

2019

Assessing the Presence of Mindfulness within Cyber and Non-Cybersecurity groups

Christopher Wilder

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of 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.

Assessing the Presence of Mindfulness within Cyber and Non-Cybersecurity groups

by

Christopher Wilder

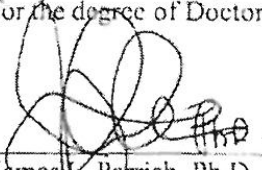
A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

November 27, 2019


Approval /Signature

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



James L. Parrish, Ph.D.
Chairperson of Dissertation Committee

11/27/2019
Date



Steven R. Terrell, Ph.D.
Dissertation Committee Member


11/27/19
Date



Timothy J. Ellis, Ph.D.
Dissertation Committee Member

11/27/2019
Date

Approved:



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

11/27/2019
Date

College of Computing and Engineering
Nova Southeastern University

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

Assessing the impact of Mindfulness on Cyber and Non-Cybersecurity groups: Intentions towards
reducing Phishing Susceptibility

by
Christopher Wilder
November 27, 2019

Corporations and individuals continue to be under Phishing attack. Researchers categorizes methods corporations and individuals can employ to reduce the impact of being caught in a Phishing scheme. Corporation enable technical mechanisms such as automated filtering, URL blacklisting, and manipulation of browser warning messages to reduce phishing susceptibility costing billions of dollars annually. However, even with robust efforts to educate employees about phishing techniques through security awareness training the abundance of attacks continues to plague organizations. This study aims to identify whether a correlation exists between mindfulness and phishing susceptibility. The goal of this research is to determine if mindful individuals are less susceptible to phishing. By showing individuals with increased awareness are significantly able to identify areas that phishing attempts exploit.

Based on a review of the literature a misconception exists between end-users, corporation and Internet Service Providers (ISP) regarding ownership of Phishing identification. Specifically, individuals blame ISPs and corporate information technology departments for failing to protect them from Phishing attacks. Still, the truth of the matter is that the end-user is ultimately the weakest link in the phishing identification chain. The methodology of this study polled participants through initial screening focusing on whether the individuals were mindful using the Mindful Attention Awareness Scale (MAAS) survey. Conclusions seen in this study in contrast with other studies saw no significant correlation between Mindfulness and phishing susceptibility, increase in cogitative ability or increase in Phishing identification. Thus, continued use of MAAS survey questionnaire is necessary to screen other groups for phishing awareness prior to focusing on other phishing cues.

Acknowledgements

Primarily, I want to give honor and praise to God for only through him have I been blessed to be able to accomplish this task. Throughout the writing of this dissertation I have received a great deal of understanding and support from my friends and family. Without the understanding of my wife Crystal, daughters Quiana and Briana, I never would have made it through this milestone and chapter of my life without their loving support.

I want to thank Dr. Parrish, my advisor for continuing to support my research and aiding in completion of my research. To my committee, Dr. Terrell and Dr. Ellis without your wisdom and guidance this report could not have been accomplished, I appreciate the guidance, conversation and pointing me in the right direction.

Finally, I want to thank my parents for believing in me and always pushing me to perform at my best and to continue being a role model for the entire Wilder family. I know my Grandmother is smiling down on me. This achievement is for you Grandma.

Table of Contents

Abstract

List of Tables

List of Figures

List of Tables	viii
List of Figures	ix
Chapter 1	1
Introduction	1
Background.....	1
Problem Statement.....	6
Dissertation Goal	6
Research Questions.....	6
Relevance and Significance.....	6
Barriers and Issues.....	8
Assumptions, Limitations, and Delimitations	8
Definitions of Terms.....	8
Summary.....	9
Chapter 2.....	10
Review of the Literature.....	10
Introduction	10
Theoretical Framework.....	16
Elaboration Likelihood Model (ELM)	17
Technology Threat Avoidance Theory.....	20
Mindfulness	24
Training Efficacy	26
Technical controls.....	34
Summary.....	39
Chapter 3.....	41

Research Methodology.....	41
Research Design	41
Research Questions.....	41
Data Necessary to Answer the Research Questions	42
Instrument Development	42
Population and Sample	43
Data Collection	44
Data analysis.....	44
Resource requirements	46
Summary.....	46
Chapter 4.....	47
Introduction	47
Data Collection	47
Sample Population.....	48
Summary of Results	54
Chapter 5.....	55
Conclusion, Implications, Recommendations, and Summary	55
Introduction	55
Conclusions	55
Implications	57
Recommendations for Future Research.....	58
Summary.....	59
Appendix A.....	65
Survey Instruments.....	65
Survey Monkey Quiz Questions.....	65
Appendix B	66
Sample Invitation to Participate in Dissertation Study	66
Appendix C	70
IRB Approval	70
References.....	71

List of Tables

- Chapter 2** Table 1 – Theory Elements and Sources of Theory
Table 2 – ELM persuasion cues
Table 3 – Research Variables
Table 4 – Mindfulness Survey Questions
Table 5 – Gartner Magic Quadrant for Security Awareness Computer-Based Training
Table 6 – Clickthrough rates
- Chapter 4** Table 7 – Demographic Statistics
Table 8 – Levene’s Test of Equality of Error Variances
Table 9 – Levene’s Test of Equality of Error Variances for Mindfulness
Table 10 – ANOVA Mindfulness Score Test of Between Subjects Effects
Table 11 – ANOVA Mindfulness Score Test of Between Subjects Effects of Mindfulness
Table 12 – Spearman’s rho Correlation

List of Figures

- Chapter 2** Figure 1. Phishing Control Matrix
- Figure 2. Phishing attack cues
- Figure 3. Phishing stages
- Figure 4. Formula for Susceptibility to Influence
- Figure 5. Research Model
- Figure 6. Components of E-Learning

Chapter 1

Introduction

Background

Despite the abundance of warnings and corporate security awareness training users against unsafe information security behavior, these “educated” users continue to click on embedded links from known and sometimes unknown email senders. Initial indications from the reviews of the literature characterize phishing as a significant threat to individuals and organizations, phishing attacks alone represent a significant drain on the economy and a global problem (Wright, Jensen, Thatcher, Dinger, & Marett, 2014). The impact from phishing spans all industrialized countries resulting in organizations losing billions of dollars according to the (RSA, 2014). Furthermore, a recent report on the top twenty phishing targets, identified CIBC, Apple, Inc., PayPal, Google, and Yahoo as the top five, having a 5,000% increase of attacks.

The Anti-Phishing Working Group (APWG) customers reported over the last quarter of 2018, 138,328 unique phishing web sites and 239,910 unique phishing email (campaigns). Meanwhile, the study by Ponemon Institute and Accenture (2017), identified 67% of companies had experienced some form of phishing and social engineering attack. While InfoWorld reported seeing 6.3 million phishing emails during the first quarter 2016. Accordingly, Abawajy (2014), and Hovav and Gray (2014), stated organizations had sustained significant cost and damage to their reputation due to the massive data breaches caused by internal employees. For example, in 2013, RSA reported 450,000 phishing attacks with estimated losses over \$5.9 billion, although less than the estimated losses posit to exceed \$1

trillion globally by Bose et al. (2008) as cited by Vishwanath, Herath, Chen, Wang and Rao (2011). Furthermore, researchers continue to identify phishing as a major issue despite the extensive attention paid to technical solutions to combat phishing; organizations remain vulnerable to end-user behavior (Wright et al., 2014).

Currently, 91% of known breaches are associated with a form of phishing attack (WIRED, n.d.) that can subject end users and organizations to malware and ransomware (CSO Online, n.d.) or other types of infections. CSO Online stresses 93% of phishing emails can cause infections from ransomware, that is up from the 80% of the 507 billion emails sent per day that are reported as spam, malware, or phishing according to Wright et al. (2014). Furthermore, a review of the literature depicts five of the top twenty phishing targets are CIBC, Apple, Inc., PayPal, Google, and Yahoo with a combined 5,000% increase in attacks. However, none of these targets are related to corporations but online access is potentially occurring using corporate infrastructure and assets.

One example of a successful phishing attack occurred twice against The National Bank of Blacksburg which lost more than \$569,000 in the incident (Krebs, 2018). In the first instance an employee fell victim to a targeted phishing email which allowed the intruder to install malware on the victim's computer. This allow the intruder to compromise a second computer with access to the STAR Network, a system run by First Data that handles debit card transaction for customer. In the second breach eight months, the STAR Network was compromised again in addition to the bank's Navigator system used to manage credits and debits to customer accounts. In another example against the taxpayers in the United States (U.S.). In 2014 the IRS reported a 66% increase in attacks on U.S. taxpayers and issued IR-2014-39 warning taxpayers about a new email phishing scheme (IRS, 2014). Phishers posing as IRS employees contacted taxpayers utilizing facial recognition messaging expressing "Your reported 2013 income is flagged for review due to a document processing error.

Your case has been forwarded to the Taxpayer Advocate Service for resolution assistance. To avoid delays processing your 2013 filing contact the Taxpayer Advocate Service for resolution assistance” (IRS, 2014, p. 1). Taxpayers’ that replied to this phishing request refunds vanished without a trace.

Because of the high incidence of users’ falling for phishing schemes, organizations have increased spending on Information Security (IS) tools (e.g., black listing web sites, enhances browser warning messages, increased security awareness training, automated detection technology and hiring of cybersecurity professional) that impact administrative, physical, and technical controls used to affect employee information security compliant behavior (Ifinedo, 2012). Furthermore, most web browsers provide automated warning messages to alert individuals about issues identified in the email or embedded links. Despite these security measures, studies show that individuals spend a limited amount of time looking at warning messages and pay little attention to warning messages they do look at because few messages tell the user what to do to cure the problem (2014 Anderson, Kirwan, Jenkins, Eargle, Howard, and Vance, 2014; .Hoban et al., 2014). The frequency of the messages also plays a role as seen in the eye movement-based memory effect (EMM) study performed by Anderson et al. (2013), which affirms people are paying less attention to security images and browser warning messages they have previously viewed, resulting to a form of habituation and mindlessness activity. Regardless, even if the messages were heeded, these technological interventions alone cannot eliminate the threat from phishing since phishers operate within legitimate communication channels, making it difficult for individuals to effectively distinguish between genuine messages and phishing messages (Alsharnouby, Alaca, and Chiasson, 2015; Ferrara, 2014; Wright et al., 2014).

A critical component for thwarting phishing starts with the individual’s diligence and resilience to resist clicking on embedded links in email messages and going to unfamiliar websites. End user training is considered a key component needed to combat security breaches and phishing attacks and

aids to improve overall security knowledge. Ferrara (2014, p. 3) hypothesizes these awareness trainings “must be continuous to maximize learning and lengthen retention of learned topics” thus improving an individual’s mindfulness. Furthermore, organizations must implement information security training and awareness programs (SETA), to ensure employees understand their security responsibilities and to increase employee security knowledge. Finally, the SETA programs must be dynamic and have ongoing awareness messages that keep employees abreast and refreshed on changes in the organization’s information security landscape as an integral part of the security culture (Abawajy, 2014).

Current research from the APWG stated for the last quarter of 2018, 138,328 unique phishing web sites and 239,910 unique phishing email (campaigns) exists that indicates phishing is still a major threat to organization and individuals alike. Therefore, automated controls, browser warning messages and even security awareness training have yet to slow down the advancement of phishing. Additionally, studies continue to identify the underlying issues surrounding phishing but fail to adequately fix the root cause for phishing, the individual. For example, Hoban et al. (2014) surveyed 301 non-cybersecurity individuals, collecting 1,062 news articles on computer security and 518 computer security education documents from universities, companies, and government institutions. Their study concluded the information received from participants only “defined the problem for them and did not offer any actions they could take to prevent an attack or how they should react to an attack that had already occurred” (Hoban, et al, 2014, p. 2). Thus, revealing a gap on how to address phishing before, during and after and individual is impacted.

In another study, performed by Ernst & Young (2013), EY’s Cybersecurity team surveyed 1,600 assurance, and advisory clients. The results of their survey found that 64% of their clients said the level of information security awareness of their employees is the greatest challenge to their

organization (van Kessel & Allan, 2013). The E&Y client responses were supported by the research of Knezevich (2014), who asserts in their study that 56% of corporate employees had not taken any information security awareness training. Subsequently, the lack of security education, training and awareness contributes to the increase of successful phishing attacks ranking phishing at 45% the second highest concern by decision makers, behind malware from web surfing at 49% (Osterman, 2015). Research shows the problem with addressing phishing continues to exist with employers continuing still have low confidence levels in their implemented security awareness training programs ability to train employees to detect phishing (Osterman, 2015; Ponemon Institute, 2016).

The literature describes an even more sizable proportion of employers have low confidence levels in their employee's ability to resist clicking on links or attachments that appear suspicious and embedded in email messages (Osterman, 2015). Still researchers report security incidents and breaches continue to be a significant problem, resulting in organizations losing billions of dollars (Ifinedo, 2014; RSA, 2014). Likewise, Ferrara (2014, p. 3) indicated within the "U.S. economy, 4 out of 10 organizations still don't provide any ongoing security education to their staff." Thus, a reduction in phishing attack success rates could mean a significant decrease in the loss of revenue associated with this attack as well as reducing one of the top concerns of information technology security decision-makers (SC Magazine, 2015).

One must note that the discussion on employee vulnerability to phishing and the weaknesses in current prevention methods and SETA programs has focused primarily on employees that function in non-security related roles. In fact, little research has been devoted to the differences between employees in security vs. non-security related positions and why non-security employees are most often the victims of organizational phishing attacks. One possible explanation is that security professionals possess higher levels of mindfulness. Mindfulness can heighten the individuals state of

involvement and wakefulness of being in the present to improve awareness to aid in the detection of phishing (Brown and Ryan, 2013). This leads us to the problem statement this research will address.

Problem Statement

While much effort and research has been devoted to identification and preventing the success of phishing attacks, it remains a major problem for organizations today. However, little research has been conducted on the role of mindfulness as it relates to phishing susceptibility and the differences between cybersecurity and non-cybersecurity employees in relation to mindfulness, resulting in a gap in the extant literature.

Dissertation Goal

The goal of this research is to better understand the role that mindfulness plays in a user's detection of a phishing message and to discover if there exists a difference in mindfulness between those people whose primary job role is to detect security exploits such as phishing and those that have other primary job roles not related to cybersecurity.

Research Questions

1. Is there a statistically significant correlation between mindfulness and phishing susceptibility?
2. Do cybersecurity professionals differ significantly from non-cybersecurity individuals statistically in their mindfulness and phishing susceptibility?

Relevance and Significance

Phishing is a worldwide issue that impacts organizations and individuals alike and is a genuine threat impacting individual and organizations financially or through disruption of service. We start with the individual's understanding and general awareness of phishing as a genuine threat to their personal and financial well-being. Phishing is not something that impacts a specific group of individuals but can be targeted to anyone with a web presence. The phishing problem is worldwide, but research

discloses the United States is targeted more than any other country with phishing attacks Ponemon Institute and Accenture (2017).

The addition of another potential variable that can be manipulated to decrease the susceptibility of individuals to phishing attacks. If mindfulness does play a role, then we can integrate mindfulness training into security training to potentially increase the efficacy of Security Education Training and Awareness (SETA) programs. is a reduction in an individual's phishing susceptibility and the increase in mindfulness attention. Researchers identify multiple avenues to thwart phishing attempts (i.e., browser warning messages, click rate tracking, polymorphic warning messages, blacking listing websites, security awareness training). However, there's not one single solution that can reduce phishing susceptibility. Only through coordination of multiple avenues can phishing identification be increased and susceptibility be reduced. It starts with mindfulness that phishing is occurring and paying attention to increases detection of phishing cues. Without individual involvement in the identification of phishing the landscape will continue to show increases from phishing attacks and increases in breaches to organizations and individuals resulting in a potential increase in financial losses.

This study adds to the body of knowledge by looking at the correlation between mindfulness and phishing susceptibility the first pairing identified in the literature review. Based on our study we identified a gap between cybersecurity professionals and non-cybersecurity individual's ability to identify phishing. Our intent is to close the gap between the groups through various phishing identification techniques along with identification of skill trait differences between the two groups. As seen in our demographic of the study cybersecurity professionals have a higher degree of education and age versus the non-cybersecurity group. This gap in age, knowledge and experience can be overcome using layers of defenses against phishing.

Barriers and Issues

The initial barrier for this study included the recruitment of cybersecurity professionals to complete the mindfulness survey. Recruitment took over four months of attending professional security chapter meetings, emails, posting to LinkedIn and twitter messaging to achieve an adequate population. As for non-cybersecurity individual's the utilization of college students completed our second group. A significant issue between the populations is their cybersecurity knowledge. Typically, a cybersecurity professional has at a minimum of a bachelor's degree, one or more security certifications and multiple years of experience in cybersecurity which would also equate to an older individual. In contrast, college students are less than 4 years out of high school still perusing their bachelor's degree, younger aged and have less experience or training in cybersecurity

Assumptions, Limitations, and Delimitations

A primary assumption is that every participant in our study has some knowledge of phishing or at least has seen a phishing message and are knowledgeable of the impact of phishing. Limitations of the study include the groups participating, we were unable to control for either group their knowledge, experience, education or age. The only delimitation imposed initially was the selection of cybersecurity individuals who were members of a cybersecurity organizations. This group of cybersecurity individuals have professional memberships that does not fully represent all cybersecurity professionals, thus making generalization somewhat difficult but possible.

Definitions of Terms

Phishing is defined as any email-based social engineering attack by PhishMe (2015). It can be any activity where confidential information such as personal as well as financial information from the user is obtained by luring the user towards an illegitimate webpage (Rakesh, Kannan, Muthurajkumar, Pandiyaraju, and SaiRamesh, 2014).

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces users to pay the ransom through specific online payment methods to grant access to their networks or to get their data back (Global Ransomware Resource Center, n.d.).

Spear Phishing is where an attacker crafts a specific email using personal and behavioral information obtained from public sites to lure an individual into clicking on links in the email or navigating to a corrupted web page.

Summary

Phishing is a global issue that shows no visible indication of slowing down. Even as organizations increase spending on IS tools to detect phishing, these types of attacks continue to rise. Meanwhile, the phishing strategy deployed by phishers remains consistent as described by a thirteen-year longitudinal study. Thus, moving individuals to a cognitive awareness from mindlessness to Mindful awareness can have a significant impact on the reduction of phishing susceptibility. However, to break the phishing cycle will require a commitment from organization and individuals towards improving training habits and frequency. Thus, enabling end users to comprehend phishing techniques and provide end users with the willingness to change their behavior to reduce phishing susceptibility. The remainder of this dissertation is structured as follows. First, there is a general review of the relevant literature that discusses techniques seen that have been tried to educate individuals on the phishing cues used by phisher's and how they are identified and can be manipulated for the phisher's advantage. Included in the literature review will be the theories used to address cognitive behavior and threat protection. Next the process for developing the methodology for individual participation and the survey instrument. The process will present the results of the quantitative statistical analysis and demographic information. Following statistical analysis of the results, the overall study context and design of phishing susceptibility will be discussed. Finally, concluding with remarks about the study, any limitations, and emphasis on future research in this area.

Chapter 2

Review of the Literature

Introduction

To answer the question proposed in this dissertation, to better understand the role that mindfulness plays in a user's detection of a phishing message and to discover if there exists a difference in mindfulness between those people whose primary job role is to detect security exploits such as phishing and those that have other primary job roles. We investigate how mindfulness practices can promote increased awareness of phishing and reduce phishing susceptibility. We begin with looking at how phishing continues to hook individuals with different variations of their messages and how interventions used to thwart such attacks. We include how increasing mindfulness activity would increase awareness of existing processes.

A review of literature looks at research from Anderson et al. (2015) and Proofpoint (2016), discuss that phishing continues to work because its techniques rely on human behavior rather than exploiting technology. Phishing attacks succeed because phishers cause users to respond to some action that is to the advantage of the attacker by tricking the end user to click on a fictitious website or installing malware by appealing to an individual's efficacy, urgency and order according to Yates and Harris (2015). Phishing attackers use spoofed business or personal email messages to trick individuals into going to compromised sites to capture information that can later cause harm to corporations or individuals. The overall design of this literature review is to identify techniques available to detect

phishing, whether through automated or manual discovery methods and how mindfulness can assist individuals by increasing awareness of methods to reduce phishing

The Proofpoint (2016), study describes phishing as preying on the personality of its victims by attacking the victim's work ethics. In this study it focused on assessing the risk perception of an individual toward phishing that could lead to increased susceptibility. These researchers emphasize when a person under-estimate's risk they increase their potential phishing susceptibility. Additionally, the study pointed out attackers are using legitimate but compromised mail servers and innocuous language to avoid automated technical defenses. As Figure 1 shows, individuals are the last line of defense for protection from phishing. One article reviewed covered risk perceptions of cyber security individuals was found in (SC Magazine, 2015). This article covered over a 1,000 Information Technology (IT) security decision-makers and practitioners, from organizations with over 500 employees, where the study found IT individuals had an increased perception of phishing or spear phishing attacks from 2014 to 2016. This increase of risk awareness stems from their training and awareness of the damage phishing and spear phishing was having on corporations. However, the article mentioned low-security education and awareness among employees and individuals could play a factor with increasing phishing susceptibility. The authors of the SC Magazine (2015, p. 1) article called this low-security knowledge the "greatest inhibitor to defending against cyber threats."

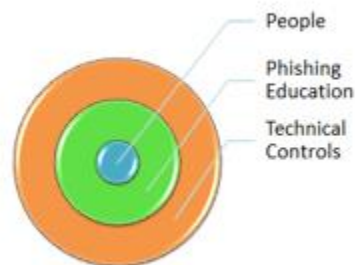


Figure 1 Phishing Control Matrix

To safeguard organization and individuals from phishing measures must include automated cues as the first line of defense in combating phishing attacks. Safeguarding measures that anyone can employ to assist in the identification of phishing should include; mechanical email filtering, email source, grammar and spelling, urgency cues and paying attention to the email title or subject. All these cues can be enhanced through an individual's use of mindfulness by paying closer attention and scrutinizing the construction of email messages received. In the study of Liang and Xue (2009), they posit that safeguarding measures with the highest perceived avoidance will aid individuals with reducing their perceived threat (e.g., threat avoidance) thereby decreasing the likelihood of responding to phishing emails. This perceived threat reduction is obtained when the individual is aware of the dangers posed by phishing and pays more attention to its potential impact to the individual or corporation.

In another study, Yates and Harris (2015), describe the method for which individuals filter email messages is based on the credibility of the email appearance qualities and judgment regarding persuasiveness of the letter to filter whether the email received is legitimate or not. Figure 2 below identifies obvious cues found within email messages phishers use to trick individuals into clicking on embedded links.

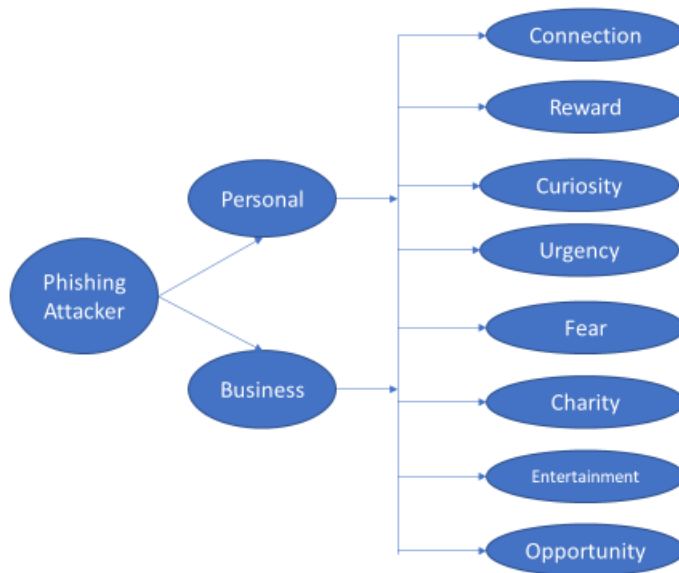


Figure 2 Phishing Attack Cues

Wright et al. (2014), describes the techniques phishers use in their attempt to trick users through email messages, however, no research will be included in this study to identify how individuals notice these phishing practices. Accordingly, they, studied 2,624 university students using the six phishing influence techniques (i.e., liking, reciprocity, social proof, consistency, authority, and scarcity) and found phishing messages that included liking, social proof, and scarcity were the most effective in getting non-cyber security individuals to click on the phishing related messages. This type of message behavior (i.e., liking, social proof, consistency and scarcity) are similar to several of the mindfulness questions of Brown and Ryan (2003), specifically question 7, “I seem to be running on automatic without much awareness of what I’m doing”; 8 “I rush through activities without being attentive to them”; and 10 “I do jobs or tasks automatically without being aware of what I’m doing” thus enabling an increase in the individuals susceptibility to phishing. Therefore, by adding

mindfulness to our phishing study the examination should allow for increased employee cognitive behavior, increased phishing knowledge and a reduction in phishing susceptibility.

According to Down, Holbrook and Cranor (2006), their study describes susceptibility to phishing as being rooted in an individual's knowledge and experience used to predict behavioral responses to phishing attacks. Furthermore, they found individuals with knowledge of phishing should have a significant reduction from falling for a phishing email, clicking a phishing link, visiting a phishing website, or entering information into a phishing website. While, other researchers Shillair et al. (2015) and Vishwanath et al. (2011), explain phishing studies tend to explore the general decision strategies that users adopt to detect phishing. Meanwhile, the technical components used to check for phishing are included the research from Akhawe and Felt (2013), Felt, Ainslie, Reeder, Consolvo, Thyagaraja, Bettes and Grimes (2015), Herzberg (2009). One technical study, Anderson et al. (2015), included the use of polymorphic warnings messages that change formats every time they are evoked as an effective method to reduce Habituation, which is fatigue from repeatedly seeing the same browser message.

In the review of the literature the study performed by Burns, Durcikova, and Jenkins (2012) described three phishing stages that impact individuals targeted by a phishing as described in Figure 3. Initially there is denial, where the employee may not perceive that they could be a target of a phishing attempt. Employees at the denial stage are categorized as mindless for not paying attention to the potential harm phishing can cause. Second, intention to avoid, has the employee realizing phishing is an issue but not performing any specific action to avoid phishing. Finally, at the action stage, the employee understands the results, is knowledgeable of vulnerabilities associated with phishing and remains mindful to avoid phishing attempts according to Burns, Durcikova, and Jenkins (2012). By

adding mindfulness to the phishing stages employees become more aware of phishing and should increase their cognitive behavior to allow them to decrease phishing susceptibility.

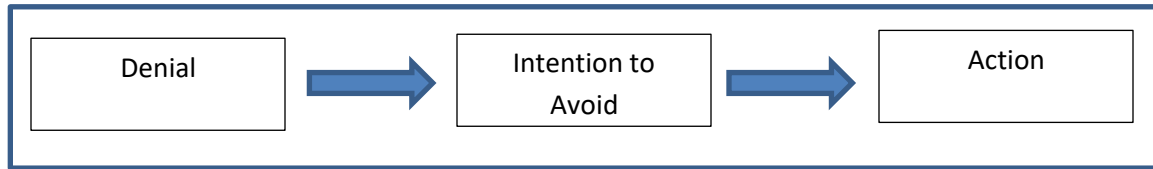


Figure 3 Phishing Stages

A significant postulation seen in the review of literature discusses how attackers create phishing messages that are like ordinary everyday email messages yet deceptive in nature. These email messages with embedded links can trick individuals into clicking on links sending the user to compromised websites where malware and other malicious activity lurks. A significant understanding among researchers suggest individuals are the weakest link and have poor judgement when it comes to detecting phishing thus increasing susceptibility to phishing (Alsharnouby, Alaca, & Chiasson, 2015). Several of the studies on user susceptibility to phishing explored area of neuroscience Anderson et al. (2015), and to combat phishing the research covered experimental studies Anderson et al. (2012), eye tracking Alsharnouby et al. (2015), breach cause case studies Hovav and Gray (2014), role play Downs et al. (2007), online gaming Shillair et al. (2015), phishing influence techniques Wright et al. (2014) and browser security warning message effectiveness (Akhawe and Felt, 2013; Felt et al., 2015; Herzberg, 2009). Studies show individuals with technical intelligence of web environments, typically identified with cybersecurity employees appear to have an increased resistance to phishing as described by Alsharnouby et al. (2015) and Downs et al.(2007). This resistance originates from employees having implied knowledge and experience with phishing, browser security cues, digital certificates, SSL and other security indicators associated with websites. Even knowledgeable individuals suffer from habituation, as described by Downs et al. (2007), as the reduction of the psychological or behavioral response occurring when a specific stimulus like browser warning

messages occurs repeatedly. The next section of the literature review will briefly discuss the theories used to investigate phishing.

Theoretical Framework

Studies on phishing susceptibility like any research study strive to strike a balance between data accuracy, ethics, and legality to guide the investigational design. The literature review points to the research of Hale, Gamble, and Gamble (2015), these researchers hypothesized if phishing emails were more complex, they would be harder for individuals to detect, we agree with their assessment and believe complex phishing messages would increase phishing susceptibility. In contrast, Yates and Harris (2015), performed a longitudinal study that concluded phishing attackers continue to rely on the same techniques they have always use to trick individuals because the old methods continue to work. However, their study also showed an increase in the use of phishing detection algorithms as a first line of defense to detect phishing. Table 1 describes the theory elements illustrated by Hale et al. (2015), in their study.

Table 1

Theory elements and sources of theory.

Theory element	Theory	Source of theory
Leakage cues	Interpersonal Deception Theory of Deception	(Buller et al., 1996; Johnson et al., 1992)
Individual prior knowledge	Theory of Deception	(Johnson et al., 1992)
Involvement	Elaboration Likelihood Model	(Petty et al., 1986)
Avoidance behavior	Technology Threat Avoidance	(Arachchilage and Cole, 2011; Liang and Xue, 2009, 2010; Sun et al., 2016)
Attitude change	Protection Motivation Theory	(Rogers, 1975; Vishwanath et al., 2011)

The next section of the literature review will briefly discuss specific theories related to the research model triad, phishing susceptibility, mindfulness and training efficacy.

Elaboration Likelihood Model (ELM)

The use of ELM is beneficial for the identification of phishing by focusing on individual involvement as part of the theory element. Petty and Cacioppo (1986), study of ELM identified two routes to persuasion; central and peripheral routes as described in Table 2. Their analysis implies the peripheral route as being unpredictable which relates to being in a mindless state, while the central route as more predictable and persistent like being attentive and mindful. Additionally, these researchers' study ponders if training efficacy would enable the systematic cognitive processing of information that motivates as a prerequisite to cognitive processing. However, according to Vishwanath et al. (2011), their study found during the central process, an individual is being an active participant in the process of persuasion and diligently considers the information cues through the

process of elaboration. A prerequisite to central processing is the individual's motivation and ability to think about the message and topic (e.g., level of attention).

In contrast to the central processing the peripheral route describes when an end user agrees with the message because the source of the communication appears to be from an expert or is visually attractive. One argument places email message from known individual as messages appearing from an expert or the potential use of colorful graphics embedded in phishing messages to make them more visually appealing. Activate participation assumes the individuals motivated and able to think about the communication and its topics according to (Petty and Cacioppo, 1986). According to the research of Vishwanath et al. (2011), peripheral information processing occurs because individuals make simple inferences about an event based on simple cues such that when the listener decides whether to agree with the message based on a different signal (e.g., trust, credibility) beside what is being seen in the email message. Petty and Cacioppo (1986, p. 21), explain that "attitude changes that result mostly from processing issue-relevant arguments (central route) will show greater temporal persistence, greater prediction of behavior, and greater resistance to counter-persuasion than attitude changes that result mostly from peripheral cues."

According to the research of Petty and Cacioppo (1986), the use of the Elaboration Likelihood Model (ELM) is a key model to identify security education, and awareness training. The ELM model has been used in other fields of study (e.g., consumer research and marketing) as a method to predict attitude changes and can explain the impact online gaming has on security awareness training. ELM explains how "predictable long-lasting behavioral changes can be achieved through cognitive processing" by ensuring the learning task are personally relevant to the learners (Pukakainen and Siponen, 2010 p. 762). Therefore, according to Vishwanath et al. (2011), elaboration describes the process through which individuals make conscious connections between what they observe and their

prior knowledge this connection fits well with increased mindfulness. Finally, ELM can help security awareness training practitioners better understand how and what training methods work, and which training methods have a longer cognitive effect increasing training-efficacy. Elaboration has a connection to mindfulness through the individual's conscious behavior, being aware of their current surroundings to be able to identify phishing activity as described in Table 2.

Table 2

ELM persuasion cues

Elaboration Likelihood Model	Central	Peripheral
Attitude is a key predictor of ELM Characteristics	Motivation	Credibility
Involvement	Authorized sender (authenticate looking)	Typos or Grammar Mistakes
Email load	Individually addressed to end user	Spoofing of legitimate sources
Knowledge	Urgency of message	Embedded Hyperlinks
Computer self-efficacy	Ability/Penalty	Visual appeal
	Justification (incentive or threat) to persuade user to act.	

As described in the literature review of Vishwanath et al. (2011), considers the level of attention individuals give to specific elements presented in email messages (e.g., source, grammar, spelling, urgency cues, and subject line) and the impact they have on elaboration. Similarly, other variables impacting email cues include individual involvement and email load, where also variables could have a direct effect on the individual's likelihood of responding to a phishing email. According to the research of (Vishwanath et al., 2011, p. 580) cites (Zaichkowsky, 1985), defining personal engagement as "the perceived relevance of a particular message or event to an individual." Furthermore, their research had limited explanation on how involvement influences phishing

susceptibility, but motivation by the individuals needing to evaluate phishing susceptibility consciously. Another area found to impact an individual's elaboration is email load regarding the number of emails received daily. According to Vishwanath et al. (2011), study the number of emails received daily reduces an individual's ability to pay attention to key cue areas in the email message thus increasing the individuals' likelihood of responding to a phishing message.

Technology Threat Avoidance Theory

The Technology Threat Avoidance Theory (TTAT) examines training-efficacy related to security awareness training programs and what they teach individuals regarding how to apply filters to email messages. Training-efficacy can include self-identification and analysis of email source, grammar, spelling, urgency cues, and title or subject characteristics. Our study presents TTAT as a theory used to explain IT threat avoidance behavior. Arachchilage and Love (2013), and Arachchilage, Love and Beznosov (2016) studies showed cognitive knowledge of perceived threats can impact the two antecedents of threat appraisals (e.g., perceived severity and perceived susceptibility).

This theory's use is part of the positive feedback loop assisting individuals with avoidance of increasing phishing susceptibility. This theory, "explains the process and determinations of IT threat avoidance behavior across a broad range of IT threats and user sub-samples" (Liang and Xue, 2009, p. 77). Liang and Xue (2009), describe the positive feedback loop as individual going through two cognitive processes to determine their responses to phishing attempts: threat (primary) appraisal and coping (secondary) appraisal. The threat appraisal coping is where users evaluate the potential negative consequences of attacks by phishing emails. But it is this threat that individuals develop a sense of urgency and become motivated to search for and evaluate information related to coping.

The literature identifies two types of coping to deal with threats: problem-focused and emotion-focused. Problem-focused coping refers to adaptive behaviors that take a problem-solving approach to attempt to change objective reality. Problem-focused coping deals directly with the source

of a threat by having the individual implement safeguarding measures for self-efficacy. Measures to execute self-efficacy can include increased mindfulness and the individual's willingness to improve self-training-efficacy. In contrast, "emotion-focused coping is oriented toward creating a false perception of the environment without actually changing it or adjusting one's desires or importance of desires that negative emotions related to threat (e.g., fear and stress) are mitigated" as defined by (Liang and Xue, 2009, p. 78). Therefore, adoption of safeguards to protect individuals from phishing attack is an integral part of the threat avoidance loop process. To lessen the risk associated with phishing susceptibility, individuals need to focus on both problem and emotion-focused coping as seen in the study performed by Sommestad, Hallberg, Lundholm, and Bengtsson (2014), which indicates that threat appraisal is a good predictor of compliance. Thus, an increase in the individual's perceived threat should increase their emotion-focused coping and problem-focused coping.

The final theoretical framework developed for phishing susceptibility is the Integrated Information Processing Model of Phishing Susceptibility (IIPM), (Vishwanath et al, 2011). This model as depicted in Figure 4 below suggests that individuals' respond to phishing related emails based on the content included within the email message, where creation of phishing cues are very persuasive in conjunction with email signatures and the knowing the sender address.

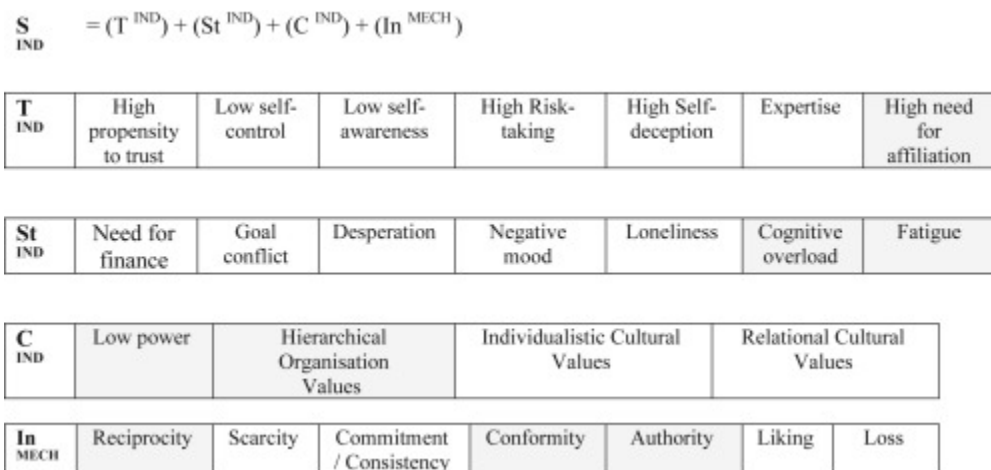


Figure 4 Formula for Susceptibility to Influence

Within this framework Williams et al. (2017), describes a formula for evaluating the possibilities the factors that make up the individual's susceptibility to influence four-factors. Their analysis of the IIPM focused on individual vulnerabilities and how those traits play a part on the individual's contextual level. The message factors may have a greater impact on susceptibility through the interaction of existing vulnerabilities. The table can be used to develop a test range of hypothesis. For example, the In^{Mech} factor included in the Susceptibility to Influence formula takes into consideration the known phishing cues used in phishing messages.

The '*Who*': Individual traits of the recipient, such as personality and risk-preference (T^{IND});

The '*When*': The recipients current state, such as their current mood, degree of self-awareness, cognitive pressure, or fatigue (St^{IND});

The '*Where*': The context an individual is operating in at the time, such as whether they are at home or at work, the communication medium used, and the impact of wider cultural values (C^{IND});

The '*What*': The influence mechanism that is used, such as invoking compliance with authority, instigating a time pressure or appealing to particular emotions (In^{MECH})" (p. 417).

Perceived susceptibility is described as "an individual's subjective probability that the malicious IT will negatively affect him or her, and perceived severity is defined as the extent to which an individual perceives that negative consequences caused by the malicious IT are severe" (Lang and Xue, 2009, p. 80). Furthermore, the researchers described perceived severity as the extent to which an individual perceives that negative consequences caused by malicious IT are severe. Therefore, when an individual believes the risk of receiving malicious information is great only then will they be motivated to reduce the perceived threat. The identification of Threat appraisal is described in the following (e.g., PMT, TRA, and TRM) theories as referenced by (Browne, Lang & Golden, 2015; Cheng, Li, Li, Holm & Zhai, 2013; Li, Zhang and Sarathy, 2010; Shilliar et al., 2015). Based on the literature review we have adopted the following research model to ascertain user Phishing susceptibility.

In our model Mindfulness, phishing susceptibility and training efficacy are dependent variable, measured by independent variables such as gender, age, race and education.

Research Model

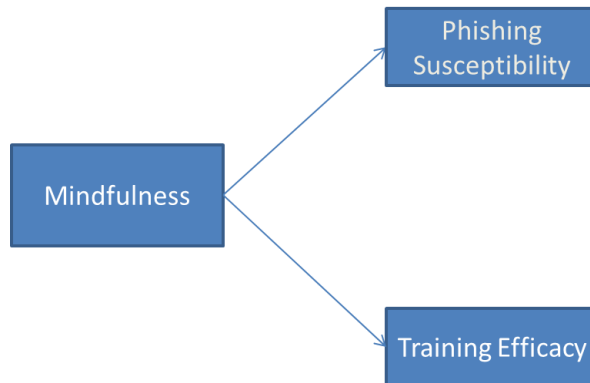


Figure 5 Research Model

Table 3 described the research variables used in our assessment of mindfulness and phishing susceptibility.

Table 3

Research Variables

Variables	Description	Reference
Mindfulness	Is described as a heightened state of involvement and wakefulness of being in the present. Training in mindfulness included new contexts to increase learning. It predicts self-regulated behavior and positive emotional states.	Brown and Ryan (2003); Langer and Moldoveanu (2000)
Phishing Susceptibility	Where an individual falls multiple times for phishing emails, clicks on a phishing URL or provides information on a phishing website. Where individuals fail to identify phishing cues (i.e., authority, urgency, reciprocity, social proof, reward, loss or scarcity)	Downs et al.(2007); Parrish Jr., Bailey, & Courtney (2009);Sheng, Holbrook, Kumaraguru, Cranor, & Downs (2010); Williams et al.(2018)
Training Efficacy	Playing online gaming to increase cognitive abilities to identify phishing cues. Individuals proactively seeking out training opportunities to learn about phishing. General education acquired form college or other technical training.	Canova et al.(2014); Sheng et al. (2010)
Age, gender, online gaming education		

Mindfulness

The literature identified numerous characterizations of mindfulness that addresses the state of being conscious or aware, in the present moment. Two studies Weick and Sutcliffe (2001) and Brown and Ryan (2003), were identified in the literature review discussing mindfulness. The study performed by Weick and Sutcliffe (2001), focused on organizations becoming high reliability organizations or HRO's. While Brown and Ryan (2003) focused on the individuals mindfulness characteristics. Since our study encompassed individuals and not organizations, we used the 15-question survey designed by Brown and Ryan (2003) to gauge how mindful individuals assess themselves using a 6-Point Likert Scale. The questions included in the mindfulness survey are presented in Table 4

Table 4

Mindfulness Survey Questions

Survey Questions	
1.	I could be experiencing some emotion and not be conscious of it until sometime later.
2.	I break or spill things because of carelessness, not paying attention, or thinking of something else.
3.	I find it difficult to stay focused on what's happening in the present.
4.	I tend to walk quickly to get where I'm going without paying attention to what I experienced along the way.
5.	I tend not to notice feelings of physical tension or discomfort until they really grab my attention.
6.	I forget a person's name almost as soon as I've been told it for the first time.
7.	It seems I am "running on automatic" without much awareness of what I'm doing.
8.	I rush through activities without being attentive to them.
9.	I get so focused on the goal I want to achieve that I lose touch with what I'm doing right now to get there.
10.	I do jobs or tasks automatically, without being aware of what I'm doing.
11.	I find myself listening to someone with one ear, doing something else at the same time.
12.	I drive places on 'automatic pilot' and then wonder why I went there.
13.	I find myself preoccupied with the future or the past.
14.	I find myself doing things without paying attention.
15.	I snack without being aware that I'm eating.

Unlike Weick and Sutcliffe (2001), process steps, to gather information from the Brown and Ryan (2003), survey participants they are asked to answer the 15 survey questions on a one to six-point scale. The simplicity of the questions posed by these researchers, approach mindfulness from a mindless lenses of survey question to achieve their mindful conclusion. Our review of the literature generally found individuals with increased mindfulness should be less susceptible to phishing due to their self-awareness versus those individuals who are less mindful.

Training Efficacy

Involvement in the study implied some general understanding (e.g., knowledge and experience) with phishing but it was not considered a prerequisite. Enhancing phishing awareness is described as a “person who defines Phishing correctly” (Alnajim and Munro, 2009, p. 407). Where defining phishing correctly could be the product of formal or self-training, education or experience. A key component of increased knowledge is teaching individuals how to identify more than just the crucial phishing cues (e.g., typos, grammar spoofed hyperlinks and message urgency) and to find the anomalous or deceptive information within a given email message. The literature review identifies various training efficacy methods to teach individuals how to identify phishing to reduce phishing susceptibility. Examples of training include classroom lecture, online course, and self-taught webinars, degrees, and certifications.

Employers have started sending employees fake phishing e-mails to evaluate user susceptibility to phishing and then following up with training (Purkait, 2012). These fake phishing attempts can also measure employee improvements towards phishing detection thus decreasing an individual’s phishing susceptibility. Other studies from Alnajim and Munro (2009), Alsharnouby et al. (2015), Arachchilage and Cole (2011), Arachchilage and Love (2013), Arachchilage et al. (2016) and Hale et al. (2015) identify role play and online gaming as prominent training approaches. Role playing provides individuals with scenarios to choose from, while online gaming a newer method to highlight vulnerabilities without taking individuals to actual phishing websites.

Alnajim and Munro (2009), covered anti-phishing training approaches which concluded individual participants with technical ability in their study showed no increase effect on identification of phishing. However, phishing knowledge had a positive impact on phishing web site detection when training intervention is utilized. In the role-play experiment Alnajim and Munro (2009), had 36 participants view email messages and internet addresses to identify which were legitimate and which

ones were phishing. The basis for their study included three groups; Control, Old Approach, and New Approach groups. During their study, they gave the control group only email from work, while the Old Approach received anti-phishing tips sent by email and the New Approach group received anti-phishing intervening messages. The results of their testing concluded that individuals receiving training intervention treatment had a significantly positive effect regarding detection and understanding phishing.

Meanwhile, online gaming studies according to Arachchilage and Cole (2011) and Arachchilage and Love (2013), are design to educate users to reduce phishing susceptibility. But Downs et al. (2007), shifts attention to the use of role playing to identify individual personality traits like gender, existing phishing awareness, email sender familiarity and other personality traits to increase phishing detection. A second form of online training gaining popularity is gaming, specifically phishing game-based training. This form of training has become a unique way to educate individuals, incorporating mobile devices and home computers to deliver training to detect phishing attacks (Arachchilage and Cole, 2011). The primary objective for developing anti-phishing mobile games is to identify phishing website addresses (URLs), and second to recognize phishing emails by analyzing the content of email messages (Arachchilage and Cole, 2011). Phishing online gaming is “designed to increase users’ avoidance behavior through motivation to protect against phishing attacks” (Arachchilage and Cole, 2011, p. 5).

Early mobile games design principles contained seven structural elements; roles, goals and objectives, outcome and feedback, conflict, competition, challenge, and opposition leading to players’ excitement, interaction, and representation or story (Arachchilage and Cole, 2011). However, Hale et al. (2015), posit that authenticity, repetition, and data accuracy are equally important game features needed when developing a game-platform for phishing. While using the mobile game prototype from

MIT App Inventory Emulator, Hale et al. (2015), performed a usability study of the game prototype to assess the subjective satisfaction of the mobile game prototype interface. Their pilot study recruited eight first-year undergraduate students who took a pre-test, played the mobile game and then a post-test. The pilot study “revealed that the mobile game was effective in teaching participants to look at URLs on their browser’s address bar when assessing a website’s legitimacy” (Hale et al., 2015, p. 190). Additionally, participants of the study scored 49 percent in the pre-test and increased their identification of phishing websites to 78 percent during the post-test after playing the mobile game. Because of the difficulty capturing actual individual actions cognitive theorists like Hale et al. (2015), posit that behavioral intentions are a strong predictor of actual behavior and the use of the mobile game prototype had a significant impact on an individual avoidance motivation.

E-learning has an advantage over other training mechanisms because it provides instant updates, data storage, retrieval and sharing of information and it is delivered via computers using standard internet technology (Omar, Abdalrahim, Drewish, Saeedand & Abdalbagi, 2015). Furthermore, e-learning follows adult learning theory by helping “adults learn by relating new learning to past experience, by linking learning to specific needs, and by practically applying to learn, resulting in more effective and efficient learning experiences” (Ruiz et al., 2006, p. 208). Furthermore, their research found evidence which suggests “e-learning is more efficient because learners gain knowledge, skills, and attitudes faster than through traditional instructor-led method” (Ruiz et al., 2006, p. 208). Figure 6 identifies the four parts of the e-learning equation as described by (Ruiz et al., 2006).



Figure 6 Components of E-Learning

Computer-gaming is gaining fast as an instrument to educate individuals, Ruiz et al. (2006), they assessed 76 studies including medical, nursing, and dental literature with web-based learning, and one-third of the studies revealed knowledge gains. A similar collaborative study conducted by Callaghan, McCusker, Losada, Harkin and Wilson (2013), was successful with inclusion of web-based and virtual worlds (VM) training for electrical engineering students. Researchers like Arachchilage and Cole (2011), are promoting online gaming because it stimulates individuals to pay closer attention and it provides immediate feedback. Furthermore, online gaming offers a better and natural learning environment, by attracting and keeping individual engaged until the end of the game, while providing immediate feedback, unlike reading a book, taking an online class or training in a classroom setting (Arachchilage et al., 2016).

Online gaming as a technique can effectively address data accuracy in phishing awareness, and training appears appropriate to affect learning. Meanwhile, the identification of which anti-phishing training or education is most effective depends on the training method employed by each employer and the learning capacity of everyone. In the study from Arachchilage and Cole (2011), it shows that embedded training works better than current security awareness training practices where sending

security notices to exist. Arachchilage and Cole (2011), used the online game Anti-Phishing Phil in their study to show the effects on participants who played the game were better able to identify fake websites. According to (Callaghan et al., 2013, p. 583), online gaming “as a modern technology is maturing rapidly and reaching the stage where it is sufficiently robust and reliable for wide-scale deployment.” A significant benefit from using online gaming stems from its design and its ability to increase users’ avoidance behavior through motivation to protect against phishing attacks according to the following authors (Arachchilage and Cole, 2011; Arachchilage and Love, 2013; Arachchilage et al., 2016).

Web-based training materials, contextual training, and embedded training are shown to improve users’ ability to avoid phishing attacks (Sheng, Magnien, Ponnurangam, Acquisti, Cranor, Hong & Nunge, 2007). Online gaming is as an alternative to computer based training and other online training methods. Online gaming design has its roots closely aligned with seminal research associated with threat avoidance behavior as found in PMT and TTAT theories. The literature clearly describes the key’s to successfully development of online gaming education tools is to ensure that users are presented with an increased perceived threat perception which will allow the individual to be motivated to avoid phishing attacks and invoke the use of safeguarding measures (Arachchilage et al., 2016). These researchers designed ten URLs with five good worms and five bad worms to teach users how to tell the difference between phishing and non-phishing URLs. A pilot study consisted of eight first-year undergraduate students from a Department of Computer Science and Technology, which revealed the prototype mobile game was effective in teaching participants to look at URL’s on their web browsers to assess the website’s legitimacy. Participants scored 49 percent on the pre-test without playing the mobile game and 78 percent on the post-test after playing the mobile game (Arachchilage et al., 2016). Within their main study, 20 participants were third-year computer science undergraduates

participating in a “think-aloud” experiment to evaluate their understanding of phishing threat awareness through the mobile game prototype. This study measured user subjective satisfaction with the mobile game prototype interface. Results from their study indicated a 28 percent increase in the participants’ phishing avoidance behavior during post-test analysis after playing the online game and achieved an average satisfaction score of 83.62% out of 100 on the System Usability Scale (SUS).

In an example of another online game Anti-Phishing Phil was assessed to educate users on phishing (Sheng et al., 2007). This online game educates users on conceptual and procedural knowledge needed to identify phishing emails and URLs. Sheng et al. (2007), looked at research from learning science for the design needed to establish its interactive environment, specifically related to online gaming. Their analysis found online gaming to be one of the most effective training methods. During the development of the Anti-Phishing Phil game, Sheng et al. (2007), applied three learning science principles: reflection, story-based agent, and conceptual–procedural. The incorporation of reflection aids in “the process by which learners are made to stop and think about what they are learning (Sheng et al., 2007, p. 90). The researchers cite, studies that show cognitive learning increases if educational games include opportunities for learners to reflect on what the individual has learned. Story based agents are defined as “characters that help in guiding learners through the learning process. These characters represent visually or verbally cartoon-like or real-life characters” (Sheng et al., 2007, p. 90). Finally, the conceptual-procedural principle builds on the individuals’ conceptual knowledge and procedural knowledge influencing one another in mutually supportive ways and creating an iterative process (Sheng et al., 2007). Sheng et al. (2007), research indicated 14 individuals were selected to participate in their phishing study to measure the effectiveness of user training. Specifically, this study looked at the false positive (e.g., an individual mistakenly judging a legitimate

site as a phishing site) and false negative (e.g., when a phishing site is incorrectly identified as a legitimate site).

Overall, according to Sheng et al. (2007), the Anti-Phishing Phil study found a significant increase in user confidence levels from 3.72 (variance = 0.09) to 4.42 (variance 0.10) for identifying phishing URLs using online gaming. Although online gaming increases user ability to identify URLs as phishing two particular problems arose; some users still have issues with phishing domains that are like the real ones, and users tend to look less for other clues once they accept the URL as not being suspicious (Sheng et al., 2007).

To further explore the effectiveness of security awareness, Carpenter and Huisman (2016), describe security awareness as a broad range of education, communication, and behavior management activities, with learning outcomes including; compliance with regulations and policy, supporting disciplinary actions, increasing employees' knowledge concerning threats, risks, and security options and changing and maintaining employees' security behavior. Likewise, (Gartner, 2016, n.p.), describes security educations as an "overarching set of activities and objectives that elevates security competence and motivates employees to make security decisions for themselves and the organization that aligns with enterprise security performance objectives and expectations."

The literature describes newer way of providing security education through various intermediaries as described in Table 5. Table 5 provides a description of the most popular third-party training programs identified in the Carpenter and Huisman (2016), study.

Table 5

Gartner Magic Quadrant for Security Awareness Computer-Based Training

Leaders/Content	Quadrant ¹	APBM ²	LMS/SaaS	SCORM	Role-Based	Gamification	Customizable	Phishing Simulation	Phishing Susceptibility
Sans	L	Yes	Yes	Yes		Yes			
PhishMe	L	Yes				Yes			Yes
Wombat	L	Yes						Yes	
Media Pro	L		Yes	Yes		Yes	Yes	Yes	
Security Innovation	L								
Inspired eLearning	L		Yes	Yes	Yes		Yes		
Terranova WW	L						Yes	Yes	
PhishLine	L	Yes	Yes						
Global Learning Systems	L	Yes	Yes	Yes					
The Security Awareness Co.	L	Yes				Yes			
KnowBe4	C	Yes							
Security Mentor	V		Yes			Yes			
Digital Defense	N		Yes	Yes			Yes		

Footnote: L-Leaders, C-Challengers, N-Niche Players, V-Visionaries

Researchers continue to voice concerns that organizations are developing internal security education, training, and awareness programs without regard to proper theoretical grounding or measuring employee existing knowledge and experience (Pukakainen and Siponen, 2010). These researchers posit existing organizational training, must mimic critical awareness training models. When an individual decides whether to open an attachment or not, the individuals assess the threat associated with opening the attachment (e.g., threat appraisal). Research of the literature describes “thinking about the likelihood of the attachment containing a virus or Trojan (vulnerability to danger) and about the seriousness of the consequences that may follow if any malicious content bypasses automated protections (threat severity)” (Shilliar et al., 2015, p. 200). Furthermore, Safa, Sookhak, Solms, Furnell, Ghani, and Herawan (2015), studied Information Security Experts and Information Technology Professionals in Malaysian organizations where 215 questionnaires were used for analysis comprising of answers based solely on their experience and knowledge.

Further review of the literature looked at anti-phishing behavior which refers to ‘choices or actions people usually take against phishing in an Internet environment to avoid becoming its victim’ (Sun et al., 2016 p. 251). As described above there are three behavioral dimensions to anti-phishing Sun et al. (2016), Deletion, Confirmation of Action, and Applying or Learning to Protect. These researchers they describe “Deletion” behavior as an individual using anti-virus software and applying it to anti-phishing scenarios; Confirmation of Action as checking or confirming URL’s and webpage content and Applying or Learning to Protect as the regular implementation of security measures such as blacklisting and password change, against phishing activities” (Sun et al., 2016,p. 252). A reduction in the individual’s susceptibility to phishing the literature maintains coping reasoning must be present. Two studies as referenced by Liang and Xue (2009) and (Yates and Harris, 2015), include training end users to identify critical cues found in phishing messages. In the thirteen-year study performed by Yates and Harris (2015), they found no significant increase between source credibility and the peripheral and central characteristics. Their results only significant event was in a negative direction where more recent messages showed weaker persuasive elements than messages from the earlier test periods. Two assumptions identified in the research according to Yates and Harris (2015), were; existing phishing technical controls phishing algorithms are doing a better job of filtering out more sophisticated attacks, which is likely, or phishing attacker are still relying on the same techniques that they have always used and are not required to innovate their messages to yield better results.

Technical controls

Technical controls are identified as another method useful in the reduction of phishing susceptibility, these controls include countermeasures like (1) URL blacklisting, (2) browser warnings (3) email labeling, (4) web filtering, (5) Single-Sign on, and (6) multi-factor authentication according to (Akhawe and Felt, 2013; Hale et al., 2015; Pompon, Walkowski and Boddy, 2018). However, Shillair et al. (2015), found protection offered by Internet Service Providers (ISPs) regardless of the

amount of automation still requires a significant amount of manual effort from end users. The use of up-to-date ISP web browser tools can assist users in making informed security decisions, but these browsers according to Alsharnouby et al. (2015), are only partially successful in thwarting phishing attacks. One research study indicated that “browser security indicators are misunderstood or ignored frequently, and many users have never noticed them” (Downs et al., 2007, p. 6).

A review of the literature posits individuals appear to have an expectation that their employers or ISP are filtering out all phishing attempts. This perception of security is just an illusion according to Herzberg (2009), regardless of receiving training to detect phishing attacks or not. With more than 3 billion emails sent daily tools like spam Assassin (<http://spamassassin.apache.org>) and DMARC (n.d.), Top phishing attacks: Discovery and prevention (n.d.), are being implemented to filter emails and prevent spoofing of corporate email addresses to reduce the number of phishing emails that reach end-users.

Another alternative method useful in thwarting phishing is URL blacklisting of IP addresses. This tactic utilizes web browsers to reduce phishing attacks, however, studies performed by Akhawe and Felt (2013) and Hale et al. (2015), show URL blacklisting is less effective since an attacker could have an unlimited number of URL addresses within the same domain. Despite that fact, Akhawe and Felt (2013), identified that browsers (e.g., Google Chrome, Mozilla Firefox and Internet Explorer) can utilize Googles Safe Browsing or Microsoft Smart Screens list to identify malware and phishing websites. However, there is also difficulty in using blacklisting due to the number of new phishing URLs discovered daily. During 2014, APGW (2014), reported there were 123,741 unique phishing attacks world wide occurring on 87,901 unique domain names. Fast forward to 2015 and Proofpoint (2016) reported over 900,000 unique phishing websites. Meanwhile, the Webroot 2018 Phishing and

Fraud Report revealed from September 1 to October 31, 2018, 13 of the top 20 fastest growing targets for phishing were financial organizations (Pompon et.al., 2018).

The literature review describes researchers believe that browser security warning messages are ineffective as specified by user clickthrough rates in Table 6. However, according to Akhawe and Felt (2013), the results seen from their testing of clickthrough rates were 18.0% and 23.2% for Google Chrome and Mozilla phishing and malware warning messages. They concluded that clickthrough rates do not appear to impact user behavior. As presented below in Table 6, we illustrate the clickthrough rates from a study of 25,405,944 warning impressions in Google Chrome and Mozilla Firefox May/June 2013. According to Akhawe and Felt (2013), “browser security warnings can be effective security mechanisms in practice, but their effectiveness varies widely” (n.p.).

Table 6

Clickthrough rates

	Google Chrome	Mozilla Firefox
Click-through Rate: n=25,405,944		
Malware	23.2%	7.2%
Phishing	18.0%	11.2%
SSL warnings	70.2%	33%
Safe browsing list	Yes	Yes

In contrast to Chrome and Mozilla, Egelman et al. (2008) and Schechter et al. (2007), studied Internet Explorer’s warning messages regarding to phishing susceptibility. Of the 59 participants in their study, 81% followed the link provided to the suspected phishing website. The study observed participant’s receiving a browser warning messages had only a 79% success rate for those heeding the warning for them and close the phishing websites. Compared to 13% who saw the passive warning messaged and obeyed them according to (Egelman et al.,2008). Furthermore, their study shows browser warning manipulations could decrease habituation (e.g., diminishing attention) and increase the amount of time participants spend viewing warning messages. These researchers believe that

participants did not understand what the warning signs included in browsers wanted them to do, thus, they did not think they were at risk. The central cue to understand phishing behavior is to increase risk perception. A second explanation why browser warnings fail to work centers on the individual's belief that someone other than themselves is bearing the risk (e.g., Internet Service Provider) by filtering email messages. Furthermore, hazard matching is defined as "accurately using warning messages to convey risk, while arousal strength is defined as the perceived urgency of the warning" (Eggleman et al., 2008, n.p.). In their study they found by using different combinations of icons and text participants' risk perceptions is impacted and when habituation sets in, the increase in arousal strength is used to recapture the user's attention reducing habituation.

In the Eggleman et al. (2008), study they experimented with using a spear phishing attack with 106 phishing messages sent to participants. Of the messages sent, the click rate was 94 or (89%) of the phishing messages. Additionally, they found that Internet Explorer (IE) users had more technical experience, were most likely to ignore browser warning messages. In contrast, it was the opposite for Firefox users where those technically experienced users obeyed all warning messages. According to Eggleman et al. (2008), their study posits that warning messages regardless of the browser should grab the user's attention by interrupting their immediate task and force the user to choose one of the options presented in the warning message. Second, effective warning messages must cause attention maintenance – grabbing the users' attention long enough for them to attempt comprehension. Finally, the results of their study found a "significant negative correlation was found between participants recognizing a warning message and their willingness to completely read it" (Eggleman et al., 2008, n.p.). Therefore, if a warning message is known a user is significantly less likely to read it entirely so in the case of high-risk area warning messages must be designed differently than other less severe warnings to increase the likelihood of the message being read.

Individuals look to their ISP and Internet browsers for protection from phishing attacks. But according to the Akhawe and Felt (2013), their study launched a phishing attack on 30 individuals during a role-playing experiment. The experiment included watching how participants interact with the security toolbar display passive phishing warning messages. Their research indicated that even with the notification of phishing browser warning messages 20 out of the 30 participants were fooled by at least one phishing attack. In a second experiment 10 participants performed a task on PayPal and a shopping wish list website, the testers injected model phishing warnings into the website, and none of the participants fell for the phishing link, requesting them to enter their PayPal credentials. Still, four participants incorrectly entered information on the phishing shopping wish list website. Egelman, Cranor and Hong (2008), looked at active and passive browser warning messages according, and concluded that participants spend more time reading the warning messages, but did not behave any differently, demonstrating that warning messages do not correctly align with users' risk perceptions.

Additionally, Herzberg (2009), identified three primary browser indicators (e.g., URL and the location bar and security icons like the padlock) and posit why individuals fail to appropriately identify phishing attacks. Their experimentation found "users often enter their password without validating that SSL/TLS is active and that the URL is correct" (Herzberg, 2009, p. 65). Additional researchers found where individuals appear overconfident when presented with familiar looking websites that they have existing knowledge of, thus spending less time distinguishing whether the website is legitimate or not (Alsharnouby et al., 2015). According to Hoban et al. (2014), security warning messages only define the problem and do not offer actionable task users can take to prevent the current or future occurrences. Because of this absence of action researchers like Shillair et al. (2015), posit that careful targeting of security warning messages to the audience based on their knowledge level would be beneficial to improving user self-efficacy and personal responsibility.

To further evaluate browser security warning messages Schechter, Dhamija, Ozment, and Fischer (2007), gave 60 participants fake site-authenticating images and 57 participated got warning-page attacks. The results of this research disclosed 97% of the participants failed to detect the false site-authenticating images. Meanwhile, 30 out of the 57, (53%) who received warning messages proceeded to enter password information. The researcher's analysis found participants paid less attention to the warning page and other indicators because the focus of the study was on site-authenticating images.

A key learning objective of this section is to teach individuals how to identify phishing emails and websites to better prepare individuals with the knowledge and skills to decrease the false positive detection rate. In combination with reading warning messages Alsharnouby et al. (2015), performed an eye-tracking movements experiment. They sampled 24 college university participants. The individuals taking part in the study looked at Areas of Interest (AOI) for websites designed for use in the research study to determine eye movement while examining browser content. According to testing performed by Alsharnouby et al. (2015), a significant correlation exists between the time participants spent looking at the chrome browser and performance scores. Their results, "suggest that the more time spent observing chrome, and the chrome AOIs in particular, led to an increased ability to correctly assess the legitimacy of websites" (Alsharnouby et al., 2015, p. 77). Furthermore, these researchers' found eye-tracking data shows users irregularly notice changes in information located in the chrome browser such as changing URLs and failed to understand the differences even when observed. A key outcome according to Alsharnouby et al. (2015), found eye tracking took participants on average 87 seconds to decide whether a website is real or fake.

Summary

The review of literature reveals there is no silver bullet type of training or level of education that can provide individuals with the absolute capacity to identify phishing. In general, the use of

automated checks to thwart phishing is only the first layer of defense needed to reduce phishing susceptibility. In general, the use of grounded theories (i.e., PMT, TTAT, ELM) are vital to understand the type of behavior modifications that cognitively influence user avoidance behavior. A specific cue requires individuals to have an increase in perceived threats and increased risk to force individuals to invoke protection coping strategies. Secondly, the next layer of defense includes expanding an individual's knowledge of phishing cues (i.e., authority, urgency, reciprocity, social proof, reward, loss and scarcity), as described by William, Hinds and Johnson (2018), and through security education practices that improve cognition and have a more lasting effect. Modifying browser warning messages and educating individuals to identify phishing cues will allow people to ascertain if any phishing attacks can be identified if they make it through automated filters. Various phishing education practices are in use today (e.g., CBT, role-play, classroom) but online gaming provides the necessary mechanisms to improve an individual's knowledge, experience, and training self-efficacy. The key conclusion identified in this research study and linked to other research studies is that individuals need to feel threatened by phishing attacks before they will invoke their threat perception to allow themselves to avoid threats. Therefore, online gaming modifications to training individuals to detect phishing must ensure that individual have increased perceived threat perceptions to trigger the necessary safeguards for protection from phishing.

Chapter 3

Research Methodology

Research Design

To answer the research questions, the following research design was employed to investigate whether there is any correlation between mindfulness and phishing susceptibility between cyber and non-cybersecurity groups exist. A sample population of cybersecurity and non-cybersecurity individuals were studied. Purposive sampling was conducted limiting cybersecurity individuals to those with cybersecurity affiliations, education and experience. The cross-sectional survey was performed utilizing the Mindfulness Attention Awareness Scale (MAAS) quantitative instrument developed by Brown and Ryan (2003). The survey questions were used to measure mindfulness and phishing susceptibility, and nominal survey responses were gathered to make correlations between mindfulness groups.

The objective of the study was to achieve completion of 150 surveys from cybersecurity individuals and 50 from non-cybersecurity individuals. Our survey was provided to the two groups using Survey Monkey's online survey tool to gather data for statistical analysis.

Research Questions

The following research questions are relevant to this study of individual mindfulness.

RQ1: Is there a statistically significant correlation between mindfulness and phishing susceptibility?

RQ2: Do cybersecurity professionals differ significantly from non-cybersecurity individuals statistically in their mindfulness and phishing susceptibility?

Data Necessary to Answer the Research Questions

The data needed to answer the research questions was collected using a survey-based instrument as found in the study conducted by (Brown and Ryan, 2003). The author gathered survey responses from individuals from two groups, North Central U.S. Cybersecurity practitioners and non-cybersecurity individuals. Cybersecurity practitioners were selected because that group was shown through literature review to be an understudied group. Additionally, the author wanted individuals that were not focused on large technical companies as found on the west coast or primarily governmental employees associated with the federal government. After announcing the survey at cybersecurity chapter meeting over a four-month period the author obtained 121 completed surveys from cybersecurity professionals. Additionally, a second survey was created and posted to Survey Monkey and obtained 37 non-cybersecurity individuals that completed the survey over a two-week period. All surveys received were accurately completed for the Mindfulness section and used in our analysis.

The online version of Brown and Ryan's (2003) mindfulness questionnaire was only available through use of the Survey Monkey application, answering question online required a response to each question before the individual could proceed to the next survey question. A copy of the survey questions is available in Appendix B. The MAAS scale measures the dispositional mindfulness range describing how participants report their believed level of awareness referenced by each item on a 6-point Likert scale (1 = "almost always" to 6 = "almost never) where higher scores reflected individuals having assessed themselves as being more mindful.

Instrument Development

The following section will address the type of instrument developed and methods used to provide validity and reliability to the study. Our main instrument is the mindfulness survey developed by (Brown and Ryan, 2003). This survey was selected for simplicity of use and the framing of the mindless question to elicit a mindful response from participants.

Reliability

Reliability is the degree to which a test consistently measures whatever it is measuring (Gay, Mills and Airasian, 2009). Reliability expresses consistency of the scores produced within any research study. The reliability of our research study will be assessed for internal consistency, to measure the extent which items in a test are like one another in content. Thus, using Cronbach's Alpha value of .893 indicates a high degree of internal reliability in our participant responses on our Likert based survey instrument. Reliability of the survey instrument does not depend on the instrument's validity alone. Thus, we calculate the Alpha value as another widely used method in research analysis. Typically seen in research studies as the estimate of reliability increases, the error rate associated with test scores should have the opposite effect and decrease.

Validity

Validity is seen as another critical component of any research study because it communicates the appropriateness of the selected test being performed. Our study proved validity in several ways, such as utilization of the Mindfulness Attention Awareness Scale (MAAS) survey test purposely for self-identification of mindful behavior. Validity of our survey is based on concurrent validity correlating the two sets of responses. The use of a survey for our analysis continues to be a consistent methodology because of the survey's external validity (Steiner et al., 2016). Because the survey questions are not biased and are easily replicated to other research studies the output from the survey has a legitimate and realistic perspective.

Population and Sample

The author initially reached out to various North Central U.S. Cybersecurity practitioners through their affiliation with Certified Information Systems Security Professional (CISSP) organizations and InfraGard. A total of 1,400 individual were members of the organizations. In the

second part of our study the author engaged non-cybersecurity individuals through social media post and email communication to elicit their participation.

Data Collection

During the data collection phase, the author utilized a web link to the online Survey Monkey site, which was sent to participants through email, social platforms, text, hard copy distribution and twitter post, where each participants was asked to give informed consent to participate in the study.

Prior to conducting the study or interacting with participants, the author was required by Nova Southeastern University to obtain approval from the Institutional Review Board (IRB). CITI training was initiated and completed by the author May 2017. Shortly, after IRB approval the survey instrument was communicated to potential individuals. Upon gathering individual to complete the survey each participant was informed their identity would be kept confidential in accordance with the university's Institutional Review Board (IRB) consent procedure. In addition to, maintaining anonymous responses to the survey questions. No explicit harm physically or emotionally would harm participants of this study. While their explicit agreement to participate would be identified by indicating "yes" on the survey their agreement to participate. The identity of the participants was kept confidential and only the college student had their identity disclosed to their professors for the extra credit attained for participating in the study.

Data analysis

Analysis of data in a causal-comparative study such as this one involves a variety of descriptive and inferential statistics. Analysis of demographic such as (Age, Gender, Race and Education) were performed utilizing descriptive statistics including mean (i.e., the average performance of a group on a measure of some variable), and standard deviation (i.e., the spread of a set of scores around the mean). Inferential statistics such as Spearman rho correlation is useful for answering research questions associated with Sociology, Medicine and Business and was the right fit

for our analysis to determine if there is a statistically significant correlation and Analysis of Variance (ANOVA) for data correlation. The purpose of the investigation was to determine if correlations between cyber and non-cybersecurity groups exists. The author used ANOVA test to assess for differences between two or more means. A score of 0 explains none of the variability of the response data around its mean. A 100% indicates that the model explains all the variability of the response data around its mean.

Step 1

Was to assess with a Box's Test of Equality of Covariance matrices of the dependent variables are equal across groups.

Step 2

Perform a review of the authorized squared established correlations to ensure that function 1 contributes to successful classification. Using Wilkes Lambda, this should provide the author with statistical significance. For our study, only one function was evaluated and proved significant in the groups.

Step 3

The author utilized the cross-validation output in SPSS to review the percentage of originally grouped cases that are correctly classified. The researcher should decide if the percentage is large enough to be considered correctly classified. With the standardized established authorized discriminate function coefficients and structured matrix should also be reviewed to determine viable classification of data. Each group of participants completed the online mindfulness survey maintained on Survey Monkey.

Step 1: Build the data set

To perform analysis of the data the researcher used the Statistical Package for the Social Sciences (SPSS) software to manipulate the collected data. All mindfulness responses were ordinal ranging from 1 – 6 and required no normalization.

Step 2: Run the data in SPSS

The second step in our analysis was to tabulate the score for each question to compute the mean for each participant of the mindfulness survey. The author produced the total score for the subject's level of mindfulness, this figure became our independent variable in our study and was further used in our ANOVA analysis.

Step3: Analysis of output

Resource requirements

The resources the researcher required to conduct this study were gathered online using Survey Monkey. A total of 158 participants responded to the mindfulness survey questions. Question asked helped to normalized scores for their level of mindfulness on the 15 question from the MAAS survey. The data collected made correlations about the level of mindfulness and its relationship to select dependent variable research possible. The researcher used Statistical Package for the Social Sciences (SPSS) software, commonly used in data analytics, to analyze data for covariance.

Summary

This chapter describes the research methodology for this study, sample methodology utilizing random purposive sampling limiting the research to cybersecurity professionals and non-cybersecurity individuals. The data collection methodology included gathering data through an online survey instrument with 15 questions designed by (Brown and Ryan, 2003). Data analysis included a variety of descriptive and inferential statistics such as demographic mean and standard deviations. While inferential statistics such as Spearman rho and Analysis of Variance (ANOVA) were utilized to evaluate for data correlations.

Chapter 4

Results from Survey Analysis

Introduction

The results from the analysis of the research study are presented in this chapter. The data collected by the researcher is described as well as methods used to statistically evaluate the data collected. What our data analysis describes is whether there is a relationship between mindfulness, phishing susceptibility and training efficacy, based on the Brown and Ryan (2003) mindfulness scale. The study concentrated on two groups, cybersecurity practitioners and non-cybersecurity individuals and any relationship between the two groups. Demographic data was obtained and is displayed in table 7 below showing participant age range, gender, education and race. All data in the study is presented quantitatively, concluding with a summary of the data results.

Data Collection

The author surveyed cybersecurity professionals from three North Central US Information Security groups. The researcher targeted the 918 members from the Information System Security Association (ISSA), 424 members from the Information Security MBA group, and 454 members from North Central US InfraGard. Solicitation of participants occurred over a four-month period with the researcher announcing the study during monthly InfraGard, ISSA and Security MBA chapter meetings. Follow up reminders were also sent via LinkedIn and Twitter to remind the population of the survey participation request. The cybersecurity sample included 119 cybersecurity specialists. A second group of non-cybersecurity individuals were included in the study to differentiate cybersecurity

versus non-cybersecurity individuals. Our non-cybersecurity sample came from two U.S. college's and comprised 36 students and two professors, giving our study a total sample (n=157). To obtain a better picture of the population the respondents were asked additional questions on the survey to assess their phishing knowledge and demographic grouping's such as gender, education, race and age factors as described in Table 7.

Sample Population

Survey responses were received using Survey Monkey, that captured a final sample of (n=157), 128 males and 28 female participants, one person failed to indicate gender in their survey response as seen in Table 8. The online survey did not have any validation requirements set for responses to demographic information. Our analysis identified significant differences in gender based on the initial assessments of the cybersecurity group that had 105, 86.8% men and 15, 12.4% women identified. Based on researcher observations of the cybersecurity field this difference between men and women is a quite common occurrence for this practitioner field of study. However, the researcher found no significant differences identified between the non-cybersecurity group with 23 male and 14 female participants and the one participant failing to supply their gender.

Table 7

Demographic Statistics

	Cybersecurity	Non-Cybersecurity	Total
<i>Gender</i>			
Male	105	23	128
Female	15	13	28
Missing		1	1
<i>Age</i>			
18-20	0	2	2
21-29	10	25	35
30-39	29	7	36
40-49	35	2	37
50-59	28	1	29
60 and above	14		14
Missing	1	2	3
<i>Race</i>			
White/Caucasian	104	16	120
African American	5	11	16
Asian	0	5	5
Hispanic	4	1	5
Multiple Races	0	3	3
Coloured	6	1	7
Some other race	1		1
<i>Education</i>			
High School/GED	2	3	3
Some college no degree	17	22	39
Associate degree	7	5	12
Bachelor's degree	60	6	66
Graduate degree	34		34

Additional significant differences between the two groups were found regarding age and education. The statistics show cybersecurity professionals are highly educated with 78% holding bachelor and graduate degrees while non-cybersecurity individuals are high school graduates and had some college. The age comparison aligned with education where cybersecurity specialist was significantly grouped at 88%, at age 30 and above, while the non-cybersecurity individuals had 75% between the age of 18 – 29, primarily still attending college or recently graduated. Our final comparison looked at race between the two groups and identified white males $n = 120$ or 76% of the sample, dominating both groups and only African Americans from the non-cybersecurity group make up 29% were significant. All other race groups were not statistically significant in our study.

Education within the cybersecurity group recognized 104 of the 120 participants had a bachelor and a significant group had graduate degrees.

Participants completed the MAAS survey on a 6-point Likert scale from 1 (“almost always”) to 6 (“almost never”), where higher scores reflected individuals having assessed themselves as being more mindful. Participants answered the questions according to what “really reflects” their experience rather than what they think their experience should be. Scoring involved calculating mean scores for each of the 15 questions as well as each participant's MAAS score across the 15 questions. The MAAS scale as showed in the research of Brown and Ryan (2003), measures the dispositional mindfulness range describing how participants report their believed level of experience referenced by each item on a 6-point Likert scale from 1 “almost always” to 6 “almost never.” Table 4 presents the 15 MAAS items included in the MAAS survey. According to the analysis performed by Brown and Ryan (2003), they computed a MAAS score ($M = 4.20$), Standard Deviation ($SD = .69$), while our initial cybersecurity group had a MAAS score ($M = 4.15$), Standard Deviation ($SD = .75$) and the non-cybersecurity group had a MAAS score ($M = 4.05$), Standard Deviation ($SD = 1.47$).

Based on analysis of the research questions the focus of this research is to see if mindfulness correlates with phishing susceptibility and if there is a difference between the mindfulness of cybersecurity professionals and non-cybersecurity individuals. The next section will detail the results of our analysis for each of the measured variables (i.e., Mindfulness and Education) and any interaction effects with other nonequivalent dependent variables. The computed reliability statistics for the 15 items from the MAAS Survey instrument produced a Cronbach's Alpha of .893, which indicates a high degree of internal reliability in our participant responses.

Initially, we performed testing using Levene's Test of Equality of Error Variances to determine Homogeneity of Variance, as described in Table 8. Our analysis discovered where $F(1, 72) = 1.617$, p

= .245, partial $\eta^2 = .022$, observed power = .068. Resulting in a Levene's computed significant value of .072 which is greater than .05, thus the two variances are approximately equal.

Table 8

Levene's Test of Equality of Error Variances Mindfulness

Levene's Test of Equality of Error Variances ^{a,b}					
		Levene Statistic	df1	df2	Sig.
MindSc	Based on Mean	3.341	1	74	.072
	Based on Median	2.740	1	74	.102
	Based on Median and with adjusted df	2.740	1	70.069	.102
	Based on trimmed mean	3.290	1	74	.074

Tests the null hypothesis that the error variance of the dependent variable is equal across groups^{a,b}

a. Dependent variable: MindSc

b. Design: Intercept + Group

Additionally, we performed a Levene's Test of Equality of Error ANOVA analysis of the dependent variable education, we computed a significant value of .245 which again was greater than our p-value of .05, as identified in Table 9.

Table 9

Levene's Test of Equality of Error Variances Mindfulness

Levene's Test of Equality of Error Variances ^a				
Dependent Variable: MindSc				
F	df1	df2	Sig.	
1.375	1	73	.245	

Tests the null hypothesis that the error variance of the dependent variable is equal across groups^a

a. Design: Intercept + Education + Group

Continued analysis between the two groups began with running an Analysis of Variance (ANOVA) to examine the significant mean difference among the two groups on an interval dependent variable. We observed in our calculation of the ANOVA an extremely low R-squared value = .097, so we elected to run a post-hoc analysis that examined the effect of education as a covariate as described

in Table 10. For our test of ANOVA on Mindfulness we selected a random sample of 39 out of the 121 cybersecurity individuals who completed the Mindfulness survey and 37 of the non-cybersecurity individuals to evaluate covariance. To effectively carryout our analysis of the nonequivalent dependent variable we initially examined the difference between group means to see if they are statistically significant. The Corrected Model Mean scores as reported in Table 10 denotes a Mean Square = 4.535 and exhibits a statistically significant degree ($F = 7.913, p = .006$). Examination shows the computed P-value $.006 < \alpha = .05$, thus rejecting the null hypothesis and concluding not all the population Means are equal, but some of the means are statistically significant between the cybersecurity and non-cybersecurity groups.

Table 10

ANOVA Mindfulness Score Test of Between Subjects Effects

Dependent Variable: MindSc Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	4.535 ^a	1	4.535	7.913	.006	.097
Intercept	1212.389	1	1212.389	2115.330	.000	.966
Group	4.535	1	4.535	7.913	.006	.097
Error	42.413	74	.573			
Total	1264.085	76				
Corrected Total	46.948	75				

A Computed using alpha = .05

We performed additional investigation using the ANOVA to reduce our error variance within our sample. The examination included a sample of 39 cybersecurity and 36 non-cybersecurity individuals for a total population of 75. After performing the ANOVA our analysis ascertained a slight error rate reduction, the ANOVA went from 42.413 to 38.399, while the total variance remained virtually unaffected. Table 11 describes the ANOVA analysis for the impact of education on reducing

the error rate. The resulting ANOVA analysis explains that education did have an effect, a two percent impact but not a significant impact on the variation of the data.

Table 11

ANOVA Mindfulness Score Test of Between Subjects Effects of Mindfulness

Dependent Variable: MindSc Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	4.488 ^a	2	2.244	4.207	.019	.105
Intercept	52.767	1	52.767	98.940	.000	.579
Education	.862	1	.862	1.617	.208	.022
Group	.087	1	.087	.164	.687	.002
Error	38.399	72	.533			
Total	1260.085	75				
Corrected Total	42.887	74				

To determine the strength of association between Mindfulness and Phishing scores we performed analysis using Spearman *rho* Correlation as described in Table 12. We elected to perform the Spearman correlation over Pearson's *r* because one of our variables (i.e., Phishing Score) is ordinal and the data is not normally distributed. Additionally, Spearman's correlation was useful for answering research questions associated with Sociology, Medicine and Business and was the right fit for our analysis to determine statistically significant correlations between mindfulness groups.

Table 12

Spearman's rho Correlation

		MindSC	PhishSC
Spearman's rho	MindSC	Correlation Coefficient	1.000
		Sig. (2-tailed)	.
		N	37
	PhishSC	Correlation Coefficient	.261
		Sig. (2-tailed)	.118
		N	37

Based on the evaluation of our research question whether there is a statistically significant correlation between mindfulness and phishing score the significant Spearman correlation coefficient value of ($r_s = .261$, $n = 37$, $p > .118$) for Mindfulness and Phishing scores both have a “weak” association (.20 - .39) according the coefficient guide for the absolute value of r_s scale. Therefore, indicating that no significant correlation between mindfulness and phishing scores exists.

Summary of Results

The objective of this analysis performed was to answer the research questions that allowed the researcher to draw conclusions based on the data analysis.

Statistical results of the research questions.

RQ1: Is there a statistically significant correlation between mindfulness and phishing susceptibility?

Statistical results of the research questions show's a computed P-value $.006 < \alpha = .05$, thus rejecting the null hypothesis and concluding not all the population Means are equal, but some of the means are statistically significant between the cybersecurity and non-cybersecurity groups.

RQ2: Do cybersecurity professionals differ significantly from non-cybersecurity individuals statistically in their mindfulness and phishing susceptibility?

Statistical results of the research questions indicated a slight reduction from 42.413 to was 38.399, but not significant.

Chapter 5

Conclusion, Implications, Recommendations, and Summary

Introduction

The main goal of this study was to better understand the role mindfulness plays in a user's detection of a phishing message and to discover if there exists a difference in mindfulness between those individuals whose primary job role is to detect security exploits such as phishing and those that have other primary job roles. This chapter begins with a brief discussion of the conclusions reached through statistical analysis and interpretation of the data collected in chapter 4. This chapter concludes with the implication of the usefulness of incorporating mindfulness into phishing detection and recommendations for actions to further incorporate mindfulness into the cybersecurity field.

Conclusions

This study focused on the use of mindfulness as an antecedent to measure phishing susceptibility between cybersecurity and non-cybersecurity individuals. This study's creation centered on whether there was a correlation between mindfulness and phishing susceptibility among cybersecurity and non-cybersecurity individuals. Based on the analysis of the responses to the mindfulness survey questions a correlation between the groups appeared imminent. However, having a diverse set of factors reduce the noise allowing the researcher to focus on mindfulness. There appeared to be no significant differences between the two groups regarding phishing scores thus we posit that this is due to becoming familiar with identifying the phishing exploits. Future research should use different phishing exploits for testing of phishing susceptibility. However, difference between groups were identified based on education, race, gender and age demographic information, thus clearly

finding no correlation between groups regarding mindfulness and phishing susceptibility. This study focused on two research questions:

1. Is there a statistically significant correlation between mindfulness and phishing susceptibility?
2. Do cybersecurity professionals differ significantly from non-cybersecurity individuals statistically in their mindfulness and phishing susceptibility?

Initially the researcher sought to identify whether correlations existed between self-reported mindfulness scores and how susceptible and individual could be to phishing. The identification of how aware an individual might be regarding their surroundings and if that awareness translates into lessening their phishing susceptibility. Secondly, difference was observed between the cybersecurity and non-cybersecurity groups, the effect of our statistical analysis indicates there seems to be a relationship between the cybersecurity and non-cybersecurity groups based on their mindfulness scores. Utilizing the Brown and Ryan (2003), mindfulness questionnaire, we computed a cybersecurity MAAS score of 4.15 and for non-cybersecurity MAAS score of 4.07. Additionally, there also seems to be a relationship between a person's mindfulness and their choice of cybersecurity as a career. Therefore, another explanation for the results received in our statistical analysis focusing on cybersecurity, education and mindfulness could be explained by the number of individuals within that field of study with advanced degrees versus non-cybersecurity where no individuals had advanced degrees and a small group had bachelor's degrees. The analysis related research question 1, might be impacted by the fact that most individuals included in our survey had familiarity with the characteristics of phishing and, therefore, being mindful is not as significant as other cues associated with phishing and cybersecurity.

A significant emphasis seen among the cybersecurity practitioners is the necessity of having more education to acquire a cybersecurity position. In contrast, the non-cybersecurity group is predominately filled with college students perusing their initial bachelor's degree. Furthermore, there is also a significant difference in the age of individuals working in cybersecurity versus individuals included in the non-cybersecurity group. Whether the dependent variable is an additional driving factors for their education and career, or a result of these factors is something else, that will have to be examined in future research. Finally, our choice of instrument may also have impacted the analysis, such that individuals are likely to be more mindful while taking the assessment than they would be in an actual workplace setting. Thus, the researcher postulates more investigation is necessary using other areas of phishing and cybersecurity to determine the true nature of the relationship (if any) between mindfulness and phishing susceptibility.

Implications

There are several implications that can be derived from the findings of this dissertation. The primary implication identified from the analysis of the data found descriptive data such as demographic information as a primary factor for difference between cybersecurity and non-cybersecurity individuals. Specifically, one must look at the age and education differences between the two groups. Almost 90% of the cybersecurity individuals were above the age of 30, while 75% of the non-cybersecurity individuals were between the age of 18 – 29. This age difference also equated to the difference seen in education between the two groups, 78% having bachelor and graduate degrees for cybersecurity individual and only 16% of the non-cybersecurity individual having a bachelor's degree.

The research study is different from other studies with the inclusion of mindfulness to measure whether correlations exists between cybersecurity and non-cybersecurity individuals. Specifically, the research targeted individuals who are information security practitioners and belong or participate in a professional information security group. The inclusion of mindfulness suggests that more mindful

individuals are more aware of their surroundings and have increase cognitive capabilities. Therefore, by having increased cognitive skills, the information security practitioners would be less susceptible to phishing. Broadening implications associated with this study, include contributions to the body of knowledge by using mindfulness as a measure between cybersecurity and non-cybersecurity groups.

Recommendations for Future Research

Based on the analysis derived from the study the researcher recommends using mindfulness as a basis to gauge participant awareness and inclusion of additional survey questions about phishing to explore the individual understanding of phishing techniques and how to detect them. Future research should identify if individuals with higher mindfulness scores had higher education, received on the job training for phishing and at what level, and finally identify what drove them to work within cybersecurity. Based on the quantitative results of the research study adding additional online game training is critical to advance the cognitive understanding of how to reduce phishing susceptibility among all groups. With improved education and awareness, individuals will become armed with additional detection techniques, beneficial to both corporations and the individual to detect phishing attacks that by-passes automated detection mechanisms.

Finally, the researcher also sees the necessity for having larger sample sizes included in the research to improve the analysis obtained to better identify correlations between groups and their self-assessment for mindfulness.

Future studies should also combine the use of manipulation of browser security warning message morphing with online game training to assess whether the automated manipulated messages coupled with online game training improves cognitive functions to identify phishing cues. Furthermore, future studies should incorporate automated browser warning messages as an additional factor to assess URL appropriateness by allowing participants to see the URL, invoke the warning and then see if online gaming training will aid as an additional filter to increase phishing identification.

Another avenue for future studies should make comparisons of online game training results between cybersecurity and non-cybersecurity groups. In addition to, requiring feedback from participants and providing immediate feedback on their responses to phishing could also increase coping behavior. Additionally, future studies should also focus on measuring the effectiveness of corporate online phishing education as well as concentrating on incorporating employee pre-existing knowledge and experiences with phishing into security awareness training.

Summary

The research study is a closed questionnaire that used a Likert scale to gather responses from participants regarding self-identification of mindfulness. The research study includes two groups addressing the 15-questions as described in the MAAS questionnaire developed by (Brown and Ryan, 2003). The sample selected came from a pool of cybersecurity practitioners from North Central US who were also members of a local information security groups (e.g., ISSA, InfraGard or another security group). Through the mindfulness questioning of the research study, a sample of 121 cybersecurity practitioners completed the 15 MAAS survey questions to assess their level of mindfulness. The second sample was selected from a pool of non-cybersecurity individuals and the same MAAS 15 mindfulness questionnaire was administered. Within the second sample group only 38 completed MAAS questionnaires were obtained.

The goal of this research is to better understand the role that mindfulness plays in a user's detection of a phishing message and to discover if there exists a difference in mindfulness between those people whose primary job role is to detect security exploits such as phishing and those that have other primary job roles.

The modification of employee cognitive behavior assists with coping strategies and avoidance of increased phishing susceptibility. With continued phishing attacks against corporations and individuals, organizations need to strike a balance between automated and manual detection programs

that assist in the reduction of risk from phishing. Globally, the number of identified phishing attempts does not appear as slowing down and continues to rise year over year thus prompting organizations and individuals to take steps to protect themselves. Additionally, despite increased spending on technological advancements, phishing remains a top attack vector costing corporations billions of dollars in damages. Notwithstanding, the use of automated detection and preventive controls, researcher still classify individuals as the weakest link (Alsharnouby et al., 2015). Therefore, the problem seen with phishing can be correlated with end-user cognitive behavior.

A review of the literature cites multiple occasions where phishing attacks were successful; the U.S. Internal Revenue Service and The National Bank of Blacksburg to name a couple of incidents. During the IRS attack, taxpayers' refunds vanished without a trace. Meanwhile, The National Bank of Blacksburg attack lost more than \$569,000. Furthermore, RSA Monthly Online Fraud Report (2014), reported 450,000 phishing attacks, resulting in over \$5.9 billion in losses during 2013. Lastly, InfoWorld reported seeing 6.3 million phishing emails during the first quarter of 2016. Phishing is and continues to be a growing problem such that the Anti-Phishing Working Group (APWG) saw an average of 70,000 phishing sites popping up monthly during the first three quarters of 2015. Due to the continued proliferation of phishing emails and URL's combined with the current overabundance of daily email messages a strain has appeared for corporations and individuals to identify legitimate versus nonlegitimate email messages. To emphasize the significance of the problem the research on phishing also shows individuals receive limited instruction on how to prevent or identify phishing even after participating in corporate information security awareness training.

Research theorist studies point to an individual's perception of phishing being rooted in their existing knowledge and experience that is usable for predicting behavioral responses to phishing attacks (Down et al., 2007). Specifically, having technical knowledge of web environments could

increase the individual's resistance to phishing attempts (Alsharnouby et al., 2015). A review of the literature states that when individuals know more about phishing, they significantly reduced their likelihood of falling for phishing (Downs et al., 2007). However, the authors of the SC Magazine (2015), called this low-security knowledge the "greatest inhibitor to defending against cyber threats" (p. 1). With the proliferation of phishing attacks, multiple research studies explored ways to address how corporations and individuals can reduce the phishing attack surfaces. Studies seen in the literature review include; general decision strategies, online gaming design, technical browser security warning messages, polymorphic warnings, and enhanced security awareness messaging.

As awareness increases personal awareness and taking ownership after falling for phishing attempts must resonate with individuals, but the research excludes any specific analysis on consequence upon falling for a phishing attack. When individuals lack attention it may contribute to their over-reliance on organizational automated information security tools to detect phishing attempts. Regardless, corporation's exhibit positions of having a low confidence level toward successfully recognizing phishing through automation (Proofpoint, 2016).

Part of the research study included addressing how individuals react to being phished. The three phases of phishing that organizations can implement as part of their awareness training components include; denial, attention to avoid and action. Adaption of these phases can help move individuals from mindless to mindful and can improve cognitive behavior to reduce phishing susceptibility. Corporation and individuals must understand that phishing has no boundaries, it's a global problem impacting all industrialized countries resulting in billions of losses. Multiple types of phishing attacks exist (e.g., Vishing, Smishing, Spear-Phishing, Whaling, etc.) succeed because phishers cause users to respond to some action that is to the advantage of the attacker by tricking the end user into clicking on a fictitious website or installing malware by appealing to an individuals'

efficacy, urgency and order. Therefore, beyond the use of automated controls to detect phishing individual must realize they are the last line of defense and arm themselves with the best information to safeguard corporate and their personal assets.

Research studies have identified various automated methods to address phishing, starting with the Internet Service Provider (ISP) who provides mechanical security detection technology. Additional studies found that discuss combating phishing include browser morphing, browser alerting, eye tracking movement, and security awareness training. Meanwhile, technical countermeasures include blacklist filtering, user interface assistance, and taking down and blocking known phishing sites. However, none of the automated or technical controls alone can thwart every phishing attack. Best practices conclude, obtaining security awareness training plays a vital part in the individual's ability to gain the knowledge needed to identify and protect themselves from phishing. Gartner performed analysis of phishing-related training providers and ranked the providers into four magic quadrants (e.g., Leaders, Niche Players, Visionaries and Challengers) that can assist corporations with setting up and establishing a robust security awareness program. Recent research studies are promoting online gaming as a critical component to administer training because it motivates individuals to play closer attention and provides immediate feedback. Online gaming matches the primary learning objective of this research by teaching individual's how to identify phishing. Specifically, the researcher used online gaming as a vehicle to increase the users' avoidance behavior through motivation to protect against phishing attacks.

Theories associated with phishing and technical elements included in this research study center on the ELM Model, it explains how predictable long-lasting behavior changes are achievable through cognitive processing (Pukakainen and Siponen, 2010). The researcher selected the Elaboration Likelihood Model (ELM) and Technology Threat Avoidance Theory (TTAT) components to model

individual behavior. The central persuasion and peripheral routes component of ELM address the active participants process of persuasion and diligently looks at information cues through the process of elaboration (Vishwanath et al., 2011). The researcher recognizes active participation to be synonymous with being mindful. The selection of ELM is a perfect fit given the specific elements presented that target an individual's knowledge, experience and education can also aid in identification of known phishing cues (e.g., automated email filtering, email source, grammar, spelling, urgency cues and paying attention to the email title or subject) that impact phishing attacks.

Furthermore, in the review of the literature, the studies show increasing awareness knowledge, and sensitivity training reduces an individual's phishing susceptibility (Vishwanath et al., 2011). The research also incorporates TTAT theory to support analysis to address how individuals cope with phishing after a successful attack. This theory according to Liang and Xue (2009), helps illustrates that users need motivation to avoid malicious actors when they perceive the threat is real and believe that the danger is unavoidable, only then will individuals take safeguards to engage in emotion and focused coping. Additionally, the literature explicitly shows that adoption of safeguards to protect individuals from phishing attacks is an essential part of the threat avoidance process. The use of Internet self-efficacy constructed survey questions allowed the researcher to examine the individual's online behavior. According to the research of Sun et al. (2016), study, review of the Analysis of Variance (ANOVA) statistic reveals a significant correlation exist between Internet self-efficacy, anti-phishing self-efficacy, and anti-phishing behavior. The Sun et al. (2016), study concluded that individuals with higher rates of success and accuracy with Internet-related task are more willing to participate in online learning.

Based on the review of the literature and examination of this studies results the researcher concludes there is not one technical control or training regimen that can provide corporations and

individuals with complete enhanced abilities to detect phishing attacks. It will continue to take layers of defense to thwart phishing attacks. Secondly, grounded theories (i.e., TTAT and ELM) are vital to understand the type of behavioral modifications that cognitively influence user avoidance behavior. Research studies show that when individuals have an increase in perceived threats and increased risk, it forces individuals to invoke protection coping strategies. Improvements in the human layer of defense must grow as part of the individual's knowledge of phishing cues through improved security education practices that increase cognition and have a more lasting effect. Modifying browser warning messages and educating individuals to identify phishing URLs and email message will allow for increased knowledge improving the human firewalls ability to detect phishing attacks that make it through the first line of defense automated filters. Finally, the literature review addresses various phishing education practices in use today (e.g., CBT, role-play, classroom, etc.) however, online gaming appears to provide the necessary mechanisms to improve an individual's knowledge, experience, and self-efficacy and have a longer lasting effect.

The key conclusion identified in this research study and linked to other research studies is that individuals need to feel threatened by phishing attacks before they will invoke their threat perception to allow themselves to avoid threats. Therefore, online gaming modifications to training individuals to detect phishing must ensure that individual have increased perceived threat perceptions to trigger the necessary safeguards for protection from phishing.

Appendix A

Survey Instruments

Survey Monkey Quiz Questions

Question Ranking	
QUESTIONS (10)	DIFFICULTY
Q37 Is https://www.amazon.com/gp/prime/pipeline/prime_gift_landing?ie=UF8&formSubmit=submit a legitimate address for Amazon?	1
Q34 Is http://www.ebates.com/target.com a legitimate address for Target?	2
Q38 Is https://www.bancofamerica.com a legitimate address for Bank of America?	2
Q33 Is http://192.192.230.48/scripts/sys.php a legitimate address for Citi Bank?	4
Q35 Is https://www.valentino-crush.com/huntington/login.asp a legitimate address for the Huntington Bank?	4
Q39 Is management@mazoncanada.ca a legitimate email address for Amazon?	4
Q31 Is this URL taking you to twitter " www.twivver.com/e/verify/?&account_secure_login "	7
Q30 Is the URL " www.paypal.com/ " taking you to paypal?	8
Q36 Is https://www.facebook.com a legitimate address for Facebook?	8
Q32 Is https://www.google.com a legitimate URL for Google?	10

Appendix B

Sample Invitation to Participate in Dissertation Study

Adult/General Informed Consent (Rev. 9/20/2011)

Consent Form for Participation in the Research Study Entitled

Assessing Mindfulness of Bank Employees in Response to Phishing: Improving Awareness and Attention Cognition

Funding Source: None.

IRB protocol #:

Principal investigator(s)

Chris Wilder, MBA, BS IT, BS Accounting
6490 Hilliard Drive
Canal Winchester, OH 43110
Cybersecurity
(614) 419-7510

Co-investigator(s)

James L. Parrish, Jr., PhD
Associate Professor and Chair
Department of Information Systems and
College of Engineering and Computing
3301 College Avenue
Fort Lauderdale, Florida 33314
(954) 262-2043

For questions/concerns about your research rights, contact:
Human Research Oversight Board (Institutional Review Board or IRB)
Nova Southeastern University
(954) 262-5369/Toll Free: 866-499-0790

IRB@nsu.nova.edu

What is the study about?

This study will assess how aware employees are to be able to find phishing attempts seen through a review of email addresses and URLs. The purpose of the study is to supply education to employees that will allow them to be more mindful of phishing emails or URLs and better sustain knowledge gained from game-based training.

Why are you asking me?

The reason for asking the subject to take part is to assess whether existing training is enough for employees to identify phishing attempts or whether inclusion of mindfulness into the users. Study will aid in further identification of phishing emails or URL questions. Approximately 100 – 150 individuals will be asked to take part in the initial survey and grouping will occur to pare down to a smaller group of individuals selected based on their knowledge or lack thereof of phishing. This smaller group of 20 – 30 individuals will complete the think a-loud part of the assessments.

What will I be doing if I agree to be in the study?

The research study includes four phases;

Phase 1 – All employees will have an opportunity to complete the SurveyMonkey.com survey questions to gauge how mindful you are. A second part of the survey will gather generic demographic information and the final part of the survey will test your awareness of phishing.

Phase 2 – Will pre-test a select group of employees to see how well they find phishing email and URLs

Phase 3 – Will the select group of individuals will be given game-based training on how to find phishing emails and URLs.

Phase 4 – will administer a post-test to measure improvements in cognition and phishing identification.

Overall the research should take no more than 1 hour using a combination of online survey and classroom observation.

Is there any audio or video recording?

This section should include information related to audio or video recording if it applies to the project proposed. If there is audio and/or video recording, please include the following paragraph:

This research project may include audio and/or video recording of participants playing the phishing game. This audio and/or video recording will be available from the researcher, to IRB, and the dissertation chair or committee. The recording will be transcribed by (BE SPECIFIC, including “The recording will not be transcribed.” if no transcription will take place). The recording will be kept securely (SPECIFY WHERE AND HOW). The recording will be kept for 12 months and destroyed after that time by wiping the DVD. Because your voice (or your image and your voice) will be potentially identifiable by anyone who hears (or hears and sees) the recording, your confidentiality for things you say (or do) on the recording cannot be guaranteed although the researcher will try to limit access to the tape as described in this paragraph.

Audio/video recording will only ask the participant to explain why a certain answer was selected during game-training.

What are the dangers to me?

The procedures or activities in this study may have unknown or unforeseeable risks (e.g., anxiety) and the researcher will make every effort to make the participants comfortable during the process.

If you have any questions about the research, your research rights, or have a research-related injury, please contact Chris Wilder and James Parrish Jr., PhD. You may also contact the IRB at the numbers indicated above with questions as to your research rights.

Are there any benefits for taking part in this research study?

Yes, the primary benefit is to introduce an online gaming training method to employees that will have a significant increase on phishing cognition and recognition into the future.

Will I get paid for being in the study? Will it cost me anything?

There are no costs to you, or payments made for participating in this study.

How will you keep my information private?

To ensure confidentiality all participants will be assigned individual numbers by their employer and only the employer will know the names of each participant. NOVA's IRB process requires a minimum of 36 months from the conclusion of the study. All information obtained in this study is strictly confidential unless disclosure is required by law.

What if I do not want to participate or I want to leave the study?

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of services you have a right to receive. If you choose to withdraw, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study and may be used as a part of the research.

If the participant may request that his/her data not be used, then it should read:

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of services you have a right to receive. If you choose to withdraw, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study, but you may request that it not be used.

Other Considerations:

If significant added information relating to the study becomes available, which may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

Voluntary Consent by Participant:

By signing below, you indicate that

- this study has been explained to you
- you have read this document, or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read and signed it
- you voluntarily agree to participate in the study entitled Assessing Mindfulness of Bank Employees in Response to Phishing: Improving Awareness and Attention Cognition

Appendix C

IRB Approval



I

MEMORANDUM

To: Christopher Wilder, B.S. Accounting; B.S. Information Technology, MBA

From: Ling Wang, Ph.D.,
Center Representative, Institutional Review Board

Date: June 22, 2017

Re: IRB #: 2017-401; Title, "Assessing Mindfulness of Bank Employees in Response to Phishing: Improvements in Awareness and Attention"

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 Category 2). 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 Ling Wang, 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: James Parrish, Ph.D.
Ling Wang, Ph.D.

References

- 93% of phishing emails are now ransomware | CSO Online. (n.d.). Retrieved June 3, 2016, from <http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html>
- Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology*, 33(3), 236–247.
- Akhawe, D., & Felt, A. P. (2013). Alice in warningland: a large-scale field study of browser security warning effectiveness. *Proceedings of the 22nd USENIX Security Symposium*, 257–272.
- Alnajim, A., & Munro, M. (2009). An anti-phishing approach that uses training intervention for phishing websites detection. *ITNG 2009 - 6th International Conference on Information Technology: New Generations*, 405–410.
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69–82.
- Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). How polymorphic warnings reduce habituation in the brain — Insights from an fMRI study. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2883-2892.
- Anderson, B., Vance, A., & Eargle, D. (2013). Is your susceptibility to phishing dependent on your memory? *WISP 2012 Proceedings*. Paper 40. <http://aisel.aisnet.org/wisp2012/40>
- APWG. (2019). Phishing Activity Trends Report 4th Quarter 2018. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf
- Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from “phishing attacks.” *International Conference on Information Society, I-Society 2011*, 1(1), 485–489. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-80052568937&partnerID=40&md5=5b7adaf97758fa9803808dec15dae0f1>
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3), 706–714.
- Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behavior: An empirical investigation. *Computers in Human Behavior*, 60, 185–197.
- Brown, K. W., & Ryan, R. M. (2003). The benefits of being present: Mindfulness and its role in psychological well-being. *Journal of Personality and Social Psychology*, 84(4), 822–848.
- Browne, S., Lang, M., & Golden, W. (2015). Linking threat avoidance and security adoption: A theoretical model for SMEs, *28th Bled eConference*, 32–43.

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Special issue: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Burns, M. B., Durcikova, A., and Jenkins, J. L. (2012). On not falling for phish: Examining multiple stages of protective behavior of information system end-users. *ICIS*
- Callaghan, M., McCusker, K., Losada, J., Harkin, J. and Wilson, S. (2013). Using game-based learning in virtual worlds to teach electronic and electrical engineering. *IEEE Transactions on Industrial Informatics*, 9(1), 575.
- Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 58(8), 1158–1172.
- Carpenter, P., & Huisman, J. G. (2016). Magic quadrant for security awareness computer-based training. Retrieved October 31, 2016, from www.gartner.com ID: G00293102
- Charters, E. (2003). The use of think-aloud methods in qualitative research an introduction to think-aloud methods. *Brock Education Journal*, 12(2), 68–82.
- Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, 39(PART B), 447–459.
- Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, 2010(3), 13–19.
- Cyveillance Blog – The Cyber Intelligence Blog Cyveillance Phishing Report: Top 20 Targets - June 8, 2015. (n.d.). Retrieved June 19, 2015, from <https://blog.cyveillance.com/cyveillance-phishing-report-top-20-targets-june-8-2015-2/>
- 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.
- Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing (p. 79). Association for Computing Machinery (ACM).
- Downs, J.S., Holbrook, M., Cranor, L.F., 2007. Behavioral response to phishing risk. In: Proceedings of the APWG eCrime Researchers Summit, ACM, Pittsburgh, USA.
- Egelman, S., Cranor, L. F., & Hong, J. (2008). You’ve been warned: An empirical study of the effectiveness of web browser phishing warnings. *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, 1065.

- Ernst & Young. (2013). Cyber-security---Thought-leadership, (October). Retrieved 2016/06/15.
- Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Grimes, J. (2015). Improving SSL warnings: Comprehension and adherence. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15)*, 2893–2902.
- Ferrara, J. (2014). Phishing scams at all-time high, employee training not keeping pace. *InformationWeek Wall Street & Technology*. Retrieved May 5, 2015, from <http://www.wallstreetandtech.com/security/phishing-scams-at-all-time-high-employee-training-not-keeping-pace/a/d-id/1306866>
- Global Ransomware Resource Center. (n.d.). Retrieved June 3, 2016, from <http://ransomware.phishme.com/>
- Hacker lexicon: What are phishing and spear phishing? WIRED. (n.d.). Retrieved April 1, 2016, from <http://www.wired.com/2015/04/hacker-lexicon-spear-phishing>
- Hale, M. L., Gamble, R. F., & Gamble, P. (2015). CyberPhishing: A game-based platform for phishing awareness testing. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2015–March*, 5260–5269.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165.
- Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.
- Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *Computers and Security*, 28(1-2), 63–71.
- Hoban, K., Rader, E., Wash, R., & Vaniea, K. (2014). Computer security information in stories, news articles, and education documents, Poster in Symposium on Usable Privacy and Security (SOUPS)
- Hovav, A., and Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis, *Communication of the Association for Information Systems: Vol. 34, Article (50)*.
- How to reduce spam & phishing with DMARC. (n.d.). Retrieved from <http://www.darkreading.com/application-security/how-to-reduce-spam-and-phishing-with-dmarc/a/d-id/1319243>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95

- 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.
- IRS warns of new email phishing scheme falsely claiming to be from the taxpayer advocate service. (2014). Retrieved April 16, 2016, from <https://www.irs.gov/uac/newsroom/irs-warns-of-new-email-phishing-scheme-falsely-claiming-to-be-from-the-taxpayer-advocate-service>
- Johnston, B. A. C., & Warkentin, M. (2010). Fear appeals and information security behaviours: An empirical study. *MIS Quarterly*, 34(3), 549–566.
- Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43, 64–76.
- Kim, Y., & Glassman, M. (2013). Beyond search and communication: Development and validation of the Internet Self-efficacy Scale (ISS). *Computers in Human Behavior*, 29(4), 1421-1429.
- Knezevich, C. (2014). 3 Security awareness training findings to surprise you. Retrieved April 30, 2015, from <https://www.twinc.com/8921/security-awareness-training-findings/>
- Krebs, B. (2014). The target breach, by the numbers. *Krebs on Security*, 6.
- Langer, E., and Moldoveanu, M. 2000. The construct of mindfulness, *Journal of Social Issues*, 56(1), 1-9.
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635–645.
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90.
- Omar, E.-N. M. M. A., Abdalrahim, A., Drewish, A., Saeed, Y. M., & Abdalbagi, Y. M. (2015). Test of information technology (IT) – Self-efficacy and online learning interaction components on student retention: A study of synchronous learning environment. *2015 Fifth International Conference on E-Learning (Econf)*, 5, 165–173.
- Osterman. (2015). Best practices for dealing with phishing and next-generation malware. Retrieved July 5, 2015, from http://www.ostermanresearch.com/programs/OR_Security_program.pdf
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5), 673–680.
- Parrish Jr., J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Southwest Decision Sciences Institute (SWDSI) Annual Meeting*, (October 2015), 285–296.

- Parrish Jr, J. L., Kuhn, J. R., & Courtney, J. F. (2008). Mindful administration of IS security policies. *14th Americas Conference on Information Systems, AMCIS 2008, 1*, 85–93.
- Petty, Richard E; Cacioppo, John T (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology: 129*.
- PhishMe. (2015). Enterprise phishing susceptibility report. Retrieved from <http://info.phishme.com/e/46382/ptibilityReport-2015-Final-pdf/2m2j7q/795633853>
- Ponemon Institute. (2013). Experimental analysis of securED training effectiveness Commissioned by Digital Defense. Retrieved September 28, 2014, from http://pg.myddi.com/rs/digitaldefense/images/Ponemon_Report_SecurED.pdf
- Ponemon Institute. (2016). Managing insider risk through training & culture. Sponsored by Experian ® Data Breach Resolution, (May). Retrieved July 7, 2016, from <http://www.experian.com/data-breach/2016-ponemon-insider-risk.html>
- Ponemon Institute and Accenture. (2017). 2017 Cost of Cyber Crime Study, 56. Retrieved from <https://www.accenture.com/t20170926T072837Zw/us-en/acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf>
- Proofpoint. (2016). Credential phishing hook, line, and sinker. Retrieved April 13, 2016, from https://www.proofpoint.com/sites/default/files/catching_credential_phish_white_paper.pdf
- Puhakainen, P. & Siponen, M. (2010). Research article improving employees' compliance through information security training: An action research study. *MIS Quarterly*, 34(4), 757-778.
- Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, 20(5), 382–420.
- Rakesh, R., Kannan, A., Muthurajkumar, S., Pandiyaraju, V., & SaiRamesh, L. (2014, December). Enhancing the precision of phishing classification accuracy using reduced feature set and boosting algorithm. In *2014 Sixth International Conference on Advanced Computing (ICoAC)* (pp. 86-90). IEEE.
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816–826.
- RSA Monthly Online Fraud Report -- January 2014 - [rsa-online-fraud-report-012014.pdf](http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf). Retrieved May 13, 2015, from <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf>
- Ruiz J., G., Mintzer M., J., & Leipzig R., M. (2006). The impact of e-learning in medical education. *Academic Medicine*, 81(3), 207–212.

- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers and Security, 53*, 65–78.
- SC Magazine. (2015). 2015 Cyberthreat defense report. *CyberEdge Group, 2*. Retrieved from https://www.scmagazine.com/resource-library/resource/Code42/whitepaper/57a3a4abed344a186455fed1?campaignId=57a39805ed344a186455fbf1&type=email&src=Custom090916-1-B&email=Bv_161oYyZO-isHvk55XgzIZDo7e_i8h0&spMailingID=15381991&spUserID=MjcxMDQ5MjE2MDY3S0&spJobID=860684427&spReportId=ODYwNjg0NDI3S0
- Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). The Emperor's New Security Indicators. *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 51–65.
- Soper, D.S. (2019). Critical Chi-Square Value Calculator [Software]. Available from <http://www.danielsoper.com/statcalc>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the 28th international conference on Human factors in computing systems. ACM*.
- Sheng, S., Magnien, B., Ponnurangam, K., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of SOUPS 2007*, 88–99.
- Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48*, 199–207.
- Siponen, Mikko; Mahmood, & M; Pahlila, S. (2009, December). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 145–147.
- Sommestad, Teodor. Hallberg, Jonas, Lundholm, Kristoffer, & Bengtsson, Johan, (2014) Variables influencing information security policy compliance: A systematic review of quantitative studies, *Information Management & Computer Security*, Vol. 22 Iss: 1, pp.42 – 75.
- Sun, J. C. Y., Yu, S. J., Lin, S. S. J., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior, 59*, 249–257.
- Top Phishing Attacks: Discovery and Prevention. (n.d.). Retrieved from www.agari.com
- Van Dam, N. T., Earleywine, M., & Borders, A. (2010). Measuring mindfulness? An Item Response Theory analysis of the Mindful Attention Awareness Scale. *Personality and Individual Differences, 49*(7), 805–810.

- Van Kessel, P., & Allan, K. (2013). Under cyber-attack EY's global information security survey 2013 (p. 28). Retrieved from [http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/\\$FILE/EY-GISS-Under-cyber-attack.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf)
- Van Someren, M. W., Barnard, Y. F., & Sandberg, J. A. (1994). The think aloud method: A practical guide to modelling cognitive processes. *Department of Social Science Informatics, University of Amsterdam*.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H.R., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support System* (51)576–586. In Chapter 1
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Computers in Human Behavior Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421.
- 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.
- Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, 25(2), 385–400.
- Yates, D., & Harris, A. L. (2015). Phishing attacks over time: A longitudinal study. In *Twenty-first Americas Conference on Information Systems, Puerto Rico* (pp. 1–6).
- Zahedi, F. M., 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.