measurement and structural models. It allows adequate valuation of the measurement and structural models (Petter, Straub, & Rai, 2007). The measurement model signifies the relationships between the observed data and the latent variables and links the measurable indicators to the unobservable latent variables (Chin, 1998). The structural model implies the relationships between latent variables while the path coefficients verify the relationships between independent and dependent variables. PLS-SEM analysis in this research study utilized SmartPLS, version 3.0, to simultaneously evaluate measurement and structural models (Hair et al., 2011).

## **Formats for Presenting Results**

The table format presented the construct reliability and validity summary and the hypotheses test summary. Furthermore, the figure format displayed the research model. The Appendices showed the survey questionnaire and IRB approval.

## **Resource Requirements**

This research study utilized the Delphi method to fetch advice from an expert panel of information security professionals. Feedback from the expert panel aided in measurement item improvements. The data sample originated from a pool of users working in the U.S.A. Each step of the research study required the use of software, hardware, and technology. Moreover, the web-based tool Google® Forms abetted in survey instrument development and participants' data collection.

Microsoft® Excel assisted in participant's data summarization and synthesis. Furthermore, IBM® SPSS® Statistics supported descriptive statistics, ANOVA, and the creation of graphs. Scholarly books reference provided critical contributions to this research study. Journals and peer-reviewed articles written by experts provided a viewpoint of significant historical research conducted. Alvin Sherman Library of Nova Southeastern University provided access to journals and peer-reviewed articles.

## **Summary**

This chapter described the rationale for selecting a specific methodology to gather, process, and summarized information to understand the problem. It described plans for conducting the research methods, data collection, and data analysis. The web survey, prepared using pre-validated items from the broader PMT literature, conducted the data collection in this research study. This chapter stated the research study participants,

procedures, and instruments. In addition, it specified that data were collected and analyzed using a reliable and recognized method in the field of this research study. It included details about IRB approval to guard human participants' privileges and well-being in this research study. It offered adequate material to permit other researchers to repeat this research study. It showed how the overall methodology provided answers to the original research question.

## **Chapter 4**

### **Results**

#### **Introduction**

This chapter states the results of the quantitative analysis of the research study. It demonstrates the complete PLS-SEM evaluation of the research model. Moreover, this chapter begins with survey validation, Delphi study, data collection, data screening utilizing Mahalanobis distance and normality test, and demographics. The rest of the chapter presents data analysis in two parts, first measurement model testing and then structural model testing. The measurement model assessment includes convergent validity, construct reliability and validity, outer loading, discriminant validity, and model fit. The structural model evaluation includes collinearity, path coefficients, hypothesis summary, total effects, coefficient of determination, effect size, predictive relevance, important-performance map analysis, and PLS predict.

#### **Survey Validation and Delphi Study**

Upon following the IRB approval process, an IRB approval letter was received (Appendix C). The Google® Forms assisted in survey creation. A panel of three information security SMEs evaluated the web-based survey as part of the Delphi study. The purpose of the Delphi study was to refine the participant survey and seek expert opinion. Literature reviews are essential and provide valuable information for the survey items; the use of SMEs in the Delphi method provides crucial guidance and practical knowledge (Gray & Hovav, 2014; Sumsion, 1998).

SMEs were selected based on their information security domain experience. The first SME was a Chief Information Security Officer, the second SME was an Information Security Manager, and the third SME was an Information Security Analyst. Furthermore, the SMEs remained anonymous as per the original plan. The survey was distributed to SMEs using emails on November 30, 2020. Subsequently, SMEs studied the survey and provided recommendations. All three responses from the SMEs were received by December 5, 2020. The responses received from the SMEs were mainly optimistic, as they found the survey effective and coherent. SMEs provided two recommendations. The first recommendation was to have all the measurement items related to questions mandatory to ensure that participants responded successfully. The second recommendation was to offer a short explanation of the constructs in the survey, which helped the participants understand the meanings of the constructs.

All measurement items in the participant survey resulted in a mandatory entry as per SMEs' suggestions. Similarly, a short explanation was added to the construct name for ease of understanding as per SMEs' suggestions. Overall, SME recommendations enhanced the survey with meaningful and valuable updates.

### **Data Collection**

The data collection spanned from January 1, 2021, to January 25, 2021. The survey was not just limited to information technology professionals. The survey targeted any individuals who are information technology users. The survey recipients included the range starting from the individuals who are information technology users to information technology professionals. The survey recipients were professionals in a professional network, including LinkedIn connections. The participants' information technology experience ranged from few



years of experience to decades of experience. Since the participants belonged to a professional network, the majority had extensive experience with information technology.

Email and LinkedIn were valuable tools to manage the communication for survey completion. The email content (Appendix D) included the participant survey (Appendix E). The survey provided clear information about the survey purpose and the expected time to complete the survey. The survey stated that the participation was voluntary and anonymous, and responses were confidential.

Data collection utilized the cross-sectional method. The research study used the individual unit of analysis and purposive sampling approach. The survey was distributed to four hundred individuals using email. The first phase included emails sent to the four hundred individuals by January 1<sup>st</sup>, 2021. Consequently, a total of twenty-five responses were received by January 8<sup>th</sup>, 2021. The second phase included emails sent to the same individuals by January 8<sup>th</sup>, 2021. Until then, a total of seventy-five responses were received by January 18<sup>th</sup>, 2021. The third and the last phase included emails sent to the same individuals by January 18<sup>th</sup>, 2021. The survey was closed on January 25<sup>th</sup>, 2021. As a result, a total of one hundred twenty-nine participants completed the survey with a response rate of 32%.

### **Data Screening**

The data was loaded into Microsoft® Excel to import into IBM® SPSS® Statistics for pre-analysis of the data.

#### *Mahalanobis Distance*

IBM® SPSS® Statistics aided with the pre-analysis activities. The Mahalanobis distance is a multi-dimensional generalization of the idea that evaluates the distance between a point and a distribution (Mahalanobis, 1936). Outliers are the values with  $p < .001$  based on the

Chi-square critical value as per Chi-square ( $\chi^2$ ) distribution (Mertler & Reinhart, 2017). Based on this, Chi-square distribution table criteria was 93.17 using fifty five degrees of freedom ( $df=55$ ) and Chi-square critical value ( $p < .001$ ) (Mertler & Vannatta, 2013). Mahalanobis distance calculation identified seven outliers (11, 33, 44, 65, 71, 93, 114) with Mahalanobis distance exceeding the criteria of 93.17 (Appendix F). Mertler and Reinhart (2017) recommended analyzing extreme values before taking further action. The next step was to remove five out of the seven extreme outliers (11, 33, 65, 71, 93) and keep two outliers with the lowest values (44, 114) in the data. Appendix G showed the results of Mahalanobis distance recalculation. The data showed only two values (42, 109) exceeding the criteria of 93.17. Further data analysis retained both the data sets.

#### *Normality Test*

Normality test results, including normality and scatter plot, ANOVA, histogram, normal P-P plot, and scatter plot, were analyzed (Appendix H) (Mertler & Vannatta, 2013). The skewness value showed the symmetry of the distribution, and the kurtosis value showed the peakedness of the distribution. Skewness and kurtosis decreased after removing five extreme values (Meyers, Gamst, & Guarino, 2006). As a result, skewness and kurtosis values were 0.645 and 1.453, respectively, in an acceptable range (Kline, 2011). The normal P-P plot and the normal Q-Q plot showed most of the instances very close to the central diagonal line demonstrating adequate range (Mertler & Reinhart, 2017; Tabachnick, Fidell, & Ullman, 2007). The R-squared value described the dependent variable variation percentage that the research model described. The R-squared value of 66% was in the suitable range. The overall pre-analysis of the data was within an acceptable range.

## Demographics

The demographic variables gathered were gender, age, education, social engineering, and information security breach exposure. Sixty-six participants were males (51.16%), sixty-two participants were females (48.06%), and one participant identified in the other category.

Table 3 exhibited the participants' gender distribution.

Table 3

### *Participants Gender Demographics*

Gender	Frequency	Percentage
Male	66	51.16%
Female	62	48.06%
Other	1	0.78%
Total	129	100.00%

The most of participants were between the ages of 45-54 (28.68%), followed by 55-64 (23.26%), 35-44 (22.48%), 25-34 (12.40%), over 65 years (10.08%), and 18-24 (3.1%).

Table 4 displayed the participants' age distribution.

Table 4

### *Participants Age Demographics*

Age	Frequency	Percentage
18-24	4	3.10%
25-34	16	12.40%
35-44	29	22.48%
45-54	37	28.68%
55-64	30	23.26%
Over 65 Years	13	10.08%
Total	129	100.00%

The most of participants had a Bachelor's degree (51.16), followed by a Master's degree (18.6%), Associate degree (10.85%), some college and no degree (9.3%), high school graduate (6.98%), Doctoral degree (2.33%), and some school no degree (0.78%). Table 5 presented the participants' education distribution.

Table 5

*Participants Education Demographics*

Age	Frequency	Percentage
Some School, No Degree	1	0.78%
High School Graduate	9	6.98%
Some College, No Degree	12	9.30%
Associate's Degree	14	10.85%
Bachelor's Degree	66	51.16%
Master's Degree	24	18.60%
Doctoral Degree	3	2.33%
Total	129	100.00%

71.32% of participants had some exposure to social engineering breaches, 24.03% had extensive exposure to social engineering breaches, and 4.65% had no exposure to social engineering breaches. Table 6 demonstrated the participants' social engineering breach exposure demographics.

Table 6

*Participants Social Engineering Breach Exposure Demographics*

Age	Frequency	Percentage
None	6	4.65%
Some	92	71.32%
Extensive	31	24.03%
Total	129	100.00%

## **Data Analysis**

The data was loaded into CSV format to import into SmartPLS, version 3.0, for analysis. In general, there are different approaches for analyzing the formative versus reflective measurement model. The constructs in this research study were reflective. The research model evaluation included measurement and structural models (Haenlein & Kaplan, 2004; Steenkamp & Baumgartner, 2000).

## **Measurement Model**

The measurement model signified the relationships between the observed data and the latent variables. The measurement model estimated the latent variables as its manifest variables' weighted sum (Bagozzi & Yi, 1988; Henseler & Chin, 2010). The measurement model analysis encompassed an in-depth analysis of the relationships between manifest indicators. The evaluation included outer loadings, composite reliability and validity, Cronbach's alpha ( $\alpha$ ), average variance extracted (AVE), cross-loadings, and model fit.

### *Convergent Validity and Outer Loadings*

Convergent validity states the degree to which a measure compares positively with the same construct's alternative measures (Hair et al., 2017). Convergent validity evaluation comprised of construct measurement item's outer loadings assessment. Table 7 exhibited the initial values for outer loadings for each construct's measurement items. Moreover, Table 7 highlighted SP04 and SP05 because their values were below 0.40 (Hair et al., 2010). The further analysis excluded the indicator's outer loadings with a value below 0.40 (Hair et al., 2017). The second round of PLS calculation omitted SP04 and SP05.

Table 7

*Initial Outer Loadings*

Item	Loading	Item	Loading	Item	Loading
Perceived Severity		Response efficacy		Security Policies	
PS01	0.84	RE01	0.977	SP01	0.959
PS02	0.862	RE02	0.923	SP02	0.945
PS03	0.853	RE03	0.935	SP03	0.602
PS04	0.944	RE04	0.932	SP04	<b>0.332</b>
PS05	0.948	RE05	0.913	SP05	<b>0.368</b>
Perceived Vulnerability		Self-efficacy		Protection Motivation	
PV01	0.826	SE01	0.973	PM01	0.965
PV02	0.854	SE02	0.943	PM02	0.902
PV03	0.779	SE03	0.917	PM03	0.871
PV04	0.898	SE04	0.932	PM04	0.91
PV05	0.95	SE05	0.937	PM05	0.898
Fear		Response Cost		Protection Behavior	
FE01	0.78	RC01	0.693	PB01	0.87
FE02	0.979	RC02	0.817	PB02	0.903
FE03	0.805	RC03	0.772	PB03	0.87
FE04	0.808	RC04	0.803	PB04	0.834
FE05	0.909	RC05	0.762	PB05	0.856
Maladaptive Rewards		SETA Program			
MR01	0.832	ST01	0.931		
MR02	0.895	ST02	0.866		
MR03	0.872	ST03	0.873		
MR04	0.961	ST04	0.853		
MR05	0.92	ST05	0.854		

Table 8 exhibited the final values for outer loadings for each construct's measurement items.

Table 8

*Final Outer Loadings*

Item	Loading	Item	Loading	Item	Loading
Perceived Severity		Response efficacy		Security Policies	
PS01	0.84	RE01	0.977	SP01	0.958
PS02	0.862	RE02	0.923	SP02	0.942
PS03	0.853	RE03	0.935	SP03	0.614
PS04	0.944	RE04	0.932		
PS05	0.948	RE05	0.913		
Perceived Vulnerability		Self-efficacy		Protection Motivation	
PV01	0.826	SE01	0.973	PM01	0.965
PV02	0.854	SE02	0.943	PM02	0.902
PV03	0.779	SE03	0.917	PM03	0.871
PV04	0.898	SE04	0.932	PM04	0.91
PV05	0.95	SE05	0.937	PM05	0.898
Fear		Response Cost		Protection Behavior	
FE01	0.78	RC01	0.693	PB01	0.871
FE02	0.979	RC02	0.817	PB02	0.903
FE03	0.805	RC03	0.772	PB03	0.87
FE04	0.808	RC04	0.803	PB04	0.833
FE05	0.909	RC05	0.762	PB05	0.856
Maladaptive Rewards		SETA Program			
MR01	0.832	ST01	0.931		
MR02	0.895	ST02	0.866		
MR03	0.872	ST03	0.873		
MR04	0.961	ST04	0.853		
MR05	0.92	ST05	0.854		

*Construct Reliability and Validity*

Table 9 presented internal consistency Cronbach's Alpha ( $\alpha$ ) statistics. Cronbach's Alpha statistics values between 0.60 and 0.70 are considered less than desirable (Hair et al., 2010). Cronbach's Alpha statistics values should be greater than 0.70 (Cronbach, 1951). All the constructs had Cronbach's Alpha greater than 0.70, hence fulfilled construct reliability criteria.

Convergent validity criteria include Average Variance Extracted (AVE) values required to be greater than 0.50 (Hair et al., 2010). Convergent validity criteria also comprise that the AVE's square root must be greater than 0.707 (Fornell & Larcker, 1981; Götz, Liehr-Gobbers, & Krafft, 2010). Therefore, all the constructs' AVE being greater than 0.50 and the square root of the AVE being greater than 0.707 resulted in acceptable convergent reliability and validity criteria.

Table 9

*Construct Reliability and Validity*

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Fear	0.91	0.926	0.933	0.739
Maladaptive rewards	0.939	0.939	0.954	0.805
Protection Behavior	0.917	0.921	0.938	0.752
Protection Motivation	0.948	0.95	0.96	0.827
Perceived Severity	0.934	0.938	0.95	0.793
Perceived Vulnerability	0.914	0.926	0.936	0.746
Response Cost	0.834	0.857	0.879	0.594
Response Efficacy	0.965	0.966	0.973	0.877
Self-efficacy	0.967	0.987	0.975	0.885
Security Policies	0.812	0.943	0.885	0.727
SETA Program	0.926	0.945	0.943	0.767



### *Discriminant Validity*

The discriminant validity requires that a reflective construct has the most solid relationships with its indicators than the other constructs (Götz et al., 2010). Discriminant validity measured the degree to which a construct was empirically different from other constructs (Hair et al., 2017). Three criteria, including cross-loadings, the Fornell-Larcker criterion, and the Heterotrait-Monotrait Ratio (HTMT), were utilized.

The cross-loading criterion means that a manifest indicator's outer loading should surpass its outer loadings on the remaining constructs (Hair et al., 2017). Cross-loadings of the threat appraisal items are shown in Table 10, coping appraisal items in Table 11, and protection items in Table 12. Indicators had the most substantial relationship with their assigned latent construct than the remaining latent constructs (Gefen & Straub, 2005). Each indicator stated the maximum value with its corresponding construct, whereas all remaining cross-loadings were lower than its related construct. All indicators had a minimum value of 0.70 (Fornell & Larcker, 1981). The indicators had the most solid relationship with their assigned latent construct than with the remaining latent constructs. The difference was at least .10 or more between the loading and the next highest loading, therefore, satisfying the cross-loading criterion for discriminant validity (Fornell & Larcker, 1981).

Table 10

*Cross-Loadings of Threat Appraisal Items*

	FE	MR	PB	PM	PS	PV	RC	RE	SE	SP	ST
<b>Perceived Severity</b>											
PS01	0.489	0.279	0.461	0.508	<b>0.840</b>	0.43	-0.047	0.358	0.053	0.119	0.326
PS02	0.508	0.236	0.347	0.365	<b>0.862</b>	0.306	-0.035	0.257	0.101	0.07	0.342
PS03	0.476	0.258	0.378	0.441	<b>0.853</b>	0.383	0.062	0.355	0.104	0.067	0.312
PS04	0.545	0.246	0.461	0.517	<b>0.944</b>	0.388	-0.02	0.36	0.103	0.07	0.362
PS05	0.493	0.242	0.366	0.474	<b>0.948</b>	0.385	-0.008	0.367	0.064	0.034	0.312
<b>Perceived Vulnerability</b>											
PV01	0.636	0.544	0.598	0.574	0.422	<b>0.826</b>	0.028	0.571	0.196	0.125	0.438
PV02	0.433	0.417	0.538	0.597	0.358	<b>0.854</b>	0.148	0.676	0.181	0.037	0.408
PV03	0.299	0.258	0.388	0.47	0.299	<b>0.779</b>	0.05	0.441	0.22	0.082	0.202
PV04	0.385	0.404	0.489	0.544	0.32	<b>0.898</b>	0.143	0.542	0.237	0.185	0.374
PV05	0.504	0.411	0.528	0.576	0.413	<b>0.950</b>	0.077	0.577	0.189	0.062	0.357
<b>Fear</b>											
FE01	<b>0.780</b>	0.207	0.385	0.33	0.362	0.349	-0.067	0.251	0.037	-0.049	0.307
FE02	<b>0.979</b>	0.339	0.54	0.545	0.54	0.506	-0.025	0.432	0.155	0.005	0.411
FE03	<b>0.805</b>	0.351	0.535	0.473	0.452	0.485	-0.017	0.422	0.163	0.032	0.318
FE04	<b>0.808</b>	0.383	0.51	0.528	0.448	0.464	0.052	0.461	0.094	0.027	0.342
FE05	<b>0.909</b>	0.381	0.574	0.58	0.583	0.49	0.034	0.524	0.205	0.124	0.477
<b>Maladaptive Rewards</b>											
MR01	0.357	<b>0.832</b>	0.462	0.328	0.165	0.369	0.05	0.463	0.157	0.161	0.457
MR02	0.382	<b>0.895</b>	0.451	0.334	0.27	0.442	0.126	0.414	0.181	0.163	0.546
MR03	0.323	<b>0.872</b>	0.456	0.326	0.287	0.484	0.155	0.352	0.165	0.151	0.484
MR04	0.362	<b>0.961</b>	0.47	0.335	0.278	0.446	0.094	0.438	0.129	0.184	0.526
MR05	0.343	<b>0.920</b>	0.5	0.351	0.27	0.431	0.09	0.416	0.164	0.137	0.528

Table 11

*Cross-Loadings of Coping Appraisal Items*

	FE	MR	PB	PM	PS	PV	RC	RE	SE	SP	ST
<b>Response Efficacy</b>											
RE01	0.504	0.468	0.65	0.708	0.388	0.66	0.151	<b>0.977</b>	0.251	0.186	0.456
RE02	0.434	0.442	0.605	0.654	0.392	0.587	0.214	<b>0.923</b>	0.335	0.23	0.428
RE03	0.414	0.441	0.592	0.619	0.31	0.603	0.215	<b>0.935</b>	0.275	0.191	0.404
RE04	0.477	0.445	0.642	0.687	0.385	0.596	0.197	<b>0.932</b>	0.272	0.221	0.433
RE05	0.498	0.379	0.668	0.663	0.313	0.631	0.149	<b>0.913</b>	0.219	0.173	0.448
<b>Self-efficacy</b>											
SE01	0.212	0.257	0.429	0.374	0.139	0.288	0.148	0.392	<b>0.973</b>	0.24	0.359
SE02	0.113	0.169	0.317	0.293	0.066	0.242	0.146	0.261	<b>0.943</b>	0.172	0.304
SE03	0.146	0.118	0.357	0.282	0.095	0.177	0.112	0.226	<b>0.917</b>	0.2	0.263
SE04	0.124	0.107	0.276	0.269	0.067	0.19	0.091	0.212	<b>0.932</b>	0.159	0.201
SE05	0.139	0.15	0.312	0.243	0.061	0.177	0.051	0.219	<b>0.937</b>	0.169	0.267
<b>Response Cost</b>											
RC01	0.031	0.127	0.065	0.079	-0.062	0.062	<b>0.693</b>	0.089	0.059	0.153	-0.023
RC02	-0.076	0.066	0.133	0.199	-0.046	0.076	<b>0.817</b>	0.168	0.138	0.097	0.015
RC03	0.031	0.077	0.143	0.166	-0.038	0.109	<b>0.772</b>	0.215	0.143	0.09	0.022
RC04	0.052	0.087	0.142	0.191	0.009	0.06	<b>0.803</b>	0.139	0.109	0.189	-0.053
RC05	-0.018	0.122	0.075	0.135	0.087	0.087	<b>0.762</b>	0.114	-0.03	0.099	-0.04

Table 12

*Cross-Loadings of Protection Items*

	FE	MR	PB	PM	PS	PV	RC	RE	SE	SP	ST
<b>Security Policies</b>											
SP01	0.059	0.22	0.156	0.166	0.1	0.151	0.155	0.242	0.221	<b>0.958</b>	0.154
SP02	-0.002	0.112	0.14	0.127	0.051	0.071	0.169	0.152	0.185	<b>0.942</b>	0.151
SP03	0.062	0.108	0.06	0.119	0.052	0.04	0.046	0.15	0.073	<b>0.614</b>	0.107
<b>SETA Program</b>											
ST01	0.412	0.628	0.479	0.355	0.329	0.467	0.027	0.415	0.335	0.16	<b>0.931</b>
ST02	0.453	0.451	0.535	0.483	0.403	0.375	-0.001	0.538	0.239	0.179	<b>0.866</b>
ST03	0.33	0.409	0.472	0.398	0.357	0.325	-0.041	0.445	0.246	0.211	<b>0.873</b>
ST04	0.352	0.509	0.355	0.268	0.227	0.355	-0.029	0.295	0.27	0.046	<b>0.853</b>
ST05	0.345	0.503	0.314	0.207	0.261	0.312	-0.052	0.242	0.229	0.061	<b>0.854</b>
<b>Protection Motivation</b>											
PM01	0.568	0.356	0.695	<b>0.965</b>	0.488	0.594	0.172	0.663	0.264	0.1	0.367
PM02	0.544	0.288	0.624	<b>0.902</b>	0.443	0.57	0.182	0.602	0.273	0.12	0.308
PM03	0.513	0.202	0.588	<b>0.871</b>	0.48	0.506	0.131	0.564	0.242	0.066	0.317
PM04	0.5	0.427	0.685	<b>0.91</b>	0.464	0.647	0.209	0.704	0.36	0.176	0.412
PM05	0.527	0.402	0.685	<b>0.898</b>	0.495	0.605	0.265	0.695	0.294	0.252	0.449
<b>Protection Behavior</b>											
PB01	0.551	0.476	<b>0.871</b>	0.678	0.429	0.574	0.139	0.661	0.253	0.022	0.424
PB02	0.583	0.502	<b>0.903</b>	0.648	0.38	0.524	0.157	0.576	0.406	0.169	0.486
PB03	0.483	0.444	<b>0.87</b>	0.572	0.4	0.487	0.131	0.523	0.385	0.237	0.452
PB04	0.398	0.39	<b>0.833</b>	0.54	0.3	0.431	0.104	0.49	0.326	0.229	0.427
PB05	0.563	0.442	<b>0.856</b>	0.678	0.451	0.566	0.131	0.657	0.226	0.019	0.418

Fornell and Larcker criterion is a reliable method for evaluating discriminant validity and preventing multicollinearity issues (Hair et al., 2010). Discriminant validity requires the square root of every AVE value related to each latent construct to be more significant than any correlation amongst any latent constructs pair (Fornell & Larcker, 1981). Every AVE square root for each latent construct was greater than the correlation with any other latent

construct, as exhibited in Table 13, meeting the Fornell and Larcker criterion requirements of discriminant validity.

Table 13

*Fornell-Larcker Criterion*

	FE	MR	PB	PM	PS	PV	RC	RE	SE	SP	ST
FE	<b>0.859</b>										
MR	0.395	<b>0.897</b>									
PB	0.6	0.522	<b>0.867</b>								
PM	0.583	0.374	0.723	<b>0.91</b>							
PS	0.565	0.284	0.455	0.521	<b>0.891</b>						
PV	0.54	0.485	0.599	0.645	0.427	<b>0.863</b>					
RC	0	0.115	0.154	0.213	-0.012	0.102	<b>0.771</b>				
RE	0.498	0.465	0.675	0.713	0.383	0.658	0.197	<b>0.936</b>			
SE	0.16	0.177	0.366	0.317	0.095	0.234	0.121	0.288	<b>0.941</b>		
SP	0.04	0.177	0.15	0.16	0.081	0.113	0.159	0.214	0.203	<b>0.853</b>	
ST	0.438	0.567	0.509	0.41	0.372	0.424	-0.018	0.464	0.302	0.162	<b>0.876</b>

Heterotrait-Monotrait (HTMT) ratio is a dependable criterion to complement the Fornell-Larcker (1981) and cross-loadings to evaluate discriminant validity (Henseler, Ringle, & Sarstedt, 2015). The complete bootstrapping function in SmartPLS 3.0 generated the HTMT value to assess discriminant validity. The bootstrap calculation, with the number of cases parameter equal to 5,000, two-tailed test type, and significance level of 0.05, was performed. Table 14 showed the HTMT ratio evaluation results. As per the HTMT criterion for discriminant validity, the HTMT statistic confidence interval did not surpass 1 for all combinations of constructs (Hair et al., 2017). Discriminant validity between latent constructs was adequate as per Heterotrait-Monotrait (HTMT) criterion.

Table 14

*Heterotrait-Monotrait Ratio (HTMT)*

	Original Sample (O)	Sample Mean (M)	2.50%	97.50%		Original Sample (O)	Sample Mean (M)	2.50%	97.50%
MR -> FE	0.42	0.422	0.246	0.581	RE -> RC	0.21	0.23	0.08	0.482
PB -> FE	0.645	0.647	0.537	0.738	SE -> FE	0.159	0.18	0.066	0.342
PB -> MR	0.56	0.556	0.353	0.707	SE -> MR	0.179	0.19	0.063	0.377
PM -> FE	0.618	0.616	0.503	0.715	SE -> PB	0.384	0.38	0.195	0.559
PM -> MR	0.391	0.389	0.184	0.572	SE -> PM	0.323	0.32	0.111	0.506
PM -> PB	0.769	0.764	0.626	0.867	SE -> PS	0.096	0.13	0.05	0.273
PS -> FE	0.604	0.604	0.462	0.729	SE -> PV	0.246	0.25	0.075	0.443
PS -> MR	0.303	0.309	0.134	0.483	SE -> RC	0.135	0.17	0.081	0.346
PS -> PB	0.486	0.485	0.331	0.621	SE -> RE	0.289	0.28	0.084	0.487
PS -> PM	0.551	0.55	0.383	0.694	SP -> FE	0.088	0.14	0.074	0.267
PV -> FE	0.569	0.565	0.415	0.694	SP -> MR	0.197	0.22	0.07	0.463
PV -> MR	0.51	0.508	0.322	0.667	SP -> PB	0.171	0.23	0.096	0.438
PV -> PB	0.64	0.633	0.476	0.762	SP -> PM	0.18	0.2	0.066	0.424
PV -> PM	0.686	0.678	0.542	0.786	SP -> PS	0.091	0.14	0.054	0.313
PV -> PS	0.453	0.45	0.284	0.596	SP -> PV	0.128	0.18	0.085	0.354
RC -> FE	0.077	0.155	0.088	0.269	SP -> RC	0.197	0.24	0.109	0.432
RC -> MR	0.144	0.196	0.08	0.419	SP -> RE	0.241	0.25	0.071	0.492
RC -> PB	0.163	0.205	0.083	0.445	SP -> SE	0.208	0.23	0.075	0.419
RC -> PM	0.225	0.243	0.084	0.492	ST -> FE	0.465	0.46	0.307	0.598
RC -> PS	0.086	0.149	0.083	0.263	ST -> MR	0.611	0.61	0.414	0.768
RC -> PV	0.121	0.184	0.088	0.387	ST -> PB	0.533	0.52	0.317	0.69
RE -> FE	0.519	0.518	0.39	0.628	ST -> PM	0.414	0.41	0.208	0.589
RE -> MR	0.489	0.484	0.296	0.641	ST -> PS	0.386	0.39	0.225	0.532
RE -> PB	0.712	0.7	0.532	0.831	ST -> PV	0.442	0.44	0.247	0.621
RE -> PM	0.742	0.735	0.596	0.837	ST -> RC	0.058	0.15	0.077	0.293
RE -> PS	0.401	0.397	0.213	0.55	ST -> RE	0.466	0.46	0.236	0.639
RE -> PV	0.693	0.688	0.518	0.817	ST -> SE	0.312	0.31	0.114	0.506
					ST -> SP	0.174	0.21	0.079	0.431

*Model Fit*

Model Fit included Standardized Root Mean Square Residual (SRMR) assessment.

SRMR is an absolute measure of fit and the standardized variance between the predicted

correlation and the observed correlation (Henseler, Hubona, & Ray, 2016). A value of zero specifies perfect fit, given that the SRMR is an absolute measure of fit (Hu & Bentler, 1999). SRMR value of less than 0.08 is an acceptable value (Hu & Bentler, 1999). Table 15 showed model fit results. The SRMR value was 0.0686 for the estimated model, resulting in a good model fit (Hu & Bentler, 1999).

Table 15

*Model Fit*

	Saturated Model	Estimated Model
SRMR	0.065	0.074
d_ULS	5.998	7.765
d_G	5.542	5.66
Chi-Square	2731.608	2752.761
NFI	0.686	0.684

In conclusion, the measurement model analysis was sufficient to begin the next set of investigations for the structural model.

### **Structural Model**

The structural model signified the relationships amongst the latent constructs (Wong, 2013). Evaluation incorporated collinearity statistics (VIF), coefficient of determination ( $R^2$ ), path coefficients ( $\beta$ ), effect size ( $f^2$ ), predictive relevance ( $Q^2$ ), Importance-Performance Map Analysis (IPMA), and PLS predict ( $Q^2$  Predict).

#### *Collinearity*

Variance Inflation Factor (VIF), a measure of collinearity, provided the reciprocal of the tolerance (Hair et al., 2017). In most cases, the VIF values lower than five have been considered acceptable (Hair et al., 2017). Table 16 presented collinearity statistics (VIF)

results. The VIF values were below five for the estimated model, representing acceptable collinearity.

Table 16

*Collinearity Statistics (VIF)*

	Fear	Protection Motivation	Protection Behavior
Perceived severity	1.223	1.525	
Perceived vulnerability	1.223	2.100	
Fear		1.848	
Maladaptive rewards		1.407	
Response efficacy		2.048	
Self-efficacy		1.103	
Response Cost		1.065	
SETA Program			1.216
Security Policies			1.038
Protection Motivation			1.215

*Path Coefficients*

Path coefficient values range between -1 to +1, with 0 or close to 0 stating statistically insignificant impact (Hair et al., 2017). The individual path coefficients were derived as the following steps, as shown in Table 17. The evaluation of algebraic signs and values of path coefficients followed next. *t* statistics and *p*-value evaluation demonstrated the significance of the path coefficient at either the .05, .01 or .001 confidence interval levels.



Table 17

*Path Coefficients*

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	<i>t</i> Statistics ( O/STDEV )	<i>p</i> - Values
<b>Fear</b>					
PS -> FE	0.408	0.408	0.074	5.488	<.001
PV -> FE	0.366	0.37	0.076	4.786	<.001
<b>Protection Motivation</b>					
FE -> PM	0.176	0.175	0.076	2.313	0.021
PS -> PM	0.194	0.192	0.083	2.325	0.020
PV -> PM	0.202	0.194	0.084	2.391	0.017
MR -> PM	-0.064	-0.058	0.069	0.932	0.351
RE -> PM	0.395	0.392	0.084	4.702	<.001
SE -> PM	0.107	0.109	0.055	1.936	0.053
RC -> PM	0.111	0.119	0.065	1.709	0.088
<b>Protection Behavior</b>					
ST -> PB	0.254	0.249	0.098	2.593	0.01
SP -> PB	0.010	0.013	0.07	0.139	0.89
PM -> PB	0.617	0.615	0.075	8.273	<.001

Figure 2 showed the final research model results.

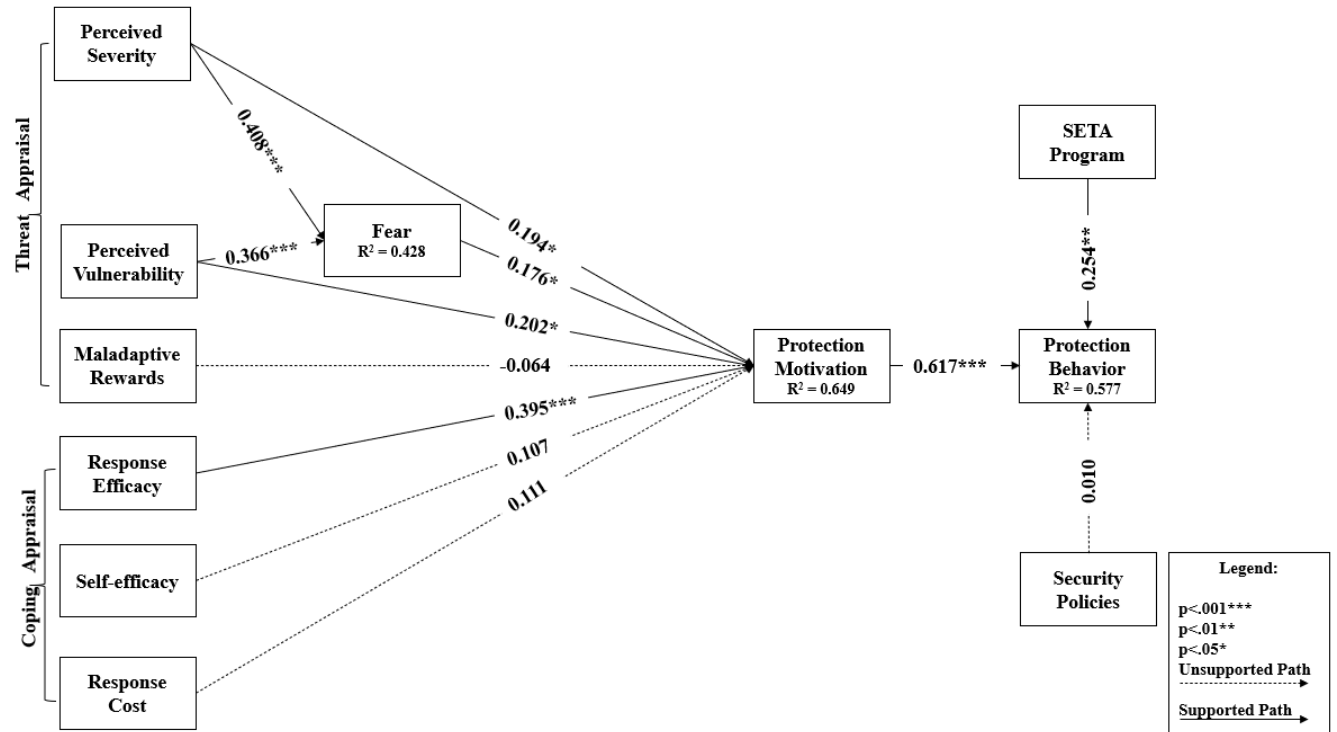


Figure 2. Final Research Model

### Hypothesis Summary

*T* statistics values should be greater than 1.96 (Two-Tailed test type and significance level of 0.05) to support a hypothesis (Hair et al., 2017). The direct effect of perceived severity on fear was statistically significant ( $\beta = 0.408, p < 0.001, t = 5.488$ ), supporting hypothesis H1. This result indicated that the degree to which a user believes in the danger would create substantial damage impacts their fear, as demonstrated by the work of Floyd et al. (2000). Similarly, the direct effect of perceived vulnerability on fear was statistically significant ( $\beta = 0.366, p < 0.001, t = 4.786$ ), supporting hypothesis H2. This result specified that a user's credence in their exposure to social engineering impacts their emotional response to that danger, as demonstrated by the work of Floyd et al. (2000). The direct effect of fear on protection motivation was statistically significant ( $\beta = 0.176, p < 0.05, t = 2.313$ ), supporting hypothesis H3. This result implied that fear could motivate a user to take protective action

against social engineering breaches, as established by the research of Rogers (1975) and Witte (1994).

The direct effect of perceived severity on protection motivation was statistically significant ( $\beta=0.194$ ,  $p<0.05$ ,  $t=2.325$ ), supporting hypothesis H4. This effect indicated that the users' belief in the degree of substantial damage impacts their motivation to exhibit protection behavior, as shown by the research of Crossler and Bélanger (2014). Additionally, the direct effect of perceived vulnerability on protection motivation was statistically significant ( $\beta=0.202$ ,  $p<0.05$ ,  $t=2.391$ ), supporting hypothesis H5. This effect specified a user's susceptibility in their exposure to social engineering impacts their motivation to exhibit protection behavior, as demonstrated by the work of Ifinedo (2012).

The direct effect of maladaptive rewards on protection motivation was statistically insignificant ( $\beta=-0.064$ ,  $p=0.351$ ,  $t=0.932$ ), not supporting hypothesis H6. This result specified that the perceived benefits of not executing protection behaviors to prevent social engineering breaches did not influence users' motivation to perform these protection behaviors (Dang-Pham & Pittayachawan, 2015). The direct effect of response efficacy on protection motivation was statistically significant ( $\beta=0.395$ ,  $p<0.001$ ,  $t=4.702$ ), supporting hypothesis H7. This result implied that users' confidence in the efficiency of a protection behavior to prevent social engineering breach is correlated to their motivation to exhibit these behaviors, as demonstrated by the research of Yoon et al. (2012).

The direct effect of self-efficacy on protection motivation was statistically insignificant ( $\beta=0.107$ ,  $p=0.053$ ,  $t=1.936$ ), not supporting hypothesis H8. This result implied that users' belief in their ability to perform protection action does not impact their motivation to perform the protection behavior (Siponen et al., 2010). In contrast, the direct effect of response cost

on protection motivation was statistically insignificant ( $\beta=0.111, p=0.088, t=1.709$ ), not supporting hypothesis H9. This result showed that users' perception of the costs acquired by execution of protection has no significant influence on their motivation to perform these protection behaviors (Ng et al., 2009). The direct effect of protection motivation on protection behavior was statistically significant ( $\beta=0.617, p<0.001, t=8.273$ ), supporting hypothesis H10. This effect implied that users' motivation to perform protection behaviors to prevent social engineering breaches is correlated to their recital of these behaviors, as demonstrated by the research of Boss et al. (2015).

The direct effect of the SETA program on protection behavior was statistically significant ( $\beta=0.254, p=0.01, t=2.593$ ), supporting hypothesis H11. This result showed that an organization's SETA program significantly impacts users' protection behavior to prevent social engineering breaches (D'Arcy & Hovav, 2007). The direct effect of security policies on protection behavior was statistically insignificant ( $\beta=0.01, p=0.89, t=0.139$ ), not supporting hypothesis H12. This result showed that an organization's security policies do not significantly impact users' protection behavior to prevent social engineering breaches (Lee et al., 2004). One of the reasons could be that the user is not well-aware of the organization's security policies. Table 18 presented support for the hypothesized relationships.

Table 18

*Hypothesis Summary*

Hypothesis	Result
H1 Perceived severity is positively associated with fear.	Supported
H2 Perceived vulnerability is positively associated with fear.	Supported
H3 Fear is positively associated with protection motivation.	Supported
H4 Perceived severity is positively associated with protection motivation.	Supported
H5 Perceived vulnerability is positively associated with protection motivation.	Supported
H6 Maladaptive rewards are negatively associated with protection motivation.	Not Supported
H7 Response efficacy is positively associated with protection motivation.	Supported
H8 Self-efficacy is positively associated with protection motivation.	Not Supported
H9 Response cost is negatively associated with protection motivation.	Not Supported
H10 Protection motivation is positively associated with protection behavior.	Supported
H11 SETA program is positively associated with protection behavior.	Supported
H12 Security policies are positively associated with protection behavior.	Not Supported

*Total Effects*

Bootstrapping utilizes resampling methods to determine the significance of PLS coefficients. PLS-SEM relies on a bootstrap procedure to make statistical inferences.

Bootstrapping output evaluation encompassed the direct, indirect, and total effects. The total effect was the sum of direct and indirect effects, as shown in Table 19. Direct effects were the relationships between two latent constructs directly connected by a single-headed arrow (Hair et al., 2017). On the other hand, indirect effects were the relationships between two latent constructs not directly connected by a single-headed arrow; though, a third construct intervened (Hair et al., 2017).

The response efficacy had the maximum direct effect on protection motivation than any other independent constructs (i.e., perceived severity, perceived vulnerability, fear, maladaptive rewards, self-efficacy, and response costs). Therefore, the most significant impact on protection motivation is a user's belief in the efficiency of the recommended security measures to prevent social engineering threats.

Table 19

*Total Effects*

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	<i>t</i> Statistics ( O/STDEV )	<i>p</i> -Values
<b>Fear</b>					
PS -> FE	0.408	0.408	0.074	5.488	<.001
PV -> FE	0.366	0.37	0.076	4.786	<.001
<b>Protection Motivation</b>					
FE -> PM	0.176	0.175	0.076	2.313	0.021
PS -> PM	0.265	0.262	0.075	3.554	<.001
PV -> PM	0.266	0.26	0.075	3.555	<.001
MR -> PM	-0.064	-0.058	0.069	0.932	0.351
RE -> PM	0.395	0.392	0.084	4.702	<.001
SE -> PM	0.107	0.109	0.055	1.936	0.053
RC -> PM	0.111	0.119	0.065	1.709	0.088
<b>Protection Behavior</b>					
ST -> PB	0.254	0.249	0.098	2.593	0.01
SP -> PB	0.01	0.013	0.07	0.139	0.89
PM -> PB	0.617	0.615	0.075	8.273	<.001
FE -> PB	0.109	0.109	0.051	2.119	0.034
PS -> PB	0.164	0.161	0.051	3.241	0.001
PV -> PB	0.164	0.16	0.05	3.31	0.001
MR -> PB	-0.039	-0.035	0.042	0.941	0.347
RE -> PB	0.244	0.241	0.059	4.157	<.001
SE -> PB	0.066	0.067	0.036	1.838	0.066
RC -> PB	0.069	0.073	0.041	1.682	0.093

*Coefficient of Determination*

R<sup>2</sup> results, also known as the coefficient of determination, provided a measure of the predictive power and fitness to the observed data in the regression analysis (Hair et al., 2017; Sarstedt, Wilczynski, & Melewar, 2013). R<sup>2</sup> values assessed the exogenous latent variable's cumulative effects on the endogenous latent variables as one of the essential steps for prediction analysis (Hair et al., 2017; Roldán & Sánchez-Franco, 2012). R<sup>2</sup> values of 0.67,

0.33, and 0.19 are substantial, moderate, and weak, correspondingly (Chin, 1998). Table 20 exhibited  $R^2$  results for the estimated model. The estimated model in this research study could explain 42.8% of the variance in fear, 64.9 % of the variance in protection motivation, and 57.7% of the variance in protection behavior. As a result,  $R^2$  results exceeded the moderate level threshold recommended for the coefficient of determination.

Table 20

*R Square*

	R Square	R Square Adjusted
Fear	0.428	0.419
Protection Motivation	0.649	0.628
Protection Behavior	0.577	0.566

*Effect Size*

Effect size ( $f^2$ ) evaluation provided the degree to which exogenous latent constructs contributed to the coefficient of determination of endogenous constructs. The  $f^2$  effect size values of 0.02, 0.15, and 0.35 are evaluated as small, median, and large effects (Hair et al., 2017). Subsequently, effect size values of less than 0.02 are not affected (Hair et al., 2017).

Table 21 presented the effect size of the estimated model.

Table 21

*f Square*

	Fear	Protection Motivation	Protection Behavior
Perceived severity	0.239	0.07	
Perceived vulnerability	0.191	0.055	
Fear		0.048	
Maladaptive rewards		0.008	
Response efficacy		0.218	
Self-efficacy		0.03	
Response Cost		0.033	
SETA Program			0.125
Security Policies			0
Protection Motivation			0.74

*Predictive Relevance*

The blindfolding procedure provided the predictive relevance ( $Q^2$ ) values of latent variables. The blindfolding process evaluated the  $Q^2$  of the path model by re-using the samples, systematically removing data points, and delivering a prediction of their original values (Hair et al., 2017). The blindfolding calculation encompassed an omission distance of seven. Table 22 displayed the results of the blindfolding. Overall, the  $Q^2$  values were above zero, confirming the predictive relevance of the estimated model (Hair et al., 2017).

Table 22

*Q Square*

	Q Square
Fear	0.302
Protection Behavior	0.417
Protection Motivation	0.517



### Important-Performance Map Analysis

Importance-Performance Map Analysis (IPMA) outspreads the estimated model by adding the performance of each construct into the interpretation. It provides the evaluation on two dimensions, including importance and performance. IPMA for protection behavior incorporated selecting direct predecessors of the chosen target construct. Figure 3 presented IPMA results.

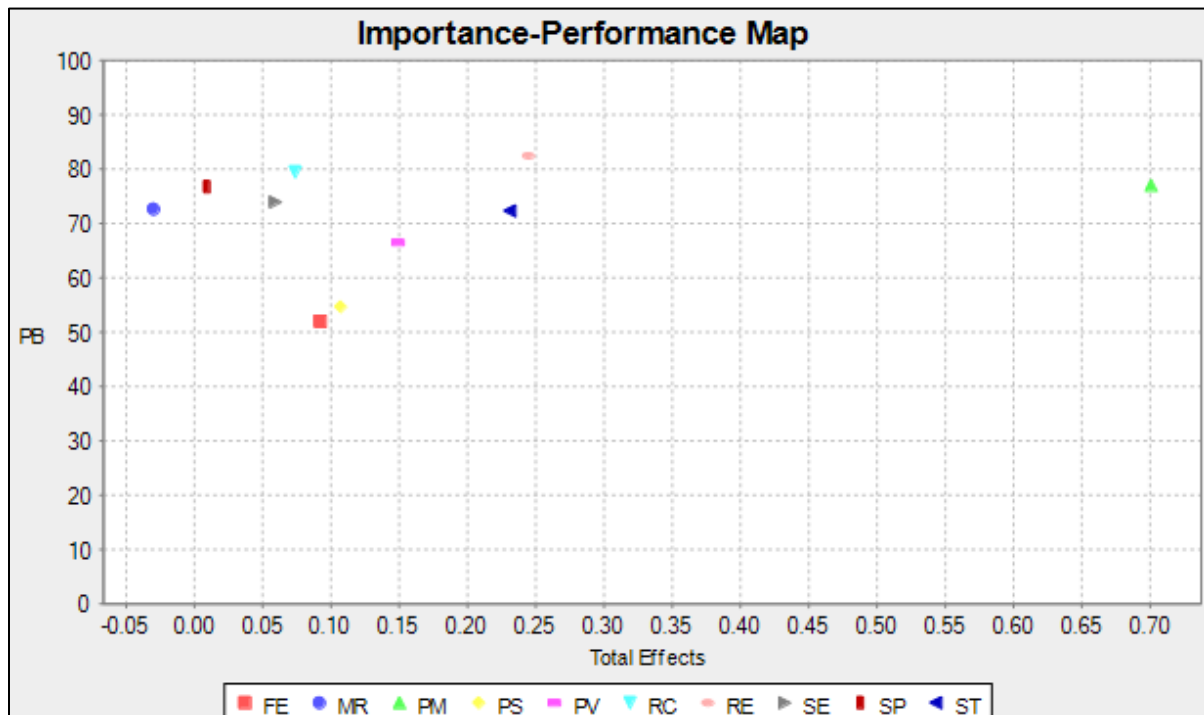


Figure 3. Important-Performance Map Analysis (IPMA)

### PLS Predict

PLS predict assessment encompassed ten folds and repetitions to predict PLS path models and evaluate their predictive performance. PLS (partial least squares) model, as well as LM (linear regression) model evaluation, incorporated a comparison between the root means squared error (RMSE) and the mean absolute error (MAE). Table 23 presented the PLS

predict results. The PLS  $Q^2$  values were bigger than zero, and the  $Q^2$  LM values were lower than the  $Q^2$  PLS values, which confirmed acceptable PLS predict assessment.

Table 23

*PLS Predict Assessment*

	PLS			LM			PLS-LM		
	RMSE	MAE	$Q^2_{predict}$	RMSE	MAE	$Q^2_{predict}$	RMSE	MAE	$Q^2_{predict}$
PB01	0.928	0.732	0.412	1.074	0.846	0.212	-0.146	-0.114	0.2
PB02	0.931	0.734	0.395	1.047	0.823	0.234	-0.116	-0.089	0.161
PB03	1.044	0.832	0.345	1.244	0.997	0.069	-0.2	-0.165	0.276
PB04	1.197	0.932	0.273	1.483	1.159	-0.116	-0.286	-0.227	0.389
PB05	0.845	0.69	0.409	0.991	0.783	0.187	-0.146	-0.093	0.222

Appendix I showed additional comments collected from the participants. Participants captured their behavior to protect themselves from social engineering breaches in these comments. The additional comments were in synchronization with the constructs of the supported hypothesis. Here are the additional comments that supported the constructs, perceived severity (additional comment number 8), perceived vulnerability (additional comment number 11), fear (additional comment number 13), response efficacy (additional comment number 5), protection motivation (additional comment number 10), SETA program (additional comment number 3), and protection behavior (additional comment number 1).

### Summary

This chapter began with a discussion of the survey validation and Delphi study. Additionally, data screening comprised of Mahalanobis distance and Normality test. The Mahalanobis distance and Normality test were re-executed after removing five outliers. Furthermore, the chapter showed descriptive statistics related to the participants' gender, age, education demographics, and social engineering breach exposure background.

The measurement model was assessed by evaluating outer loadings, composite reliability and validity, Cronbach's alpha ( $\alpha$ ), average variance extracted (AVE), cross-loadings, and model fit. Further analysis removed the indicator's outer loadings with a value below 0.40. All the constructs had Cronbach's Alpha ( $\alpha$ ) greater than 0.70, meeting construct reliability criteria. All average variance extracted (AVE) values were greater than 0.50, meeting convergent validity criteria. All three criteria, including cross-loadings, the Fornell-Larcker criterion, and the Heterotrait-Monotrait Ratio (HTMT), were utilized to validate discriminant validity. Lastly, the SRMR value was less than 0.08, confirming the model fit and concluding measurement mode evaluation.

The structural model was assessed by evaluating collinearity statistics (VIF), coefficient of determination ( $R^2$ ), path coefficients ( $\beta$ ), effect size ( $f^2$ ), predictive relevance ( $Q^2$ ), Importance-Performance Map Analysis (IPMA), and PLS predict ( $Q^2$  Predict). The VIF values were lower than five, confirming collinearity. In addition, the path coefficients and total effects were analyzed and resulted in supporting eight out of twelve hypotheses. The estimated model in this research study could explain 42.8% of the variance in fear, 64.9 % of the variance in protection motivation, and 57.7% of the variance in protection behavior. The  $Q^2$  values were above zero, confirming the predictive relevance. IPMA provided the evaluation on two dimensions, including importance and performance. PLS predict assessment showed acceptable values concluding structural model assessment. The next chapter comprises a comprehensive discussion, limitations, implications, recommendations, and conclusion of the research findings.

## **Chapter 5**

### **Discussion, Limitations, Implications, Recommendations, and Conclusion**

#### **Introduction**

This research study examines the influences on users' protection behavior to prevent social engineering breaches and encompasses the development and empirical evaluation of a research model based on PMT full nomology, SETA program, and security policies. The previous chapter comprehended the quantitative research results from this research study. This chapter offers a thorough discussion of the results learned in the last chapter.

This discussion includes influences on fear, influences on protection motivation, influences on protection behavior, support for the research model, and support for the research question. The chapter then presents limitations, implications, contributions to theory, contributions to practice, and recommendations. Finally, the last part of the chapter provides conclusions and a thesis summary.

#### **Discussion**

Social engineering is one of the most significant threats organizations face today. Social engineering involves persuading users to provide sensitive information to perform unauthorized actions to achieve illegitimate financial advances (Dodge et al., 2007). Despite several research studies completed in recent times in the social engineering area, there is a scarcity of theory-grounded empirical studies to prevent social engineering breaches. An empirical investigation of protection motivation and protection behavior to prevent social engineering breaches utilizing PMT full nomology, SETA program, and security policies did not exist; henceforth, this research model originated.

### *Influences on Fear*

A robust and flexible theory, protection motivation theory, was primarily designed to explicate fear appeals (Rogers, 1975). Prior research leveraging PMT did not include the critical parameter of fear (Alashoor et al., 2017; Chen & Zahedi, 2016; Youn, 2005). Fear is an adverse sentiment on behalf of a response that ascends from diagnosing a threat (Boss et al., 2015). Fear takes different forms, including scare, stimulation, distress, and alarm. Similarly, fear is emotional tension, anxiety, nervousness, shock, provocation, apprehension, or uneasiness users feel when they are scared of future security threats that may cause them damage.

This research study derived that perceived severity positively impacted fear. Fear concerning perceived severity played an impactful part in PMT. The more fear users feel about a threat, the more severe the user believes the danger is (Milne et al., 2000). Prior research derived a similar positive relationship between perceived severity and fear (Arachchilage & Love, 2013; Boss et al., 2015; Liang & Xue, 2010). Therefore, the perceived severity envisaging fear matches the results of this research study (Boss et al., 2015).

This research study derived that perceived vulnerability positively impacted fear (Boss et al., 2015; Chen & Zahedi, 2016). Fear concerning perceived vulnerability played a crucial role in PMT. Specifically, the more fear users feel of a threat; the more vulnerable users believe themselves to be (Milne et al., 2000). Perceived vulnerability foreseeing fear matches this research study's outcomes (Arachchilage & Love, 2013; Boss et al., 2015). The influence of perceived severity on fear was more significant than that of perceived vulnerability in this research study, consistent with Arachchilage and Love (2013).

### *Influences on Protection Motivation*

This research study found that perceived severity positively impacted user's protection motivation, unswerving with the empirical testing conducted in the prior literature (Chen & Zahedi, 2016). PMT's previous research found perceived severity to have a non-significant influence (Yang et al., 2017). In addition, this research study exhibited that perceived severity is vital for users' protection motivation to follow suggested security measures to avert social engineering breaches. Subsequently, this is reinforced by previous research in perceived severity applying PMT. Dang-Pham and Pittayachawan (2015) posited the positive impact of perceived severity on protection motivation in research conducted in Australia. Similarly, Johnston et al. (2015) hypothesized a positive effect of perceived severity on protection motivation in a study in Finland.

This research study found a positive impact of perceived vulnerability on user's protection motivation similar to former PMT evaluations (Alashoor et al., 2017; Yang et al., 2017). This research study showed that perceived vulnerability is a vital influence on users' protection motivation to follow recommended security measures to prevent social engineering breaches. Earlier research in perceived vulnerability utilizing PMT supported this finding. Lee (2011) deliberated intention to adopt an antiplagiarism system and derived positive impact of perceived vulnerability employing PMT corroborating this research study. Similarly, Mohamed and Ahmad (2012) showed a positive influence of perceived vulnerability utilizing PMT by studying social networking sites in Malaysia.

This research study derived a positive impact of fear on users' protection behavior analogous to prior PMT research (Zhang & McDowell, 2009). While most of the extant research did not embrace the crucial aspect of fear while leveraging PMT (Lee et al., 2008),

this research study incorporated fear appeal, considering it vital for PMT. This research study verified that the higher the fear, the more likely the user will be exhibiting protection motivation to follow recommended information security measures, thus substantiating the critical factor of fear appeal (Milne et al., 2000). Furthermore, Arachchilage and Love (2013) also posited a positive relationship between fear and protection motivation, corroborating this research study's discoveries.

This research study did not find a negative impact of maladaptive rewards on protection motivation, which corresponds to previous research (Dang-Pham & Pittayachawan, 2015). Preceding research leveraging PMT did not comprise the impact of maladaptive rewards in their research model (Alashoor et al., 2017; Lee et al., 2008; Yang et al., 2017). Marett et al. (2011) did not find any significant relationship between extrinsic rewards and the revelation of sensitive information. Dang-Pham and Pittayachawan (2015) conducted an empirical investigation incorporating PMT in Australia and derived a non-significant influence of maladaptive rewards.

This research study highlighted a positive impact of response efficacy on protection motivation corresponding with previous research (Ifinedo, 2012; Lwin et al., 2012; Yang et al., 2017). However, some incidences of preceding research leveraging PMT did not comprise the impact of response efficacy in their research model (Alashoor et al., 2017). It was evident from this research study that response efficacy played an impactful role in protection motivation matching with former research (Chen & Zahedi, 2016; Crossler et al., 2014; Meso et al., 2013). Boehmer et al. (2015) and Lee (2011) posited a positive impact of response efficacy confirming user's belief in the efficiency of the suggested security measures impacts protection motivation. Davis, Bagozzi, and Warshaw (1989) asserted that

response efficacy positively impacted protection motivation, verifying findings from this research study.

It is apparent from this research study that the positive relationship between self-efficacy and protection motivation did not confirm, similar to preceding research (Alashoor et al., 2017). There was evidence in the prior research of a positive relationship between self-efficacy and protection motivation (Yang et al., 2017). Preceding research leveraging PMT did not comprise the impact of self-efficacy in their research model (Youn, 2005). The discovery of this research study conformed to the prior literature (Youn, 2009).

One of the thought-provoking findings of this research study was the dynamics between self-efficacy and response efficacy. Prior research studies frequently showed self-efficacy as a more critical factor than response efficacy in the information security arena (Crossler et al., 2013). Conversely, this research study highlighted that response efficacy is more vital than self-efficacy. This research study also emphasized that response efficacy has the highest impact on protection motivation than any other construct in the research model. Response efficacy represents a user's views of the effectiveness of recommended information security measures to prevent social engineering breaches. In comparison, self-efficacy represents a user's confidence in their capacity to execute recommended information security measures.

Users must understand how recommended security measures secure an organization and how information security investments lead to a return. Even though some users understand the dangers and potential penalties of not following recommended information security measures, they are still not keen on following them. Frequently, users do not believe that their organization has comprehensive measures and controls to ensure the confidentiality, integrity, and availability of organizational information. Henceforth, this research study



provides critical evidence helping organizations to improve protection behavior by carefully crafting a strategy to enhance users' response efficacy.

This research study did not find a negative relationship between response cost and protection motivation, similar to preceding research (Hanus & Wu, 2016; Ng et al., 2009). Preceding research leveraging PMT did not encompass the influence of response cost (Alashoor et al., 2017; Lee et al., 2008; Youn, 2005). Ifinedo (2012) conducted a study in Canada and found a non-significant impact of response cost utilizing PMT. Crossler et al. (2014) instituted a non-significant impact of response cost employing PMT. Thus, response efficacy was the most critical impact on the coping appraisal for the protection motivation to prevent social engineering breaches found by this research study.

#### *Influences on Protection Behavior*

This research study found a positive impact of protection motivation on protection behavior to prevent social engineering breaches like erstwhile PMT research (Posey et al., 2015). The protection motivation to protection behavior hypothesis had the highest impact of any other hypothesis in this research model. It had emerged as the relationship with the highest path coefficient and *t* statistics value. Moreover, this indicates that users' motivation to perform protection behaviors against social engineering threats is strongly associated with their actual performance of these behaviors. Conclusions from previous research, such as Johnston and Warkentin (2010) and Pahnla et al. (2007), contended that the protection motivation positively influenced the protection behavior to prevent the information security breach corroborating the discoveries from this research study.

This research study led to a positive relationship between the SETA program and protection motivation like former research (Posey et al., 2015). One of the best defenses

against social engineering threats is layers of well-designed multi-dimensional SETA programs, helping users perceive and retort the attacks in the most appropriate way. The comprehensive SETA program defends digital assets for the endurance and success of the organization and aims that every user turns out to be a portion of security solutions and not security problems (Chen, Ramamurthy, & Wen, 2015; Heartfield & Loukas, 2015).

Subsequently, the SETA program provides a security-based foundation for users and positively influences users' protection behavior to prevent social engineering breaches (Posey et al., 2015).

This research study did not find a positive relationship between security policies and protection motivation. Security policy in an organization outlines how to protect organizational digital assets from information security threats, including social engineering breaches (Moody et al., 2018). Chen et al. (2015) asserted that the SETA program positively impacts an organization's security policies; therefore, a better SETA program improves security policies. The SETA program and security policies improve users' protection behavior to follow information security measures to prevent social engineering breaches (Chen et al., 2015).

#### *Support for the Research Model*

The research model utilized PLS-SEM because the investigation included verifying a theoretical framework from a prediction perspective. The  $t$  statistics value greater than equal to 1.96 with the two-tailed test at a 5% significance level indicates support of a hypothesis (Hair et al., 2017). Perceived severity, perceived vulnerability, and fear comprised threat appraisal and positively impacted the user's protection motivation to follow recommended security measures to prevent social engineering breaches.

Response efficacy covered coping appraisal and positively impacted protection motivation. Response efficacy had the highest impact on protection motivation than any other individual constructs. At the same time, hypotheses of maladaptive rewards, self-efficacy, response cost, and security policies remained non-supported. The SETA program had a positive impact on the protection behavior. Moreover, protection motivation positively impacted the protection behavior with the highest  $t$  statistics value in the entire research model.

#### *Support for the Research Question*

This research study addressed the following main research question:

*RQ: What are the factors influencing the users' information security protection behavior towards social engineering breaches?*

The discoveries and conclusions from this research study demonstrated factors influencing users' protection behavior to prevent social engineering breaches. Overall, this research study assessed impacts of threat appraisal (perceived severity, perceived vulnerability, fear, and maladaptive rewards), coping appraisal (response efficacy, self-efficacy, and response cost), protection motivation, SETA program, and security policies on users' protection behavior to prevent social engineering breaches.

#### **Limitations**

There are some limitations related to this research study, like most academic research studies. First and foremost, participants of this research study were limited to those who had access to the computer or mobile, considering this research study involved an online survey. Assuming that this research study involved social engineering and information security, participants with access to the computer or mobile device made rational logic. Secondly, the sample size of this research study could have been larger. Future research on this topic

should utilize a larger sample size considering the number of constructs utilized in this research study.

Finally, the participants who responded to this research study were limited to the U.S.A. Thus, the conclusions of this study may apply to one country only and may not be illustrative of all the countries and regions. The participants from one country may have also been less culturally diverse than the sample collected from multiple countries.

### **Implications**

The results of this research study have provided significant insinuations for theory and practice.

#### *Contributions to Theory*

This research study makes a number of academic contributions in the realm of social engineering research. First and foremost, it provided valuable evidence of using PMT to understand the intricacies of social engineering. Social engineering attacks revolve around how users think, decide, behave, and respond. Once a social engineer has a comprehensive understanding of users' behavior, it is easy to betray them. PMT provided a suitable framework for the users' protection motivation and protection behavior. There was a dearth of PMT theory-backed empirical investigation in the social engineering area. Henceforth, this research study enlarged PMT usage to a comparatively unutilized sphere of social engineering in the information security area.

Secondly, this research study examined the full nomology of the PMT model and not just the partial PMT model for the social engineering area. Much prior research applying PMT to information security did not incorporate the full nomology of the PMT model and did not include the critical component of fear appeal (Dang-Pham & Pittayachawan, 2015). For this

reason, this research study exhibited that PMT full nomology utilization, including fear appeal, is necessary (Boss et al., 2015).

Thirdly, this research study incorporated the protection behavior in addition to protection motivation and thus posited that preventing social engineering breach goes beyond protection motivation, demonstrating the relevance of protection behavior. Previous research focused on users' protection motivation in various areas, including viruses, threats, unauthorized access, disruptions, attacks, malware, and spyware (Dinev & Hu, 2007; Mahmood, Siponen, Straub, Rao, & Raghu, 2010). However, prior research recommended that researching actual behavior is more vital than motivation (Anderson & Agarwal, 2010; Crossler et al., 2013). Incorporating protection behavior and motivation gave the complete picture of the high priority issue of social engineering breaches (Boss et al., 2015).

Finally, this research study combined the full nomology of the PMT model with the SETA program and security policies for the social engineering area. Social engineering fortification begins with the SETA program and security policies so that collective awareness progresses. The SETA program trains users to make clever security decisions and helps users exhibit specific behavior resulting in a diminution in social engineering breaches. By combining the SETA program and security policies into the traditional PMT model, this research study undertook significant aspects to bridge the gap of leveraging PMT in social engineering research and overall information security research.

#### *Contributions to Practice*

Social engineering breaches have become so prevalent that organizations are in dire need of assistance to prevent an implausible amount of monetary loss. Social engineering has shown itself to be an efficacious mode for a criminal to get the keys of the kingdom. Social

engineering is dangerous because it relies on user error and not technology error, as it is trickier to predict user error. Henceforth, users should be cognizant of social engineering, be accustomed to frequently used maneuvers, and know how to respond to them appropriately. This research study may help organizations build mechanisms that foster protection motivation to prevent compliance with information systems security policies and processes. A better understanding of users' information security protection behavior to prevent social engineering breaches helps organizations formulate broader and better training programs, policies, and processes.

Organizations' goal is to have users understand who and what to trust. Likewise, organizations must be on top of having a comprehensive SETA program and ensuring that the SETA program regularly encompasses emerging trends. Therefore, this research study has provided in-depth information about increasing users' protection behavior to prevent social engineering breaches. The findings of this research study may help information security leaders reinforce and upsurge organizations' resilience and prevent violations and break-ins.

### **Recommendations**

All participants of this research study were from the U.S.A. This research study may produce variations in the results in other countries and regions of the world. Hence, the recommendations included conducting a replica of this research study in other areas of the world. A future research study should retest the questionnaire with samples from other countries to identify alterations across countries. Forthcoming studies should deliberate collecting data based on culture, as there is a possibility of finding a new outlook based on

such criteria. Additionally, future research on this topic should employ a larger sample size because of the number of constructs used in this research study.

### **Conclusion and Thesis Summary**

Contemporary information security research has begun to focus more on human behavior in preventing security breaches than the traditional approach of technological angle. Social engineering entails manipulating users into disclosing confidential information or conducting actions to achieve illegal financial gains. Social engineering breaches have become so widespread that organizations and governments worldwide are facing severe unprecedented financial loss. The social engineering area has been deficient in theory-grounded empirical research.

This research study used the full nomology of PMT (Rogers, 1975) and social engineering literature to empirically inspect how threat appraisal, coping appraisal, SETA program, and security policies impact user's protection motivation and protection behavior to prevent social engineering breaches. Threat appraisal and coping appraisal both impact protection motivation. The threat appraisal evaluated the severity of the threat and scrutinized how severe the danger is. The coping appraisal demonstrated how users replied to the threat.

The research model was established based on the original research question and in-depth literature review. Data collection included web-based survey completion by one hundred twenty-nine participants from the U.S.A. Successful evaluation of the research model using PLS-SEM preceded with a practical Delphi study and data screening.

Protection motivation theory is a theory that initially elucidated fear appeals (Rogers, 1975). All three hypotheses related to fear were supported, which is a significant contribution considering a lesser-explored fear appeal in prior research utilizing PMT. Furthermore, the

research study verified positive impacts of perceived severity, perceived vulnerability, fear, response efficacy, protection motivation, and the SETA program.

The conclusions of this research study have provided significant insinuations for research and practice. It demonstrated that PMT is a valued model for predicting users' protection behavior to prevent social engineering breaches. At the same time, one of the essential factors in information security research is to combine multiple angles to elucidate emerging phenomena and solve critical problems. This research study benefits organizations in transforming security posture from reactive to proactive by improving users' behaviors. Overall, this research study has shown significant implications to the theory and practice in social engineering. Finally, this research study has propositioned insight into social engineering and information security while finding groundwork to provide future research.



## **Appendices**

## Appendix A

### *Summary of Measurement Items*

Construct	Description	Reference
<b>Perceived Severity</b>		
PS01	If I were to experience information security compromise due to social engineering breach, I would suffer much pain.	Boss et al., 2015
PS02	If I were to experience information security compromise due to social engineering breach, it would be severe.	Johnston & Warkentin, 2010
PS03	If I were to experience information security compromise due to social engineering breach, it would be serious.	Johnston & Warkentin, 2010
PS04	If I were to lose data due to social engineering breach, it would be significant.	Johnston & Warkentin, 2010
PS05	Having my data destroyed by social engineering breach would be a serious problem for me.	Yoon et al., 2012
<b>Perceived Vulnerability</b>		
PV01	I am likely to experience information security compromise due to social engineering breaches.	Boss et al., 2015
PV02	My chances of losing sensitive data in the future are high due to social engineering breaches.	Boss et al., 2015
PV03	There is a chance that my personal information has been disclosed due to social engineering breach.	Yoon et al., 2012
PV04	My data is likely to be undermined by malicious software such as viruses during social engineering breaches.	Yoon et al., 2012

---

PV05	My system is likely to be damaged by a social engineering breach.	Workman et al., 2008
<b>Fear</b>		
FE01	I am worried about the experience of information security compromise due to social engineering breaches.	Boss et al., 2015
FE02	I am frightened about the experience of information security compromise due to social engineering breaches.	Boss et al., 2015
FE03	I am anxious about the experience of information security compromise due to social engineering breaches.	Boss et al., 2015
FE04	I am scared about the experience of information security compromise due to social engineering breaches.	Boss et al., 2015
FE05	My computer might become unusable as a result of information security compromise due to social engineering breaches.	Boss et al., 2015
<b>Maladaptive Rewards</b>		
MR01	Not complying with information security measures to prevent social engineering breaches saves me time.	Boss et al., 2015
MR02	Not complying with information security measures to prevent social engineering breaches saves me money.	Boss et al., 2015
MR03	Not complying with information security measures to prevent social engineering breaches keeps me from being confused.	Boss et al., 2015
MR04	Not complying with information security measures to prevent social engineering breaches would make it easier to use other programs on my computer.	Boss et al., 2015
MR05	Not complying with information security measures to prevent social engineering breaches would make it easier to use the functionality of my Internet browser.	Boss et al., 2015

---

---

**Response Efficacy**

RE01	Complying with information security measures is a good way to reduce the risk of social engineering breaches.	Boss et al., 2015
RE02	If I were to comply with information security measures, I would reduce my social engineering breach chances.	Boss et al., 2015
RE03	Information security measure works for protection against social engineering breach.	Johnston & Warkentin, 2010
RE04	Information security measure is effective for protection against social engineering breach.	Johnston & Warkentin, 2010
RE05	When complying with information security measures, data is more likely to be protected against social engineering breaches.	Johnston & Warkentin, 2010

**Self-efficacy**

SE01	Information security measures to prevent social engineering breaches are easy to use.	Johnston & Warkentin, 2010
SE02	Information security measures to prevent social engineering breaches are convenient to use.	Johnston & Warkentin, 2010
SE03	I am able to use Information security measures to prevent social engineering breaches without much effort.	Johnston & Warkentin, 2010
SE04	I have the necessary skills to protect myself from information security violations.	Workman et al., 2008
SE05	For me, taking information security precautions is easy.	Workman et al., 2008

---

---

**Response Cost**

RC01	The cost of complying with information security measures to prevent social engineering breaches outweighs the benefits.	Boss et al., 2015
RC02	I would be discouraged from complying with information security measures to prevent social engineering breaches because it would take too much time.	Boss et al., 2015
RC03	Taking the time to comply with information security measures to prevent social engineering breaches would cause many problems.	Boss et al., 2015
RC04	I would be discouraged from complying with information security measures to prevent social engineering breaches because I would feel silly doing so.	Boss et al., 2015
RC05	The inconvenience of implementing recommended security measures to prevent social engineering breaches outweighs the benefits.	Workman et al., 2008

**SETA Program**

ST01	My organization delivers training to help employees improve their awareness of computer and information security issues.	Al-Omari, El-Gayar, & Deokar, 2012
ST02	My organization educates employees on the appropriate use of information technology resources.	Al-Omari et al., 2012
ST03	My organization briefs employees on the consequences of modifying computerized data in an unauthorized way.	Al-Omari et al., 2012
ST04	My organization trains employees on their computer security responsibilities.	Al-Omari et al., 2012
ST05	My organization educates employees on their responsibilities for managing computer passwords.	Al-Omari et al., 2012

---

---

**Security Policies**

SP01	My organization has prescribed rules and regulations to prevent information security compromise due to social engineering breaches.	Al-Omari et al., 2012
SP02	My organization's security policies prescribe my responsibilities toward preventing information security compromise.	Al-Omari et al., 2012
SP03	My organization has a formal policy that forbids employees from modifying computerized data in an unauthorized way.	Al-Omari et al., 2012
SP04	My organization has a formal policy that forbids employees from installing their software on work computers.	Al-Omari et al., 2012
SP05	My organization has specific guidelines that describe the acceptable use of computer passwords.	Al-Omari et al., 2012

**Protection Motivation**

PM01	I intend to comply with information security measures to prevent social engineering breaches during the next three months.	Boss et al., 2015; Johnston & Warkentin, 2010
PM02	I predict I will comply with information security measures to prevent social engineering breaches during the next three months.	Johnston & Warkentin, 2010
PM03	I plan to comply with information security measures to prevent social engineering breaches during the next three months.	Johnston & Warkentin, 2010
PM04	I will take precautions against information security violations during the next three months.	Yoon et al., 2012
PM05	I will not install unreliable software on my computer during the next three months.	Yoon et al., 2012

---

---

**Protection Behavior**

PB01	I intermittently check and remove viruses and malicious software.	Yoon et al., 2012
PB02	I immediately remove suspicious e-mails without reading them.	Yoon et al., 2012
PB03	Under no circumstances would I ever share anyone my ID, password, or any other credentials.	Yoon et al., 2012
PB04	I ensure the execution of the latest tools and technologies on my devices per recommended information security measures.	Liang & Xue, 2010
PB05	I do not proceed with any activity that I suspect can cause a social engineering breach (for example, using an unsecured internet connection).	Self-developed

---

## Appendix B

*Summary of Reliability Evidence*

Construct	Reference	Reliability Evidence
Perceived Severity	Boss et al., 2015	.915
Perceived Severity	Johnston & Warkentin, 2010	.943
Perceived Severity	Yoon et al., 2012	.86
Perceived Vulnerability	Boss et al., 2015	.817
Perceived Vulnerability	Yoon et al., 2012	.83
Perceived Vulnerability	Workman et al., 2008	.854
Fear	Boss et al., 2015	.755
Maladaptive Rewards	Boss et al., 2015	.777
Response Efficacy	Boss et al., 2015	.898
Response Efficacy	Johnston & Warkentin, 2010	.897
Self-efficacy	Johnston & Warkentin, 2010	.942
Self-efficacy	Workman et al., 2008	.929
Response Cost	Boss et al., 2015	.845
Response Cost	Workman et al., 2008	.793
SETA Program	Al-Omari et al., 2012	.846
Security Policies	Al-Omari et al., 2012	.787
Protection Motivation	Boss et al., 2015	.984
Protection Motivation	Johnston & Warkentin, 2010	.954
Protection Motivation	Yoon et al., 2012	.85
Protection Behavior	Yoon et al., 2012	.77
Protection Behavior	Liang & Xue, 2010	.92



## Appendix C

*IRB Approval*MEMORANDUM

**To:** Nisha Patel

**From:** Wei Li, Ph.D.  
Center Representative, Institutional Review Board

**Date:** May 21, 2020

**Re:** IRB #: 2020-253; Title, "An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breaches"

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under 45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies). You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

**Cc:** Ling Wang, Ph.D.  
Ling Wang, Ph.D.

## Appendix D

### *Participant Email Message*

Dear Participant,

I am conducting a research study that emphasizes on users' information security protection behavior towards social engineering breaches. The results of this research study will offer researchers and practitioners a further understanding of users' information security protection behavior towards social engineering breaches.

I would appreciate your contribution and time in participating in this research study. Your participation is voluntary, and all responses will be protected. All information and data collected as part of this study will be confidential and utilized solely for the objective of this research study.


This survey is completely anonymous, and no personally identifiable information (PII) data will be collected to protect the privacy of the participants. There is no cost for participation in this survey, nor is there any payment. This survey is a one-time survey and will take 15 minutes to complete. There are no conceivable risks associated with your participation in this survey. Your participation is entirely voluntary. You may stop your participation at any time.

Thank you for your participation in this research opportunity.

Nisha Patel, Ph.D. Candidate in Information Systems  
College of Computing and Engineering, Nova Southeastern University  
Email: Np826@mynsu.nova.edu

## Appendix E

### *Participant Survey*

 <p><b>NSU</b> Florida NOVA SOUTHEASTERN UNIVERSITY</p>	<p><b>INSTITUTIONAL REVIEW BOARD</b> 3301 College Avenue Fort Lauderdale, Florida 33314-7796 PHONE: (954) 262-5369</p>
<p><b>Participant Letter for Anonymous Surveys</b> <i>An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breaches</i></p>	
<p><b><u>Who is doing this research study?</u></b></p>	
<p>This person doing this study is Nisha Patel with the College of Computing and Engineering. They will be helped by Dr. Ling Wang as the Advisor and Dissertation Chair.</p>	
<p><b><u>Why are you asking me to be in this research study?</u></b></p>	
<p>You are being asked to take part in this research study because you are an adult over the age of 18 and have experience with issues relevant to social engineering and security breaches.</p>	
<p><b><u>Why is this research being done?</u></b></p>	
<p>The purpose of this study is to find out factors that contribute to users' information security protection behavior towards social engineering breaches.</p>	
<p><b><u>What will I be doing if I agree to be in this research study?</u></b></p>	
<p>You will be taking a one-time, anonymous survey. The survey will take approximately 15 minutes to complete.</p>	
<p><b><u>Are there possible risks and discomforts to me?</u></b></p>	
<p>This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.</p>	
<p><b><u>What happens if I do not want to be in this research study?</u></b></p>	
<p>You can decide not to participate in this research, and it will not be held against you. You can exit the survey at any time.</p>	
<p><b><u>Will it cost me anything? Will I get paid for being in the study?</u></b></p>	
<p>There is no cost for participation in this study. Participation is voluntary, and no payment will be provided.</p>	
<p><b><u>How will you keep my information private?</u></b></p>	
<p>Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Personally identifiable information (PII) data will not be collected to protect the privacy of the participants. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if</p>	
<p>Page 1 of 2</p>	



**INSTITUTIONAL REVIEW BOARD**  
3301 College Avenue  
Fort Lauderdale, Florida 33314-7796  
PHONE: (954) 262-5369

applicable). All confidential data will be kept securely in secured Google Drive. All data will be kept for 36 months from the end of the study and destroyed after that time by permanently purging the data.

**Who can I talk to about the study?**

If you have questions, you can contact Nisha Patel at 862 703 6311 and or Dr. Ling Wang at 954 262 2020.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll-free at 1-866-499-0790 or email at [IRB@nova.edu](mailto:IRB@nova.edu).

**Do you understand, and do you want to be in the study?**

If you have read the above information and voluntarily wish to participate in this research study, please complete this survey.

### Demographic information

1. What is your gender?
  - 1. Male
  - 2. Female
  - 3. Other
  
2. What is your age range?
  - 1. 18-24
  - 2. 25-34
  - 3. 35-44
  - 4. 45-54
  - 5. 55-64
  - 6. Over 65 Years
  
3. What is your highest education achieved?
  - 1. Some School, No Degree
  - 2. High School Graduate
  - 3. Some College, No Degree
  - 4. Associate's Degree
  - 5. Bachelor's Degree
  - 6. Master's Degree
  - 7. Doctoral Degree
  
4. What are your exposures to social engineering breaches?
  - 1. None
  - 2. Some
  - 3. Extensive

### Definitions

**Social Engineering:** Social engineering is the initiative of tricking you into revealing information or taking action.

**Social Engineering Breach:** An event that exposes your confidential data to unauthorized people using social engineering



























Please provide information regarding what behavior you exhibit to protect from social engineering breaches?

Thank you for your time!

Submit

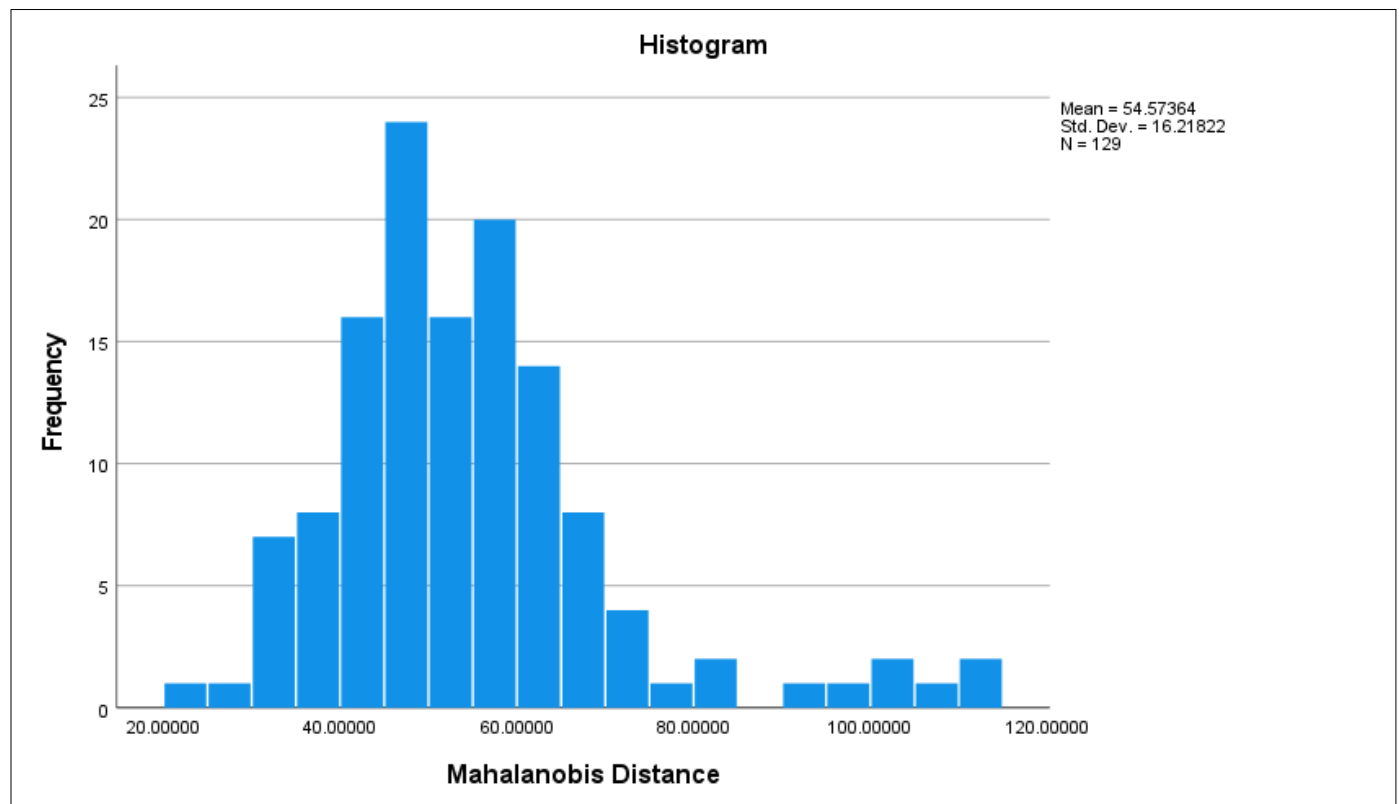
## Appendix F

### *Mahalanobis Distance and Stem & Leaf Plot*

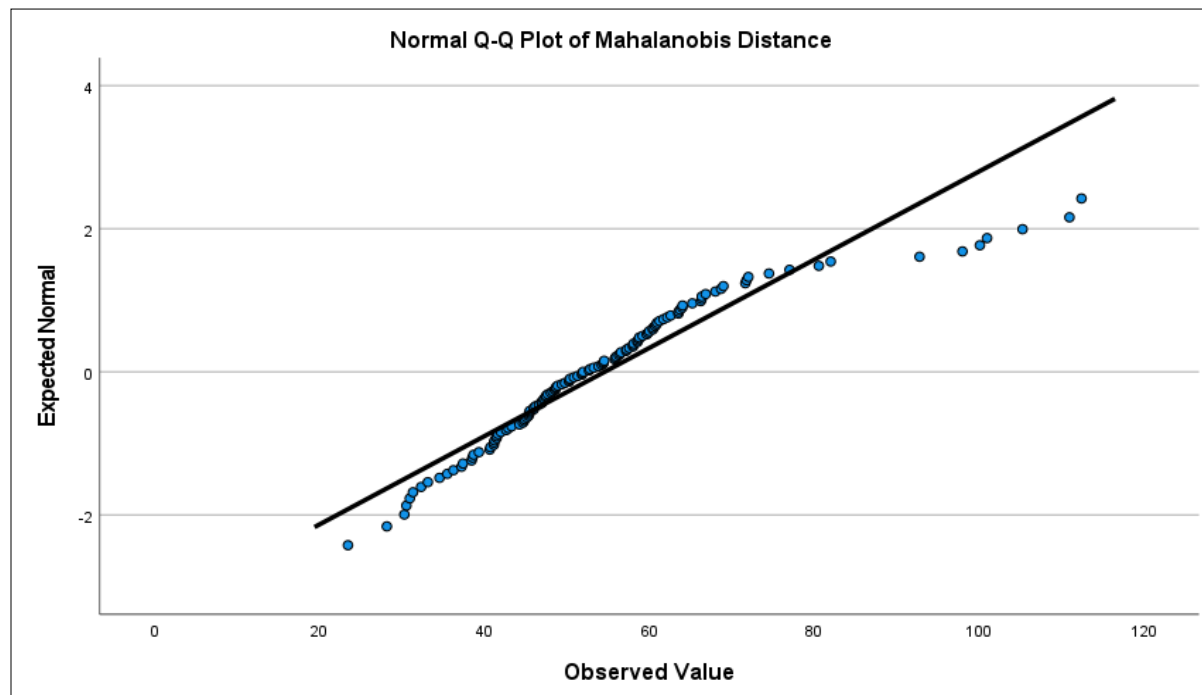
<b>Descriptives</b>			Statistic	Std. Error
Mahalanobis Distance	Mean		54.5736434	1.42793504
	95% Confidence Interval for Mean	Lower Bound	51.7482300	
		Upper Bound	57.3990569	
	5% Trimmed Mean		53.2411465	
	Median		51.9612901	
	Variance		263.031	
	Std. Deviation		16.21822444	
	Minimum		23.44277	
	Maximum		112.42643	
	Range		88.98366	
	Interquartile Range		16.04851	
	Skewness		1.340	0.213
	Kurtosis		2.724	0.423

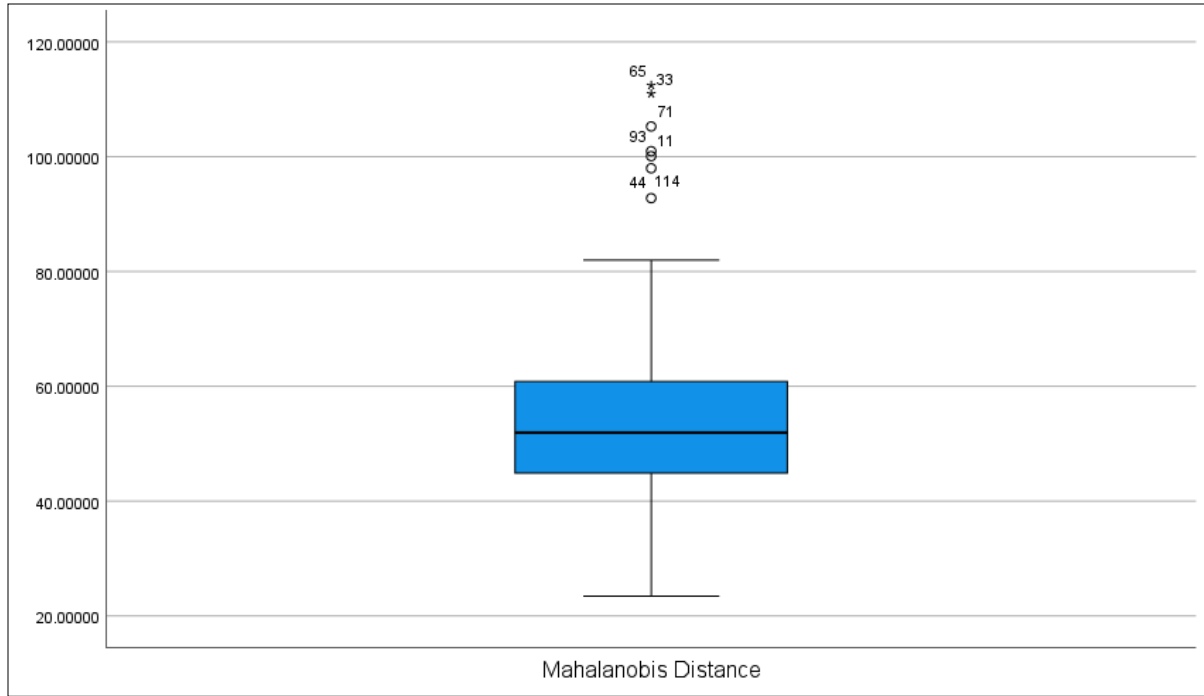
<b>Extreme Values</b>				
		Case Number		Value
Mahalanobis Distance	Highest	1	65	112.42643
		2	33	110.96614
		3	71	105.27385
		4	93	100.96868
		5	11	100.10160
	Lowest	1	48	23.44277
		2	9	28.15799
		3	101	30.28290
		4	72	30.52780
		5	29	30.94282

Tests of Normality						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	0.109	129	0.001	0.903	129	0.000
a. Lilliefors Significance Correction						



Mahalanobis Distance Stem-and-Leaf Plot	
Frequency	Stem & Leaf
1.00	2 . 3
1.00	2 . 8
7.00	3 . 0001234
8.00	3 . 56778889
16.00	4 . 0011111122234444
24.00	4 . 555555566667777788888899
16.00	5 . 0000111122334444
20.00	5 . 55566677788888889999
14.00	6 . 000001122333334
8.00	6 . 56666888
4.00	7 . 1124
1.00	7 . 7
2.00	8 . 02
7.00	Extremes (>=93)
Stem width:	10.00000
Each leaf:	1 case(s)





## Appendix G

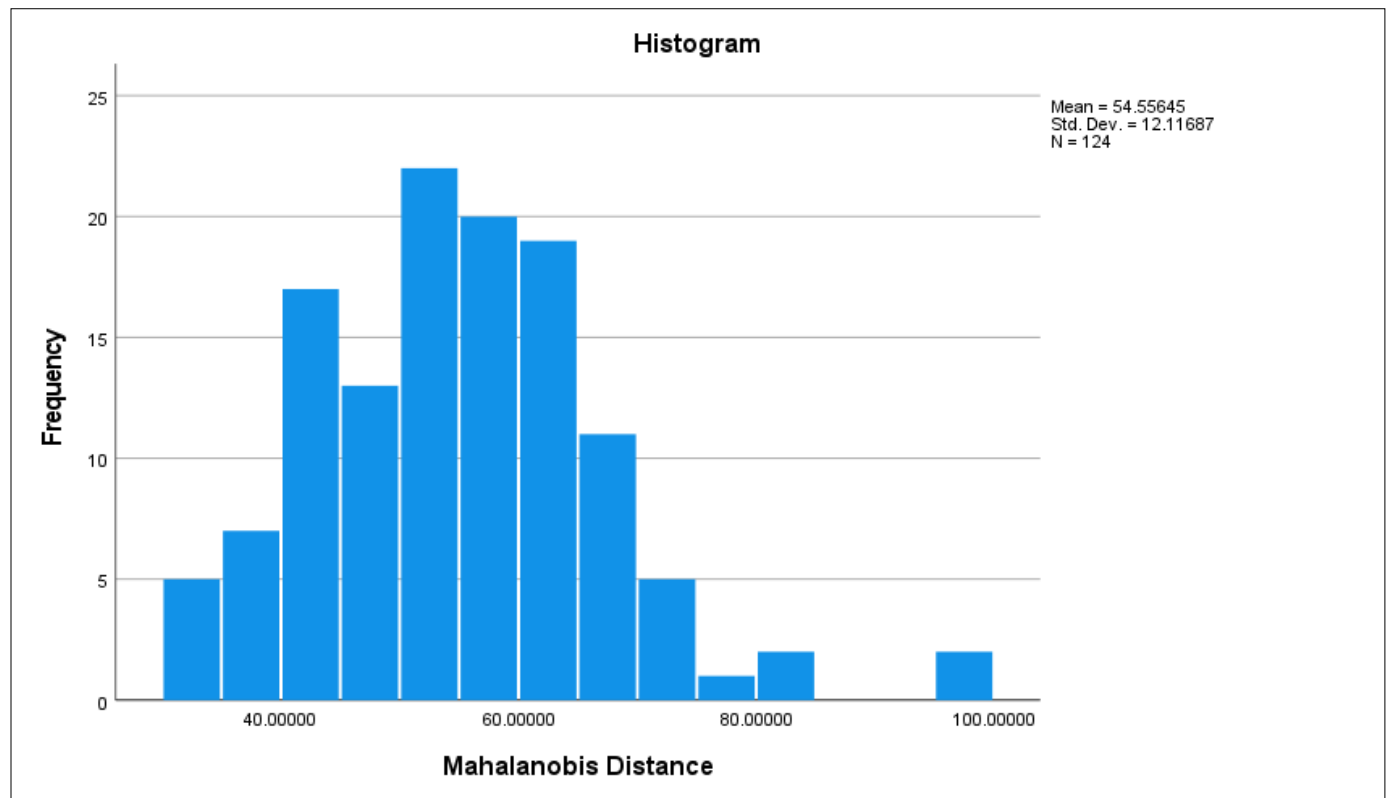
*Return of Mahalanobis Distance and Stem & Leaf Plot after removal of 5 extreme values*

<b>Descriptives</b>			Statistic	Std. Error
Mahalanobis Distance	Mean		54.5564516	1.08812698
	95% Confidence Interval for Mean	Lower Bound	52.4025710	
		Upper Bound	56.7103323	
	5% Trimmed Mean		54.1137729	
	Median		53.8557106	
	Variance		146.819	
	Std. Deviation		12.11686929	
	Minimum		30.64232	
	Maximum		99.40180	
	Range		68.75949	
	Interquartile Range		15.97395	
	Skewness		0.645	0.217
	Kurtosis		1.453	0.431

<b>Extreme Values</b>				
		Case Number		Value
Mahalanobis Distance	Highest	1	42	99.40180
		2	109	96.66706
		3	112	80.92948
		4	67	80.09708
		5	84	75.32278
	Lowest	1	96	30.64232
		2	9	30.67283
		3	68	33.60169
		4	28	33.64770
		5	46	33.89013

Tests of Normality						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mahalanobis Distance	0.052	124	.200*	0.968	124	0.005

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

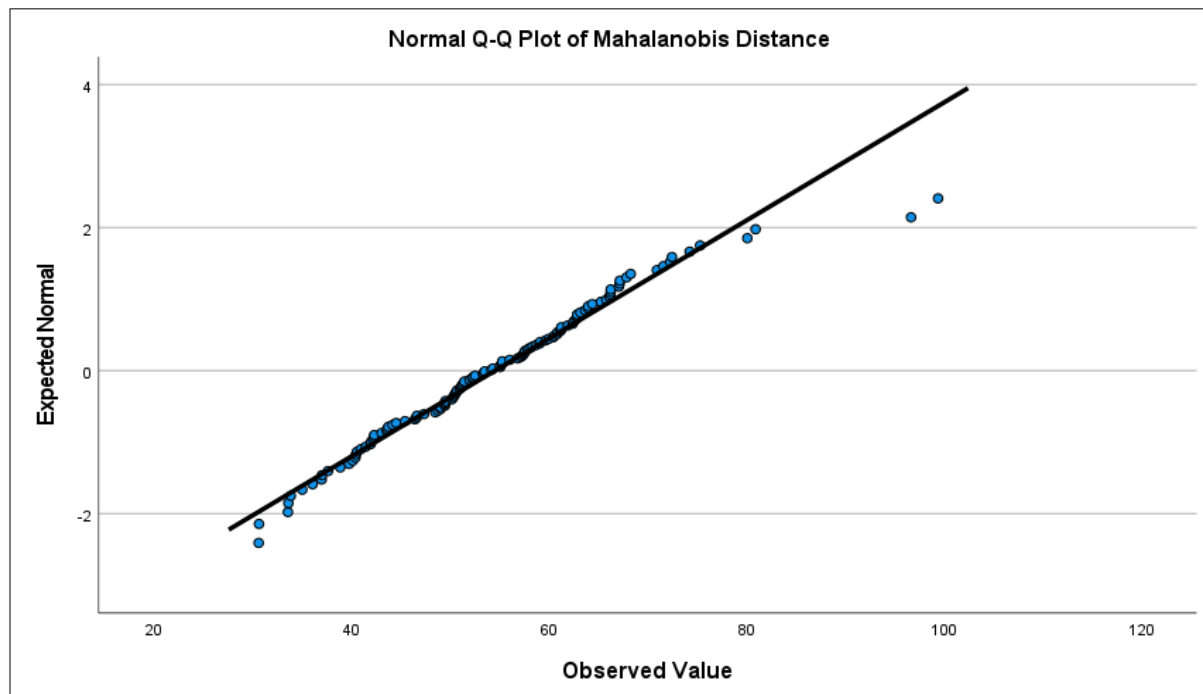


### Mahalanobis Distance Stem-and-Leaf Plot

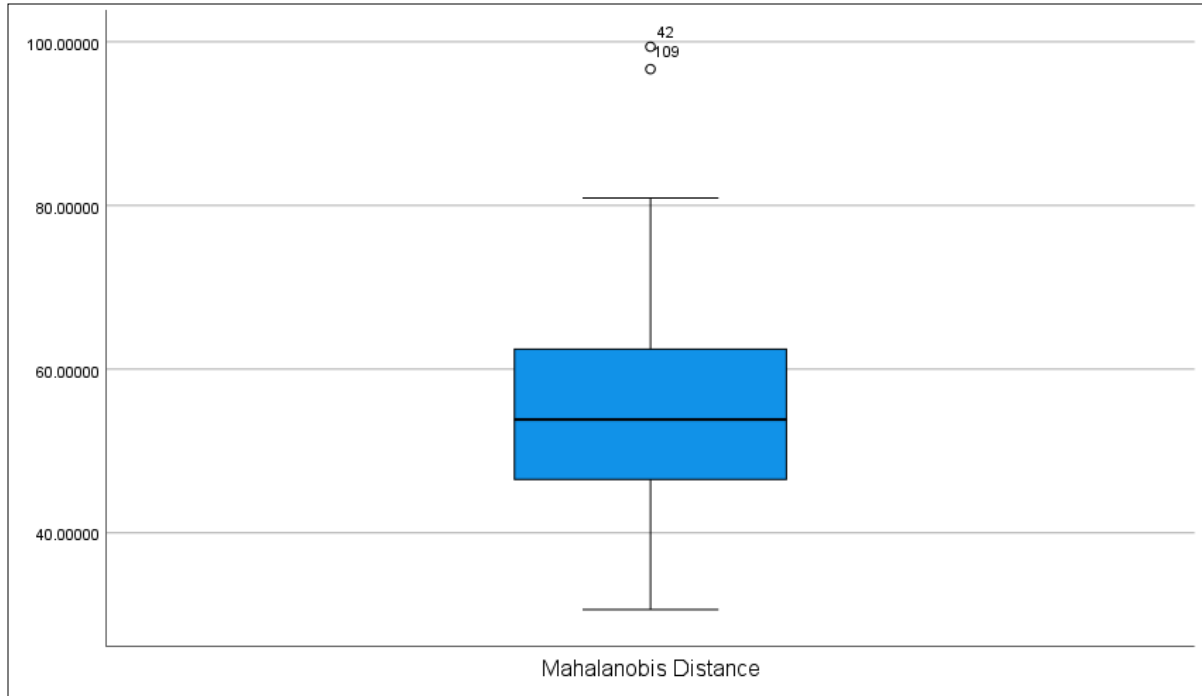
Frequency	Stem & Leaf
5.00	3 . 00333
7.00	3 . 5677789
17.00	4 . 00000112222333344
13.00	4 . 5666788999999
22.00	5 . 0000000111111122233344
20.00	5 . 55555667777778889999
19.00	6 . 0000111122222233334
11.00	6 . 55666677778
5.00	7 . 01224
1.00	7 . 5
2.00	8 . 00
2.00	Extremes (>=97)

Stem width: 10.00000

Each leaf: 1 case(s)





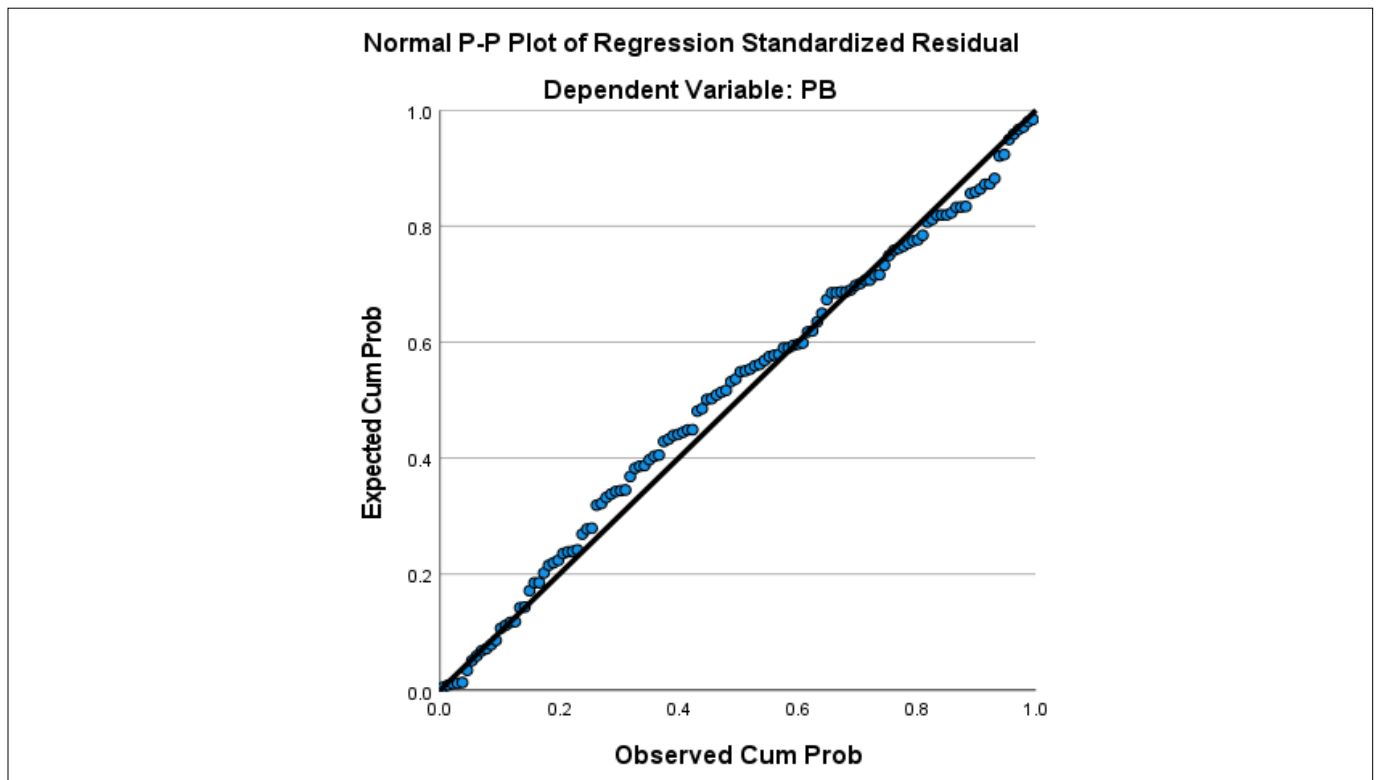
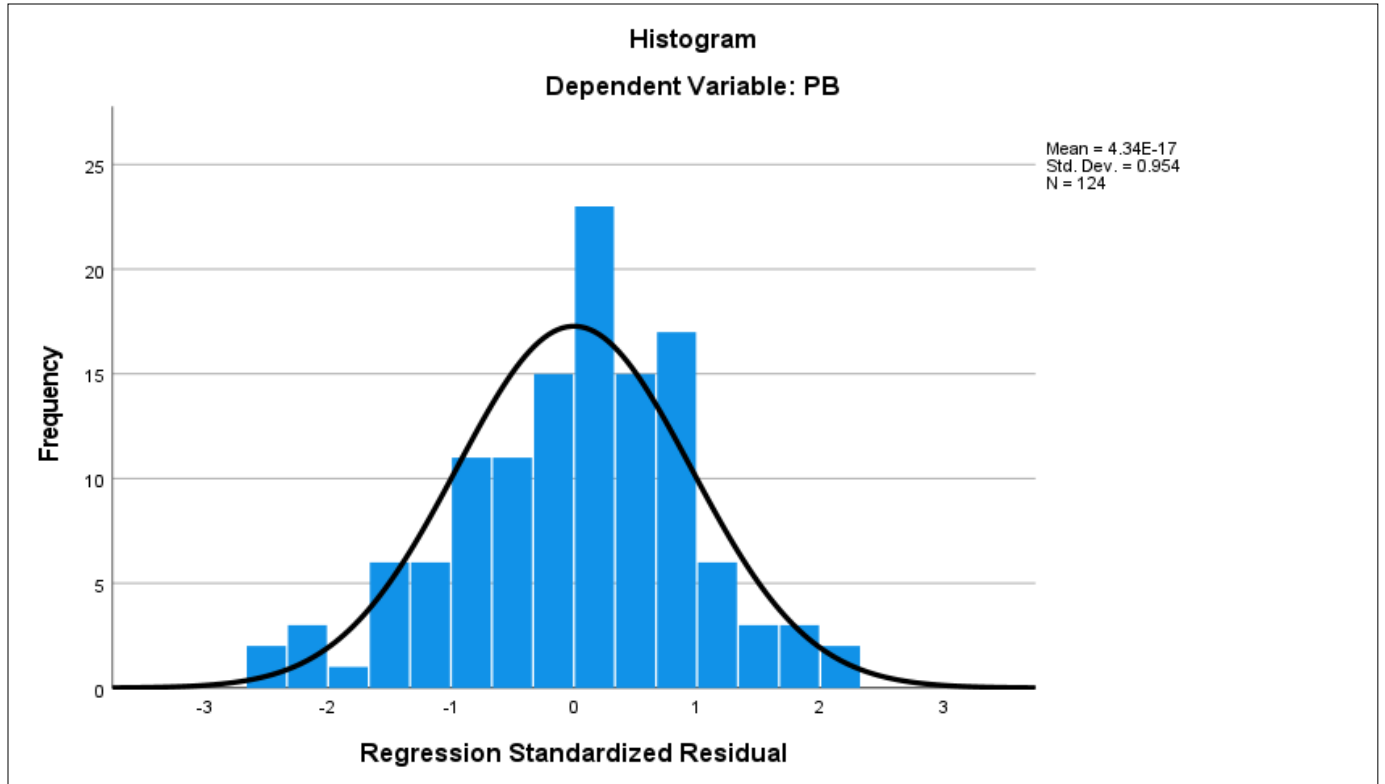


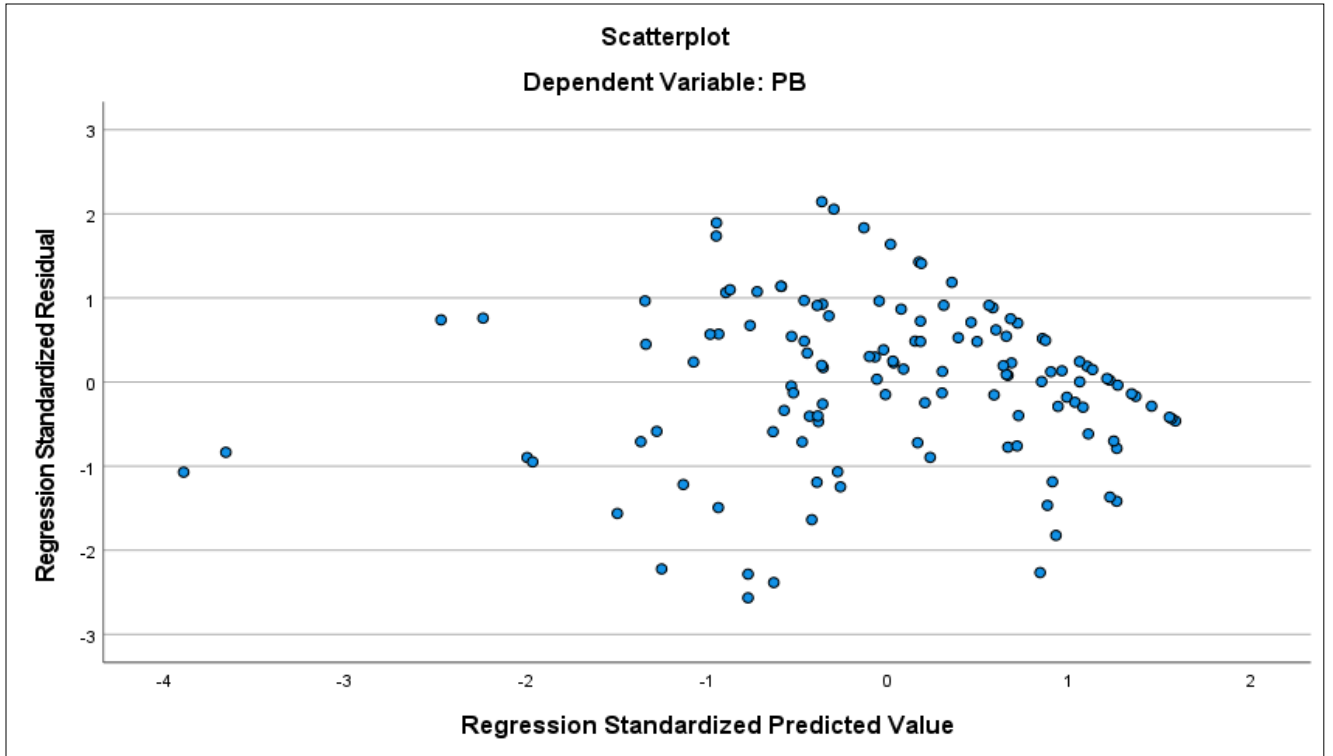
## Appendix H

### *Normality and Scatter Plot*

Model Summary <sup>b</sup>				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.814 <sup>a</sup>	0.662	0.629	0.611722
a. Predictors: (Constant), ST, RC, Case ID, SP, SE, PS, PV, MR, FE, RE, PM				
b. Dependent Variable: PB				

ANOVA <sup>a</sup>						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.064	11	7.460	19.937	.000 <sup>b</sup>
	Residual	41.911	112	0.374		
	Total	123.975	123			
a. Dependent Variable: PB						
b. Predictors: (Constant), ST, RC, Case ID, SP, SE, PS, PV, MR, FE, RE, PM						





## Appendix I

### *Additional Comments*

Comments number	Comments Description
1	I am always watchful about my passwords. A weak or lost password is one of the biggest reasons for a security breach. I have seen people sharing the same password for multiple systems; or sharing the same password for their work accounts and personal accounts. Some people use a file on their computer to store all the passwords, which is a problem.
2	I wish my organization had a robust training program to increase awareness among employees.
3	My company runs phishing breach drills. Phishing is one of the most frequent types of social engineering. Phishing simulation tracks users who are clicking on the links, users who do nothing, and intelligent enough to report to the security group. It benefits us in testing how well employees are following security procedures. The employees who fail to respond as per the expectations are trained further.
4	I try to keep myself up-to-date with the emerging trends. Awareness is the key here. The best way to combat any information security crimes is for companies to educate their employees to recognize social engineering tricks and techniques successfully. The content publication and education strategy should consider different approaches as different people consume information in different ways.
5	I make sure that I have antivirus running on all my personal devices. Good antivirus software should be able to flag malicious messages and suspicious websites. It not only just protects from viruses but also spam and ads. It provides protection from removable devices like USBs.
6	We all click on links that promise to give us something for free and look too good to be true. Reputed organizations generally do not contact people directly to lure them.
7	My company is now learning to focus on giving employees the knowledge and skills to spot security attacks. The biggest problem for an organization's data defense is its people. Many organizations do not realize this.

- 
- 8 I am a big proponent of cultivating a cyber-secure mindset. Social engineering is about finding out what makes people act without thinking. Social engineering causes 22% of all data breaches. Do not let employees fall victim to the attackers.
- 9 I feel that everyone should be interested and engaged in building security awareness in a company. It is about building a cyber-aware culture. Just one incident is enough for an attacker to compromise a company.
- 10 I am cautious about these things: 1) How I use email 2) What links I click on 3) What websites I browse. 4) What Internet I use other than my home Internet. 5) Do not share confidential information. 6) Destroy important papers before disposing of them. 7) What files I download.
- No one is immune from security breaches, and hackers are moving at light speed. Criminals' sophistication level has increased, and they are using artificial intelligence and machine learning to build patterns and improve their tactics. Everything is a target, including credit cards, bank accounts, financial reports, user passwords, employee information, and intellectual properties.
- 11 I experienced social engineering where an attacker impersonated my CFO and asked to do a wire transfer.
- 12 I cross-check that online content is from trustworthy sources. If I receive content from external sources, I check that it is safe to consume.
- 13 I feel that it is a good idea to check everything every time. It is like having a strategy to trust no one.
- 14 My company is a small startup, and we do not have a single full-time employee staffed to manage security issues.
- 15 I am mindful of the process of employees' authority to wire payments and do electronic fund transfers. I demand extra scrutiny of international wires.
- 16 I do not open attachments from unidentified sources.
- 17 We experienced an attack where we lost control over all the servers and all my organization's applications. It was dangerous and took us several days to be back to normal. We overhauled our security program after learning our lesson.
-

- 
- 18 I watch out for suspicious emails. I have observed spelling and grammar mistakes in phishing emails. On the contrary, I have also seen perfect emails without any mistakes. I have noticed that phishing emails often demand urgent actions.
- 19 I believe that every organization's biggest problem is cybercrime. In large organizations, not everyone knows everyone. Hackers spend much of their time before the attack researching, and they are looking to take advantage of the employees who are eager to help. I help employees realize and visualize how information can be exploited.
- 20 I think it is vital to stop emails that cause information security attacks. All email systems provide spam filter functionality. I set the spam filter option to high to keep the suspicious emails out of access. I balance it by checking the spam folder so that spam folders do not have genuine emails. I get many emails that are spam.
- 21 I have seen people getting calls from hackers pretending to be a Help Desk person from their company. I am continually alert with all incoming calls to ensure that they are from a trusted source.
- 22 Never reveal passwords.
- 23 In general, breaches happen due to either technical problems or user problems. Cyberattacks are mainly network-based or social-based. Network attacks involve acquiring unauthorized access through applications or infrastructure. Social attacks involve social engineering to tricking people into gaining unauthorized access to information. I have learned from my experience where someone contacted me posing as my antivirus software company account representative.
- 24 I have engaged with an external vendor who provides cybersecurity solutions to my small business.
- 25 As a Global CISO, the best advice I can give is to make information security training a regular activity.
- 26 Our executive leadership understands the value and supports the program. Our program is checked with the auditors and regulators to assess if we are doing the right thing.
- 27 My company did a security campaign. However, it was "one and done". A one-time program is not good enough for the employees to continuously make a more thoughtful selection.
-

- 
- 28 Be careful with everything in today's time. If someone offers a free iPhone, then be suspicious. No one is going to provide a free iPhone to an unknown person without any reason.
- 29 I am constantly cautious not to get free Wi-Fi.
-



## References

- Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196. doi:10.1016/j.techsoc.2010.07.001
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. doi:10.1126/science.aaa1465
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. doi:10.1016/0749-5978(91)90020-t
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012, January). Security policy compliance: User acceptance perspective. In *Proceedings of the 45th Hawaii International Conference on System Sciences* (pp. 3317-3326). HICSS. doi:10.1109/hicss.2012.516
- Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO Model. *Communications of the Association for Information Systems*, 41, 62-96. doi:10.17705/1cais.04104
- Alazri, A. S. (2015). The awareness of social engineering in information revolution: Techniques and challenges. *Institute of Electrical and Electronic Engineers International Conference for Internet Technology and Secured Transactions*, 198- 201. doi: 10.1109/ICITST.2015.7412088
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661-687. doi:10.1057/s41303-017-0057-y
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613. doi:10.2307/25750694
- Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490. doi:10.1287/isre.1100.0335
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3), 706-714. doi:10.1016/j.chb.2012.12.018
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312. doi:10.1016/j.chb.2014.05.046

- Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74–94. doi:10.1007/bf02723327
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191–215. doi:10.1037/0033-295x.84.2.191
- Bandura, A., Adams, N. E., Hardy, A. B., & Howells, G. N. (1980). Tests of the generality of self-efficacy theory. *Cognitive Therapy and Research*, 4(1), 39–66. doi:10.1007/bf01173354
- Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?. *Information Technology & People*, 28(3), 426-441. doi:10.1108/itp-10-2014-0232
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1042. doi:10.2307/41409971
- Beldad, A., van der Geest, T., de Jong, M., & Steehouder, M. (2012). Shall I tell you where I live and who I am? Factors influencing the behavioral intention to disclose personal data for online government transactions. *International Journal of Human-Computer Interaction*, 28(3), 163–177. doi:10.1080/10447318.2011.572331
- Bhakta, R. & Harris, I. G. (2015). Semantic analysis of dialogs to detect social engineering attacks. *Institute of Electrical and Electronic Engineers International Conference on Semantic Computing*, 424-427. doi: 10.1109/HICSS.2015.422
- Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, 34(10), 1022–1035. doi:10.1080/0144929x.2015.1028448
- Boss, S. R., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864. doi:10.25300/misq/2015/39.4.5
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164. doi:10.1057/ejis.2009.8
- Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy Magazine*, 9(2), 18–26. doi:10.1109/msp.2010.198

- Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: Social engineering. *International Journal of Accounting & Information Management*, 20(4), 335–347. doi:10.1108/18347641211272731
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548 doi:10.2307/25750690
- Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), 97-115. doi:10.1007/s11292-014-9222-7
- Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190-209. doi:10.1016/j.chb.2016.11.018
- Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*, 25(5), 517-533. doi:10.1108/02640470710829514
- Cappelleri, J. C., Darlington, R. B., & Trochim, W. M. K. (1993). A01 Power analysis of cutoff-based randomized clinical trials. *Controlled Clinical Trials*, 14(5), 399. doi:10.1016/0197-2456(93)90067-n
- Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52(2), 167–182. doi:10.1109/tpc.2009.2017985
- Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), 247–256. doi:10.14257/ijisia.2016.10.1.23
- Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, 29(3), 157-188. doi:10.2753/MIS0742-1222290305
- Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, 55(3), 11-19. doi:10.1080/08874417.2015.11645767
- Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly*, 40(1), 205-222. doi:10.25300/misq/2016/40.1.09

- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.
- Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334-345. doi:10.1016/j.chb.2016.08.034
- Churchill, G. A., Jr. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73. doi:10.2307/3150876
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Cohen, J. (1992). Quantitative methods in psychology: A power primer. *Psychological Bulletin, 112*(1), 155-159. doi:10.1037/0033-2909.112.1.155
- Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211. doi: 10.2307/249688
- Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31–38. doi:10.19101/ijacr.2016.623006
- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26*(6), 605–641. doi:10.1057/s41303-017-0059-9
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297. doi:334. 10.1007/bf02310555
- Crossler, R. E., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 45*(4), 51-71. doi:10.1145/2691517.2691521
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. doi:10.1016/j.cose.2012.09.010

- Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28(1), 209–226. doi:10.2308/isys-50704
- D’Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643–658. doi:10.1057/ejis.2011.23
- D’Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285–318. doi:10.2753/mis0742-1222310210
- D’Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113–117. doi:10.1145/1290958.1290971
- D’Arcy, J., & Hovav, A. (2008). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89(1), 59–71. doi:10.1007/s10551-008-9909-7
- D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. doi:10.1287/isre.1070.0160
- D’Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43–69. doi:10.1111/isj.12173
- Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, 281–297. doi:10.1016/j.cose.2014.11.002
- Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*, 24(1), 116–134. doi:10.1108/ics-04-2015-0018
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982–1003. doi:10.1287/mnsc.35.8.982
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127–153. doi:10.1046/j.1365-2575.2001.00099.x
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. doi:10.1287/isre.1060.0080

- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), doi:10.17705/1jais.00133
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73–80. doi:10.1016/j.cose.2006.10.009
- Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based model of human weakness for attack and defense investigations. *International Journal of Computer Network and Information Security*, 9(1), 1–11. doi:10.5815/ijcnis.2017.01.01
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13-23. doi:10.1016/j.dss.2016.02.012
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407-429. doi:10.1111/j.1559-1816.2000.tb02323.x
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50. doi:10.1177/002224378101800104
- Gall, M. D., Borg, W. R., & Gall, J. P. (1996). *Educational research: An introduction*. White Plains, NY: Longman
- Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, 35(2), iii-A7. doi:10.2307/23044042
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems*, 16(1), 5. doi: 10.17705/1CAIS.01605
- Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4), 281–295. doi:10.1016/j.jsis.2010.10.002
- Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 22–44. doi:10.17705/1jais.00447

- Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony Playstation network breach. *MIS Quarterly*, *41*(3), 703-727. doi:10.25300/misq/2017/41.3.03
- Götz, O., Liehr-Gobbers, K., & Krafft, M. (2010). Evaluation of structural equation models using the partial least squares (PLS) approach. In *Handbook of partial least squares* (pp. 691-711). Springer, Berlin, Heidelberg. doi:10.1007/978-3-540-32827-8\_30
- Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers*, *16*(3), 337-345. doi:10.1007/s10796-014-9514-5
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236. doi:10.2753/mis0742-1222280208
- Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*, *17*(3), 276–289. doi:10.1108/09685220910978112
- Haenlein, M., & Kaplan, A. M. (2004). A beginner's guide to partial least squares analysis. *Understanding Statistics*, *3*(4), 283-297. doi:10.1207/s15328031us0304\_4
- Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388-407. doi:10.1108/09685220911006687
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. Upper Saddle River, NJ, USA: Prentice Hall.
- Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles, CA: Sage.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139-152. doi:10.2753/mtp1069-6679190202
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. doi:10.1108/eb-11-2018-0203
- Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. doi:10.1080/10580530.2015.1117842
- Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1–39. doi:10.1145/2835375

- Henseler, J., & Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling: A Multidisciplinary Journal*, 17(1), 82-109. doi:10.1080/10705510903439003
- Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, 116(1), 2-20. doi:10.1108/imds-09-2015-0382
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135. Doi:10.1007/s11747-014-0403-8
- Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. doi:10.1016/j.dss.2009.02.005
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. doi:10.1057/ejis.2009.6
- Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275-298. doi:10.25300/misq/2013/37.1.12
- Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49(2), 99–110. doi:10.1016/j.im.2011.12.005
- Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1-55. doi:10.1080/10705519909540118
- Hu, Q., & Dinev, T. (2005). Is spyware an Internet nuisance or public menace? *Communications of the ACM*, 48(8), 61. doi:10.1145/1076211.1076241
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660. doi:10.1111/j.1540-5915.2012.00361
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95. doi:10.1016/j.cose.2011.10.007



- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69–79. doi:10.1016/j.im.2013.10.001
- International Organization for Standardization, & International Electrotechnical Commission. (2005). *Information Technology: Security Techniques: Code of Practice for Information Security Management*. ISO/IEC.
- Jakobsson, M. (Ed.). (2016). *Understanding social engineering based scams*. New York, NY: Springer.
- Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), 584–593. doi:10.1080/0144929x.2011.632650
- Jayanti, R. K., & Burns, A. C. (1998). The antecedents of preventive health care behavior: An empirical study. *Journal of the Academy of Marketing Science*, 26(1), 6-15. doi:10.1177/0092070398261002
- Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2), 597–626. doi:10.1080/07421222.2017.1334499
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566. doi:10.2307/25750691
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134. doi:10.25300/misq/2015/39.1.06
- Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75-87. doi:10.1016/j.chb.2016.09.012
- Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139–154. doi:10.1016/s0268-4012(02)00105-6
- Kaushalya, S. A. D. T. P., Randeniya, R. M. R. S. B., & Liyanage, A. D. S. (2018, November). An overview of social engineering in the context of information security. In *Proceedings of the 5th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1-6). IEEE. doi:10.1109/icetas.2018.8629126
- Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy Magazine*, 10(2), 24–32. doi:10.1109/msp.2011.179

- Kline, R. B. (2011). *Principles and practice of structural equation modeling*. New York, NY: Guilford.
- Krishnamurthy, B., & Wills, C. E. (2009, August). On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM Workshop on Online Social Networks* (pp. 7-12). ACM. doi:10.1145/1592665.1592668
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 22, 113-122. doi:10.1016/j.jisa.2014.09.005
- Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security. *Information Management & Computer Security*, 21(1), 5–15. doi:10.1108/09685221311314383
- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, 25(2), 241-280. doi:10.2753/mis0742-1222250210
- Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52(2), 353–363. doi:10.1016/j.dss.2011.09.002
- LaRose, R., & Eastin, M. S. (2004). A social cognitive theory of Internet uses and gratifications: Toward a new model of media attendance. *Journal of Broadcasting & Electronic Media*, 48(3), 358–377. doi:10.1207/s15506878jobem4803\_2
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–1092. doi:10.1108/mrr-04-2013-0085
- Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454. doi:10.1080/01449290600879344
- Lee, H., Lim, D., Kim, H., Zo, H., & Ciganek, A. P. (2013). Compensation paradox: The influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, 34(1), 45–56. doi:10.1080/0144929x.2013.805244
- Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2), 57–63. doi:10.1108/09685220210424104
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707–718. doi:10.1016/j.im.2003.08.008

- Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361–369. doi:10.1016/j.dss.2010.07.009
- Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, 48(8), 72. doi:10.1145/1076211.1076243
- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187. doi:10.1057/ejis.2009.11
- Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th Ed.). Upper Saddle River, NJ: Prentice Hall.
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71-90. doi:10.2307/20650279
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413. doi:10.17705/1jais.00232
- Liang, H., Xue, Y., Pinsonneault, A., Wu, Y. (2019). What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly*, 43(2), 373–394. doi:10.25300/misq/2019/14360
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173-186. doi:10.2307/249574
- Luga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1). doi:10.1186/s13673-016-0065-2
- Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence*, 35(1), 31–41. doi:10.1016/j.adolescence.2011.06.007
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469-479. doi:10.1016/0022-1031(83)90023-9
- Mahalanobis, P. C. (1936). On the generalized distance in statistics. *National Institute of Science of India*, 2, 49-55.

- Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431-433. doi:10.2307/25750685
- Malfaz, M., & Salichs, M. A. (2011). Learning to avoid risky actions. *Cybernetics and Systems*, *42*(8), 636-658. doi:10.1080/01969722.2011.634681
- Mansfield-Devine, S. (2016). The imitation game: How business email compromise scams are robbing organisations. *Computer Fraud & Security*, *2016*(11), 5-10. doi:10.1016/s1361-3723(16)30089-6
- Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction*, *3*(3), 170-188. doi:10.17705/1thci.00032
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156. doi:10.1016/j.chb.2016.11.065
- McCoy, D., Park, Y., Shi, E., & Jakobsson, M. (2016). Identifying scams and trends. In M. Jakobsson (Ed.), *Understanding Social Engineering Based Scams* (pp. 7-19). New York, NY: Springer.
- Meguerdichian, S., Koushanfar, F., Qu, G., & Potkonjak, M. (2001, July). Exposure in wireless ad-hoc sensor networks. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking* (pp. 139-150). ACM. doi:10.1145/381677.381691
- Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230. doi:10.1080/07421222.2017.1394083
- Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems*, *55*(1), 83-91. doi:10.1080/08874417.2014.11645743
- Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). New York, NY: Routledge.
- Mertler, C. A., & Vannatta, R. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (5th ed.). Glendale, CA: Pyrczak Publishing.
- Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67. doi:10.1080/15536548.2013.10845672

- Meyers, L. S., Gamst, G. & Guarino, A. J. (2006). *Applied Multivariate Research: Design and Interpretation*. Thousand Oaks, CA: Sage Publications.
- Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), 449-473. doi:10.1111/j.1745-6606.2009.01148.x
- Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143. doi:10.1111/j.1559-1816.2000.tb02308
- Mitnick, K. D., & Simon, W. L. (2002). *The art of deception. Controlling the human element of security*. Indianapolis, IN: Wiley Publishing, Inc.
- Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366-2375. doi:10.1016/j.chb.2012.07.008
- Moody, G. D., Siponen, M., & Pahnla, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1) 285–311. doi:10.25300/misq/2018/13853
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209. doi:10.1016/j.cose.2016.03.004
- Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, 42. doi:10.17705/1cais.04207
- Myyry, L., Siponen, M., Pahnla, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126–139. doi:10.1057/ejis.2009.10
- Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825. doi:10.1016/j.dss.2008.11.010
- Niederman, F., & March, S. (2015). Reflections on replications. *AIS Transactions on Replication Research*, 1, 1-16. doi:10.17705/1attr.00007
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. New York, NY: McGraw-Hill.

- Olson, R., Verley, J., Santos, L., & Salas, C. (2004). What we teach students about the Hawthorne Studies: A review of content within a sample of introductory I-O and OB textbooks. *The Industrial-Organizational Psychologist*, 41(3), 23-39. doi:10.1037/e578812011-002
- Osuagwu, E. U., & Chukwudebe, G. A. (2015). Mitigating social engineering for improved cybersecurity. *Institute of Electrical and Electronic Engineers International Conference on Cyberspace Governance*, 91-100. doi: 10.1109/CYBER-Abuja.2015.7360515
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183-199.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, 52, 194–206. doi:10.1016/j.cose.2015.02.008
- Petter, S., Straub, D. W., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656. doi:10.2307/25148814
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. doi:10.1037/0021-9010.88.5.879
- Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63(1), 539-569. doi:10.1146/annurev-psych-120710-100452
- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214. doi:10.1080/07421222.2015.1138374
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 37(4), 1189–1210. doi:10.25300/misq/2013/37.4.09
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778. doi:10.2307/25750704
- Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, 51(3), 493-505. doi:10.1016/j.dss.2011.02.013

- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803
- Roldán, J. L., & Sánchez-Franco, M. J. (2012). Variance-based structural equation modeling: Guidelines for using partial least squares in information systems research. In *Research methodologies, innovations and philosophies in software systems engineering and information systems* (pp. 193-221). IGI Global. doi:10.4018/978-1-4666-0179-6
- Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*(4), 328–335. doi:10.1177/109019817400200403
- Rosenstock, I. M. (2005). Why people use health services. *Milbank Quarterly, 83*(4). doi:10.1111/j.1468-0009.2005.00425.x
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82. doi:10.1016/j.cose.2015.10.006
- Saleem, N. (1996). An empirical test of the contingency approach to user participation in information systems development. *Journal of Management Information Systems, 13*(1), 145-166. doi:10.1080/07421222.1996.11518116
- Sarstedt, M., Wilczynski, P., & Melewar, T. C. (2013). Measuring reputation in global markets—A comparison of reputation measures' convergent and criterion validities. *Journal of World Business, 48*(3), 329–339. doi:10.1016/j.jwb.2012.07.017
- Schaller, T. K., Patil, A., & Malhotra, N. K. (2014). Alternative techniques for assessing common method variance: An analysis of the theory of planned behavior research. *Organizational Research Methods, 18*(2), 177-206. doi:10.1177/1094428114554398
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th ed.). West Sussex, United Kingdom: John Wiley & Sons LTD.
- Siponen, M., Pahnla, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71. doi:10.1109/mc.2010.35
- Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289–305. doi:10.1057/ejis.2012.59
- Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current directions in psychological science, 15*(6), 322-325. doi:10.1111/j.1467-8721.2006.00461.x

- Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, 9(1), 26–46. doi:10.4018/ijisp.2015010102
- Stajano, F., & Wilson, P. (2011). Understanding scam victims. *Communications of the ACM*, 54(3), 70. doi:10.1145/1897852.1897872
- Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2), 355–378. doi:10.25300/misq/2014/38.2.02
- Steenkamp, J. B. E., & Baumgartner, H. (2000). On the use of structural equation models for marketing modeling. *International Journal of Research in Marketing*, 17(2-3), 195–202. doi:10.1016/s0167-8116(00)00016-1
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169. doi:10.2307/248922
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. doi:10.1287/isre.1.3.255
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441. doi:10.2307/249551
- Sumsion T. (1998). The Delphi technique: An adaptive research tool. *British Journal of Occupational Therapy*, 61(4), 153-156. doi:10.1177/030802269806100403
- Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2007). *Using multivariate statistics* (Vol. 5). Boston, MA:Pearson.
- Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, 38, 159–173. doi:10.1016/j.chb.2014.05.027
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014-1023. doi:10.1080/0144929x.2013.763860
- Thomas, L., & Juanes, F. (1996). The importance of statistical power analysis: An example from Animal Behaviour. *Animal Behaviour*, 52(4), 856–859. doi:10.1006/anbe.1996.0232
- Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150. doi:10.1016/j.cose.2016.02.009



- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506–517. doi:10.1016/j.im.2015.03.002
- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198. doi:10.1016/j.im.2012.04.002
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. doi:10.2307/30036540
- Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, 39(1), 91-112. doi:10.25300/misq/2015/39.1.05
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11), 759–783. doi:10.17705/1jais.00442
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101-105. doi:10.1057/ejis.2009.12
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13. doi:10.1016/j.ijhcs.2018.06.004
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20. doi:10.25300/misq/2013/37.1.01
- Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs*, 61(2), 113–134. doi:10.1080/03637759409376328
- Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, 33(2), 597-620. doi:10.1080/07421222.2016.1205934
- Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1-32.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816. doi:10.1016/j.chb.2008.04.005

- Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1), 273–303. doi:10.2753/mis0742-1222270111
- Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, 22(2), 400–414. doi:10.1287/isre.1090.0266
- Yang, J., Zhang, Y., & Lanting, C. J. M. (2017). Exploring the impact of QR codes in authentication protection: A study based on PMT and TPB. *Wireless Personal Communications*, 96(4), 5315-5334. doi:10.1007/s11277-016-3743-5
- Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in security. *Journal of Information Systems Education*, 23(4), 407-415. doi:10.3938/npsm.63.227
- Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110. doi:10.1207/s15506878jobem4901\_6
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389-418. doi:10.1111/j.1745-6606.2009.01146.x
- Zahedi, F., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, 16(6), 448–484. doi:10.17705/1jais.00399
- Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), 180-197. doi:10.1080/15332860903467508
- Zweighaft, D. (2017). Business email compromise and executive impersonation: Are financial institutions exposed? *Journal of Investment Compliance*, 18(1), 1-7. doi:10.1108/joic-02-2017-0001