International Journal of Business and Management; Vol. 13, No. 6; 2018
ISSN 1833-3850 E-ISSN 1833-8119
Published by Canadian Center of Science and Education

Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks

Jason E. Thomas[1,2,3,4,5,6]

[1] Graduate Student, Bush School of Government and Public Service, Texas A&M University, College Station, Texas, United States

[2] Graduate Student, American Military University, Charles Town, West Virginia, United States

[3] Adjunct Faculty, School of Business & Technology, Excelsior College, Albany, New York, United States

[4] Adjunct Faculty, Colangelo College of Business, Grand Canyon University, Phoenix, Arizona, United States

[5] Adjunct Faculty, College of Business and Communication, Concordia University Texas, Austin Texas, United States

[6] Chief Operating Officer (COO), The Collective Group, Austin, Texas, United States

Correspondence: Jason E. Thomas, Bush School of Government and Public Service, Texas A&M University, College Station, Texas, United States. E-mail: jason.thomas@tamu.edu

Received: April 10, 2018 Accepted: April 30, 2018 Online Published: May 1, 2018

doi:10.5539/ijbm.v13n6p1 URL: https://doi.org/10.5539/ijbm.v13n6p1

Abstract

One of the most difficult challenges in information security today is phishing. Phishing is a difficult problem to address because there are many permutations, messages, and value propositions that can be sent to targets. Spear phishing is also associated with social engineering, which can be difficult for even trained or savvy employees to detect. This makes the user the critical point of entry for miscreants seeking to perpetrate cyber crimes such as identity theft and ransomware propagation, which cause billions of dollars in losses each year. Researchers are exploring many avenues to address this problem, including educating users and making them aware of the repercussions of becoming victims of phishing. The purpose of this study was to interview security professionals to gain better insight on preventing users and employees from succumbing to phishing attack. Seven subject-matter experts were interviewed, revealing nine themes describing traits that identify users as vulnerable to attack or strongly resistive to attack, as well as training suggestions to empower users to resist spear phishing attacks. Suggestions are made for practitioners in the field and future research.

Keywords: computer security, computer information systems, cyber security, identity theft, information systems, information system security, phishing, ransomware, social engineering, spear phishing

1. Introduction

Phishing is a major problem in the business, government, and technology sectors, and when unaddressed, the effects of phishing have devastating consequences. Estimates place greater than 80% of organizations as having experienced phishing attacks (Derouet, 2016). These attacks result in billions of dollars in losses annually (Goel, Williams, & Dincelli, 2017; Jensen, Dinger, Wright, & Thatcher, 2017). While many resources have been brought to bear in the face of this problem, phishing attacks continue to grow in frequency (Greenwald, 2016).

Cyber security is a growing public concern. These issues have become so prominent that one can see daily reports of cyber attacks in the news with large institutional victims such as JP Morgan, Target, and Sony. These attacks are not limited to large corporations; even the United States government became a victim of a recent attack on the Office of Personnel Management (Javelin Research and Strategy, 2014). In fact, these issues have become so pervasive that even more benign organizations such as the American Association of Retired People provide awareness information on such issues as spear phishing, identity theft, and ransomware attacks (Mitnick, 2017). The cost of addressing these security breaches is staggering. Sony's recent cyber attack cost some $171 million to address, excluding legal fees and damages (Richwine, 2014).

Two of the most damaging effects of spear phishing are identity theft and ransomware infection. In 2013, more than 13 million people became victims of identity theft, and more than $18 billion in economic losses occurred

because of identity theft (Javelin Research and Strategy, 2014). During this period, the Federal Trade Commission (FTC) received more than 290,000 complaints regarding identity theft (FTC, 2015). This is a global issue and affects many more areas than the United States alone. In 2015, incidents of identity theft grew by more than 49% despite enhanced governmental efforts to combat identity theft (Cifas, 2016).

Similarly, the ransomware epic is growing at an alarming rate (Collier, 2017; Richardson & North, 2017). This cyber attack is extremely damaging because it encrypts sensitive data and makes computer systems unusable. Further, ransomware can spread like wildfire. The WannaCry ransomware attack infected more than 100,000 organizations around the globe (Lelii, 2017). These ransomware attacks are becoming too familiar. In another attack, over 60 trusts in England's National Health Service were infected and ultimately spread to over 200,000 computer systems in some 150 countries (Collier, 2017).

Several studies have examined the psychology of information security compliance and how to increase security awareness (Anderson & Agarwal, 2010; Anderson & Moore, 2009; Bulgurcu, Cavusolglu, & Benbasat, 2010; Herath & Rao, 2009; Siponen, 2000; Siponen, 2000; Stanton, Stam, Mastrangelo & Jolton, 2005). However, one of the significant challenges in combating phishing is that a lack of information exists regarding human psychological factors such as decision making and their effects on phishing attacks (El-Din, Cairns, & Clark, 2015). There is a dearth of empirical research in this area that needs to be addressed. Employees are the first line of defense for cyber security and simultaneously the most accessible vehicle for miscreants to gain access to valuable computer systems and sensitive data (Clarke & Knake, 2010). While security groups and information technology (IT) professionals can harden systems and create robust processes, they must depend on able and informed user participation to make these processes work. They must empower users with the tools and knowledge to resist spear phishing attacks and the subsequent adverse effects of falling victim to spear phishing such as ransomware and identity theft. Consequently, scholars, practitioners, and government officials are calling for additional research in this area and new methods to address this problem (Collier, 2017; Komatsu, Takagi, & Takemura, 2013; Sun & Lee, 2016).

1.1 Statement of the Problem

The problem addressed in this research was spear phishing. Spear phishing is one of the greatest challenges faced by IT departments. Spear phishing is the entry point for many intrusions and hacking activities such as ransomware and identity theft (Goel et al., 2017; Sjouwerman, 2015). The results of these attacks are devastating. Identity theft, for example, has been touted as the signature crime of the information age (Zaeem, Mnaoharan, Yang, & Barber, 2017). In 2013, more than 13 million people fell victim to identity theft and suffered some $18 billion in losses (Javelin Research and Strategy, 2014). Phishing attacks enable many different types of intrusion beyond identity theft—scholars have identified end users and employees as the most vulnerable point of entry for these attacks and have called for additional research to address this growing problem (Komatsu, Takagi, & Takemura, 2013; Sun & Lee, 2016).

1.2 Purpose of the Study

The purpose of this exploratory, single, qualitative case study was to investigate the reasons that users succumb to spear phishing and to gather and document observations and recommendations from known subject-matter experts (SMEs) to address the problem. The information gathered in this study could be used to address the problem of spear phishing and to prevent the results of the malicious activities facilitated by spear phishing, such as ransomware propagation and identity theft. Employees who use computers are the first point of access and protection for computer systems and sensitive data and can facilitate easy access for miscreants looking to do harm to organizations (Sun & Lee, 2016). Therefore, it is imperative to understand how to better empower these key resources to resist these dangerous and damaging attacks.

1.3 Research Questions

The research question for this study explored the reasons that users succumb to spear phishing attacks. The question served as the central question to frame the study. Subquestions for the interview guide added depth to the interviews and facilitated meaningful interactions with the SMEs. The interview guide provided consistency in the interview process and aided in the performance of consistent and timely interviews (Rubin & Rubin, 2012; Yin, 2014).

Q1. Why do users succumb to spear phishing attacks?

Q2. What can be done to prevent users from succumbing to spear phishing attacks?

1.4 Significance of the Study

The results of this study can be used by practitioners in the field to better empower users to identify and resist spear phishing attacks. The data in this study provide insight from SMEs about why users succumb to spear phishing attacks and capture observations and best practices about how to mitigate and prevent exposure to spear phishing attacks. In the academic realm, the data from this study could be used to expand theories that explore predicting and influencing behavior such as the theory of planned behavior (TPB) (Ajzen, 2014) and protection motivation theory (PMT) (Floyd, Prentice-Dunn, & Rogers, 2000). This information is valuable to IT directors and security managers who are responsible for protecting organization's assets from cyber attack. The information gathered from this study can be used to create more effective user education programs and learning aids to help users resist spear phishing attacks. Spear phishing is worldwide problem for IT departments, and more than 8 out of 10 firms have experienced a spear phishing attack (Derouet, 2016).

1.5 Use of Two-Word Compound Cyber Terms

Two-word compound cyber terms have several different forms in common usage. For example, cyber attack can be seen as cyberattack and cyber-attack in many written works. The author has standardized usage of these terms based on the Federal Bureau of Investigation's (FBI's) use of these terms, as the FBI is the lead federal agency for investigating cyber issues (FBI, 2018).

1.6 Assumptions of the Study

The assumptions for this study were as follows:

1. There would be enough information available to conduct the study successfully.
2. A sufficient number of SMEs would be available to participate in the study interviews.
3. The individuals who participated in the study would be truthful about their backgrounds and expertise and provide meaningful responses that would be useful in the research.

2. Literature Review

2.1 Introduction

Spear phishing is a targeted form of phishing, typically an email attack that utilizes specialized social engineering methods to attempt to influence users to expose sensitive account, personal, or business information or to enable intrusion into the computing infrastructure (Goel et al., 2017; Sjouwerman, 2015). Spear phishing is difficult to detect because it uses a targeted approach to entice users to lower their guard and to act by perceptions of urgency or by communications from important contacts, even superiors in one's organization. As technology has enabled more ubiquitous remote communication, spear phishing attacks have become even more challenging to detect. Spear phishing acts as a gateway or enabler to other cyber crimes such as ransomware and identity theft, which cause billions of dollars in damages each year.

There are several studies in the literature that examine an individual user's potential susceptibility to spear phishing, and some researchers present profiles of users who might be more susceptible to spear phishing attacks (Aguilar, 2015; Boss, Galletta, Lowry, Moody, & Polak, 2015; Brewer, 2017; Caputo, Pfleeger, Freeman, & Johnson, 2014; Lötter & Futcher, 2017; Vishwanath, 2015). However, there is a gap in the knowledge regarding how successful users are with tools to resist spear phishing and thereby avoid negative consequences such as identity theft and ransomware. Given the significant problem caused by this phenomenon, more research is needed to help combat spear phishing.

2.2 Theoretical Framework

The focus of this study was to understand why users fall prey to spear phishing attacks. Because the goal was to understand this human behavior and work to influence it, the study used two theories for predicting and moderating behavior as the theoretical framework: protection motivation theory (PMT) and the theory of planned behavior (TPB).

PMT is a behavioral theory model that both explains and predicts the processes that create protection responses from subjects as a result of communications based on fear appeals (Floyd, Prentice-Dunn, & Rogers, 2000). The core premise of PMT is that fear appeals stimulate the cognitive appraisal process, which then informs and drives protection intentions. Essentially, effective fear appeals increase protection motivation. This increased protection motivation heightens the subject's awareness and increases the willingness to engage in protective behaviors. With some success, researchers in the field are exploring the effects of making users aware of the disastrous effects and losses caused by phishing to regenerate a protective response to increase awareness and

mindshare about phishing and improve the user's ability to detect and avoid phishing attacks (Komatsu et al., 2013; Sun & Lee, 2016).

TPB is widely used in social science research to understand motivation and predict behavior (De Leeuw, Valois, Ajzen, & Schmidt, 2015). A foundational premise of TPB is that people first consider the implications of potential actions prior to taking action on a given event. Further, TPB can help identify opportunities to change or influence behavior (Ajzen, 2014). Ajzen asserted that intentions comprise three different types of beliefs: (a) behavioral beliefs, (b) control beliefs, and (c) normative beliefs. These beliefs coalesce to form intentionality, which results in behavior. TPB has been used extensively in social science fields to predict behavior. These theories were selected for this work because they apply to the study subject of understanding why users succumb to spear phishing attacks for the purpose of addressing this behavior and preventing its negative effects.

2.3 Spear Phishing

Spear phishing is one of the greatest cyber security challenges faced by businesses today, with as many as 84% of firms having experienced at least one spear phishing attack (Derouet, 2016). Spear phishing is a targeted form of phishing, typically an email attack that utilizes specialized social engineering methods to attempt to influence users to expose sensitive account, personal, or business information or to enable intrusion into the computing infrastructure (Goel et al., 2017; Sjouwerman, 2015). Spear phishing usually involves research on the target to create a personalized message to trick the receiver into taking an action that would be detrimental in some way.

Spear phishing and phishing are the most prevalent global cyber attack vectors according to the Enterprise Phishing Susceptibility and Resiliency Report (PhishMe, 2016). Criminals account for nearly 90% of phishing-based attacks, with the vast majority of the remaining attacks being perpetrated by government-based actors (Verizon, 2016). A survey conducted by McAfee with more than 19,000 respondents found that only 3% of users are able to successfully identify phishing emails (McAfee, 2015).

In the fast-paced world of email, incidents happen quickly. Approximately one-third of phishing emails are opened by their victims within 1 minute, 40 seconds (Verizon, 2016). Of those who open the emails, 12% click a link or execute an attachment within the email in under four minutes. The information used to entice the user to action may be obtained through public information, social media information, fraudulent methods, or any other available source (Greenwald, 2016). In essence, spear phishing is a personalized attack that attempts to make the target believe they are interacting with someone they know or with an official authority in an effort to prompt the user to give up sensitive information. These attacks affect both businesses and consumers (Bleau, 2017).

2.4 Discrete Targets for Phishing Attacks

Understanding which organizations are targets for phishing attacks and the vectors of attack is essential to effective security planning (Wueest, 2016). While the range of targets for phishing attacks is broad, there are particular targeted groups. Employees in human resources departments are often targets for spear phishing because of their access to sensitive employee data, such as W-2 forms and social security numbers (Greenwald, 2016). In the first quarter of 2016, 68 firms reported becoming victims of large, elaborate, coordinated W-2 spear phishing attacks (Landesman, 2016).

The Internal Revenue Service (IRS) issued a warning on February 2, 2017 that W-2 email phishing scams were spreading beyond the corporate sector and targeting schools, nonprofits, and tribal organizations (IRS, 2017). Often the stimulus for these attempts is a fraudulent email from the chief executive officer (CEO) or chief financial officer (CFO) (Landesman, 2016). The IRS found that, in some cases, organizations that were victims of wire fraud scams were also being targeted for W-2 phishing scams. Essentially, the miscreants perpetrating these crimes were double-dipping in an attempt to take advantage of known victims twice.

Financial firms are a favored target of cyber miscreants and are targeted more often than other types of institutions (Wueest, 2016). Financial targets have electronic access to vast amounts of monetary resources. Wueest (2016) has estimated that losses from financial institutions alone have accounted for anywhere from $10 million to as much as $1 billion. Calculating these damages is challenging, however, because firms may not wish to report incidents due to business and reputation losses associated with perceptions of insufficient security measures.

Spear phishing has also been reported to target elements of the United States government. During the 2016 election cycle, the Democratic National Convention (DNC) became a victim of cyber attack (Lipton, Sanger, & Shane, 2016). According to Lipton et al. (2016), this was the first known attempt of a foreign power to disrupt a United States election. The DNC did not have robust security practices or strong IT resources. Hackers had

access to the DNC systems for as many as seven months. Once inside the DNC systems, hackers also were able prosecute other targets such as Hillary Clinton and John Podesta.

The entry point to the DNC systems occurred by means of spear phishing attack, where spear phishing emails were sent to DNC employees (Alperovitch, 2016). Ironically, John Podesta, who was singled out as a victim of these attacks, authored a 2014 report on cyber privacy for the Obama administration (Lipton, Sanger, & Shane, 2016). This irony demonstrates exactly how difficult it is to combat the pervasive cyber attack methodology. Once the DNC became a victim of the spear phishing attack, miscreants had access to its data, and private information was leaked to the public.

Spear phishing attacks can be tangential and indirect while still causing significant damage and problems. The news covered a major breach of IT security for Target stores that resulted in significant counts of identity theft, as well as substantial damages and fines to Target of more than $10 million (Riley & Pagliery, 2015). However, the vector of attack for Target was a spear phishing attack on a heating/cooling vendor that serviced Target stores (Weiss & Miller, 2015). A spear phishing email was used to install malware, which then invaded Target's point-of-sale systems and computer networks. Gaining access to the point-of-sale systems enabled miscreants to steal identity and payment information.

2.5 Social Engineering: User Interactions with Spear Phishing

Whereas phishing and spear phishing are the gateways to cyber attacks, social engineering tactics are the enablers. Social-engineering-based spear phishing attacks account for the vast preponderance of data breaches (Verizon, 2016). Social engineering is the act of interacting with people on a personal level to get them to reveal confidential information (CSO, 2012). Social engineering attacks the weakest link in security—people.

While the dominance of email as a communication method is now shared with text messaging and social media, email is still favored by miscreants for phishing attacks (Symantec, 2018). Email is ubiquitous and capable of contacting a large amount of targets quickly and efficiently. Over 50% of email traffic consists of spam emails, 1% of which consists of phishing attacks.

Social engineering and phishing attacks are evolving as technology progresses. One paradigm resulting from this evolution is advanced persistent threats (APTs). APTs are growingly sophisticated methods of cyber attack by miscreant organizations that attempt to gain access to sensitive information, maintain a footprint in the organization for future attack, and modify data to disrupt target efficiency (Daly, 2009). APT is tough to combat and predict because of its adaptive nature. APT efforts can identify additional targets to spread infections and leave resources dormant on hosts for future attacks.

2.6 Phishing Prevention

Phishing attacks are a major business and technology issue costing billions of dollars, and they are growing at an alarming rate (Derouet, 2016; Goel et al., 2017; Jensen et al., 2017). Consequently, researchers have spent significant resources examining potential methods to address the problem. But the problem still remains and is growing in severity. Organizations generally rely on three techniques to combat phishing: (a) automatic removal of phishing messages from the email system, (b) warning mechanisms that detect potential phishing activity and notify users, and (c) behavioral training that assists users in identifying phishing attempts and encourages users to report incidents (Komatsu et al., 2013).

While automated detection of phishing attacks is certainly useful, it has not proved very effective at filtering out all dangerous messages because there are many permutations of phishing attack that can be easily modified. Because of this complexity, training users is still an essential part of an information security phishing defense plan (Sun & Lee, 2016). One method of addressing phishing and educating end users is the rules-based approach to training. In this method, an organization develops a set of rules to follow that is disseminated to employees and users of the systems in order to combat phishing (Komatsu et al., 2013; Kumaraguru, Sheng, Acquisiti, Cranor, & Hong, 2010).

However, researchers have found that rules-based training alone is insufficient to prevent many attacks (Komatsu et al., 2013). This is likely due to the fact that users are generally unconcerned with phishing or learning how to deal with phishing until after they have been the victim of an attack (Sun & Lee, 2016). Observing reactions of users after attack has led several researchers to consider the implications of PMT. Researchers have been exploring the possibility of making users aware of the damages caused by phishing to trigger a protection response, which seems to make training and awareness more effective (Komatsu et al., 2013; Sun & Lee, 2016)

Identification of phishing emails is a particular challenge for users. In a study conducted by Intel Security with 19,000 participants from some 144 countries, participants were sent 10 different emails that were potential phishing-based attacks (McAfee, 2015). Only 3% of people passed the test with 100% success, and another 20% was able to correctly identify phishing emails except in one case. The study methodology entailed sending out quiz emails to a list of known users in 144 different countries including the United States, Canada, the Middle East, Europe, Latin America, and Asia, appearing to be an extremely large convenience sample. The average global score earned on the security quiz was 65.54%. The study did not fully disclose scoring methodology, which could undermine reliability (McAfee, 2015).

Another issue hindering efforts to combat spear phishing is incident reporting. It has been known for a long time that victims of cyber attacks are reticent to report attacks (FBI, 2005). Reasons for this can range from personal embarrassment to fear of consequences. The Office of the Inspector General of the United States Postal Service (USPS) found that the vast majority of phishing victims does not report incidents (USPS Office of Inspector General, 2015). In a phishing readiness test, 3,125 postal workers were sent simulated phishing messages. Of those who received the messages, one-quarter of them clicked links in the simulated phishing emails. Of those who clicked the links, less than 10% reported the incident to IT security officials within USPS.

2.7 Lines of Thought on Phishing Vulnerability

As this problem is pervasive, there has been a fair amount of discourse on why users are vulnerable to phishing attack. One point of view suggests that there are standard personality traits that are simply vulnerable based on items such as demographic data, Internet usage, and personality traits. Darwish, Zarka, and Aloul (2013) constructed a profile of individuals who might be susceptible to phishing attack by analyzing several significant empirical studies (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Kumaraguru et al., 2009; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

Darwish et al.'s (2013) study is a detailed literature review examining how other researchers have approached identifying traits that might predict potential susceptibility to phishing attack. After reviewing common tools and methodologies for phishing-based attacks, Darwish et al. (2013) examined a list of human traits that could indicate phishing susceptiblity, including victim gender, level of education, level of anti-phishing education, method of phishing training delivery, personality, and Internet usage.

One of the main challenges to this study is that the studies reviewed generally researched victims. While these data are useful in observing patterns in victims, it would seem difficult to validate these data without examining non-victims. In essence, the research had no control group. This study could serve, though, as an expanded case study and certainly provides empirical insight into the issue.

The results of the profile suggest that the person most susceptible to phishing attack is between the ages of 18 and 25, majored in college in humanities, has no anti-phishing training, and is active in ecommerce (Darwish, et al., 2013). Other researchers found that neurological traits could be indicative of susceptibility to phishing attack. An empirical study by Halevi, Memon, and Nove (2015) suggested that those with neuroticism and high conscientiousness levels are vulnerable to attack. Specifically, phishing attacks can exploit the desire to do well and perform, such as the feeling that one is behind in their work or that an emergency needs to be addressed quickly.

Another view of phishing susceptibility revolves around factors including disposition and experience, which can indicate potential phishing susceptibility or resistance. Wright and Marett (2010) found that items such as perceived self-efficacy, experience, and information literacy affect one's vulnerability to phishing attack. Essentially, high levels of information literacy, self-efficacy, and security knowledge better enable one to resist spear phishing attacks.

Other researchers have confirmed the results of Wright and Marett (2010). Those with knowledge of phishing attacks and higher information literacy skills are more skeptical of clicking on foreign links and entering personal information into unknown websites. Higher levels of technical acumen, such as knowledge of tracking information like cookies, spyware, network security, and virus propagation, also result in lower levels of phishing susceptibility (Sheng et al., 2010).

Researchers have also investigated disposition factors such as risk aversion, level of trust, and suspicious nature as indicators of phishing susceptibility (Sheng et al., 2010; Wright & Marett, 2010). Suspicious nature is a strong indicator of the ability to resist phishing (Vishwanath, Harrison, & Ng, 2016). Essentially, those who are naturally suspicious are more careful with which email links they click. An enhanced level of suspicion helps an

individual detect deception and cheating attempts (Bobko, Barelka, Hirshfield, & Lyons, 2014; Vishwanath et al., 2016).

Another approach to examining phishing vulnerability is email experience and cognitive information processing. Research exploring behavior in email use has provided some indications of phishing susceptibility. The information in email messages can be divided into two distinct groups. The first group displays information about the sender, recipient, and message delivery information and is generally referred to as the header. The second group of information includes the message, message title, and any attachments. The first group of information is often only examined in a cursory way, but often it can be the first technical indicator of suspicious activity. Users who do not examine the technical information in the first part of an email message with diligence and scrutiny are more susceptible to phishing attack (Vishwanath, 2015). Users who glance at email headers and intuit a sense of urgency or relevance from the email message body are more likely to succumb to a spear phishing attack (Harrison, Svetieva, & Vishwanath, 2016; Vishwanath, Harrison, Chen, Wang, & Rao, 2011).

While information literacy and technology familiarity can aid one in avoiding phishing attacks, familiarity and habitual use of email can make one more vulnerable to them. Users who process a large volume of emails on a consistent basis can build up habits and can respond reflexively to click on a phishing link. Accordingly, habitual use of email can make one more vulnerable to phishing attack (Vishwanath, 2015).

2.8 Ransomware: A Consequence of Phishing

Ransomware, often distributed by phishing, is an extortion-based malware threat that is growing rapidly and that proves a significant IT problem that is challenging for both users and IT professionals (Thomas & Galligher, 2018). Ransomware has many different vectors of attack such as social engineering strategies like phishing and spear phishing (when users open emails or click on malicious links from websites or instant messages) (Allen, 2017). Ransomware growth has ballooned dramatically in the past few years and has been labeled an epidemic (Collier, 2017; Mansfield-Devine, 2016; Richardson & North, 2017). Ransomware attacks and infections are growing at an alarming rate and have become a global problem (Lelii, 2017). Ransomeware is the most prominent type of extortion-based malware attack (Thomas & Galligher, 2018).

Ransomware has been a prevalent topic in recent news stories (Thomas & Galligher, 2018). One example is the WannaCry ransomware attack. Some 100,000 organizations fell victim to the Wanna Cry ransomware attack (Lelii, 2017). Similarly, another attack targeted some 60 trusts in England's National Health Service (Collier, 2017). Over time, this attack affected some 200,000 systems in more than 150 countries worldwide.

Ransomware is dangerous and difficult to control (Thomas & Galligher, 2018). Even when attempting to target a specific group of computer systems, ransomware can be difficult to control. The Petya ransomware attack was designed to target users of tax accounting software in Ukraine, but spun out of control and infected 64 different countries before it was brought under control (Ghosh, 2017).

The effects of the attacks from these few examples were devastating (Thomas & Galligher, 2018). Businesses lost access to critical computer systems. Medical facilities lost access to patient records. Surgical procedures had to be delayed or canceled. Ambulances were diverted to alternate hospitals, increasing the time before critical patients could receive emergency medical care. In the latter part of 2015, more than half of the trusts in England's National Health Service succumbed to ransomware attacks (Collier, 2017).

2.9 Ransomware Progression

The recent rise of prominent ransomware attacks in the media may create an opinion that ransomware is a relatively new computer-based threat, but in reality ransomware has been a tool for miscreants for the better part of 30 years (Thomas & Galligher, 2018). Ransomware was introduced to attendees of the World Health Organization's AIDS conference in 1989 (KnowBe4, 2017). Conference attendees received by distribution the first ransomware malware on 5.25-inch floppy disks. Some 20,000 copies of the ransomware virus were handed out to participants of the conference with labels suggesting the disks contained information about AIDS.

Humorously, the disks were given out with a pamphlet containing a disclaimer that using the disk could negatively affect operations and cause computers to cease functioning properly— and even that payment would be due to the PC Cyborg Corporation (KnowBe4, 2017). This was, in fact, the first ransomware notification. This first virus is now known as the AIDS Trojan or PC Cyborg virus (Longstaff, 1989). Figure 1 shows the actual ransomware notification displayed by the AIDS Trojan.

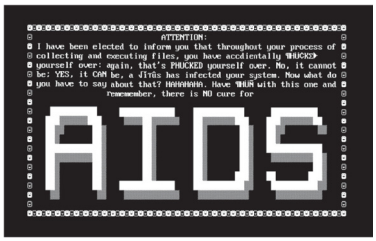

Figure 1. Ransom notification from the AIDS Trojan released in 1989

Adapted from KnowBe4 (2017).

The AIDS Trojan remained dormant on computer systems until 90 reboots had occurred (Manes, 2017). After these reboots, the virus sprang into action and changed file names and directory names, making the system inoperable. At that point, the ransom demand depicted in Figure 1 was presented to the victim. The 90-reboot cycle incubation period allowed the virus to spread widely to other users. The virus used symmetric encryption, which was easy to break once the general public understood what was occurring.

Ransomware has grown in prominence in the past few years and generally presents itself in three different ways (Thomas & Galligher, 2018):

- Screen-locking
- File encryption
- False alerts or bluffs

In each of these presentations, the software eventually presents a ransom request and asks the victim to pay a fee in exchange for removal of the ransomware (Richardson & North, 2017). After the rapid growth starting in 2013, ransomware has become the most prevalent type of extortion malware attack (Symantec, 2016). Figure 2 shows the relative frequency of attacks and their ratio of distribution from 2005 to 2016.

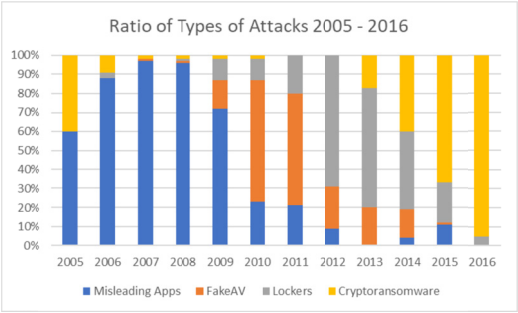

Figure 2. Extortion malware attack frequency

Adapted from Symantec (2016).

From the period of 2005 to 2016, one can see a distinct pattern of growth in extortion-based malware attacks. In 2005, misleading applications held a 60% market share of attacks and grew rapidly until 2008 (Symantec, 2016). This type of attack presented itself as a utility to improve system performance and remove spyware (Savage, Coogan, & Lau, 2015). Many programs used this approach, such as Performance Optimizer and SpySheriff, targeting both Mac-OS-based systems and PCs. These specific programs offered to fix issues for prices ranging from $30 to $90. Often no issue even existed. During this time, the first sets of crypto ransomware began to appear (Symantec, 2017).

In 2008, a new trend began, with FakeAV programs beginning to emerge (Savage et al., 2015; Thomas & Galligher, 2018). In this approach, a fake virus program and aggressive misleading applications infected user machines (Majauskas, 2009). The programs filled the screen with errors and offered to fix them in exchange for fees ranging from $40 to $100, with some even trying to sell multiyear subscriptions. By this time, users and malware knowledge had become more sophisticated, and some users removed the malware altogether. These actions lowered the return on investment (ROI) for the miscreants using this strategy, which likely brought about the demise of FakeAV efforts, which seem all but dormant in recent years (Thomas & Galligher, 2018).

In 2013, crypto locker ransomware vigorously resurfaced and quickly became the dominant player in extortion-based malware (Thomas & Galligher, 2018). From 2013 to 2016, ransomware grew, moving from holding 20% of the market share for extortion-based ransomware to holding 95% (Symantec, 2016). Crypto locker ransomware was an evolution of the FakeAV paradigm (Savage et al., 2015). When users began to bypass the ransom request because of the weak or nonexistent threat, miscreants adapted and increased the threat level to something with real consequences (Thomas & Galligher, 2018).

Modern ransomware variants are very sophisticated and can be installed with or without human aid (Brewer, 2017). The pretense for interaction has evolved from emulating law enforcement entities offering to take fine payments on demand for illicit actions to restore systems access to literally holding hostage system data. Modern ransomware encryption variants are crippling (Mansfield-Devine, 2016; Richardson & North, 2017). Encrypted file systems all but shut down critical systems. Access is denied to a system's critical software, operating systems, and vital business data (Collier, 2017). Moreover, the encryption used by these miscreants appears unbreakable and leaves victims with few choices (Thomas, 2017a). They can pay the ransom and hope their data are restored, restore from backups, or accept the data loss. After infection of a single system, the ransomware spreads with shared credentials through system network connections and by means of shared storage (Richardson & North, 2017).

2.10 Ransomware Infection Process

The ransomware infection process consists of five distinct phases (Brewer, 2017). The process starts with the infection phase and quickly moves to delivery of the virus, attack of the backup system, storage encryption, and demand of ransom payment to the user. Figure 3 illustrates the ransomware infection process (Thomas & Galligher, 2018).

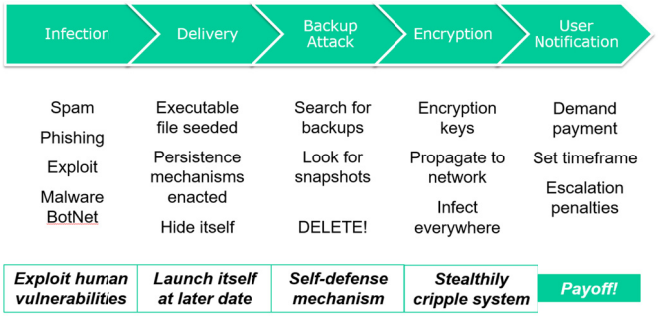

Figure 3. Ransomware infection process

Adapted from Thomas and Galligher (2018).

In the first phase of the ransomware process, the ransomware implants in the system and infection occurs. Often the entry point into the system is facilitated by an exploit kit or by spam mail (Thomas & Galligher, 2018). During this phase, human error is often exploited to allow infection, such as inadequate training, lack of user awareness, ineffective security policies, or failure to adhere to effective security policies (Allen 2017; Brewer, 2017).

In the second phase of the ransomware infection process, the ransomware is delivered and begins to execute its protocol for infection (Thomas & Galligher, 2018). An executable file is planted into the system, and persistence mechanisms are established to embed the ransomware deep into the system. Registry keys are altered to integrate the ransomware into the system even after a shutdown or reboot. This step enables the ransomware to establish an incubation period and encrypt storage at a later date with no assistance (Brewer, 2017).

In the third phase of the ransomware infection process, the ransomware seeks to neutralize the backup system, removing the last line of defense to protect data (Thomas & Galligher, 2018). The ransomware searches for and attempts to delete local backup data. This inhibits the victim's ability to respond to the infection by restoring the system or data to a known uninfected state. When successfully executed, this step strengthens the ransomware's position and increases the likelihood of significant damage and subsequent payment (Brewer, 2017; Harnedy, 2016).

The fourth phase is when data encryption occurs (Thomas & Galligher, 2018). An encryption key is established, with encryption time varied based on several factors such as network design, file size, and number of other devices connected to the host system (Allen, 2017; Brewer, 2017). This is the phase were punitive action occurs.

The last phase of the ransomware process is user notification (Thomas & Galligher, 2018). This is the point at which the ransomware displays a notification of infection and requests ransom payment (like Figure 1). Often the miscreants demand payment within a specified timeframe. If payment is made and the miscreants keep their word, the ransomware removes itself from the system and simultaneously tries to eliminate all traces that might lead forensic investigators to those responsible for the infection (Brewer, 2017; Lelii, 2017).

According to Thomas and Galligher (2018, p. 19) ransomware encryption is continuing to grow in complexity:

Ransomware has further evolved into a combination of shared-secret traditional encryption using fast algorithms such as the Triple Data Encryption Algorithm and Advanced Encryption Standard combined with a public-key system that encrypts the encryption key so it can't be found. This methodology has two basic paths: (1) using a command-and-control system to provide the public key to use to encrypt the shared-secret encryption key and (2) embedding the public key into the application itself. In the former case, the encryption cannot be truly secured (e.g., encrypting the shared-secret encryption key) until the system can connect with the command-and-control center, and in the latter case, all attacked systems will share the same public key so that once the private key is provided to users who have paid the ransom, the private key can then be shared for all others attacked similarly. Often, the system is tagged with a unique identifier given to the user for payment of the ransom. Encryption methods vary by the type of ransomware infecting the system.

2.11 Identity Theft: A Consequence of Phishing

Identity theft, one of negative consequences of phishing attacks, refers to crimes in which a miscreant wrongfully obtains someone else's personal data and uses that information for deception, fraud, or economic gain (DOJ, 2018). The exponential growth of Internet access, mobile device use, ecommerce, and social networking has accelerated cyber crimes such as identity theft (Hille, Walsh, & Cleveland, 2015). The FTC defines identity theft as an intentional attempt or commissions of fraud on another person's personal identifying information without permission or the authority to do so (FTC, 2013).

In 2013, more than 13 million people became victims of identity theft, and more than $18 billion in economic losses occurred because of identity theft (Javelin Research and Strategy, 2014). During this period, individual consumers lodged more than 290,000 identity theft complaints with the FTC (FTC, 2015). Nonconsumers such as public and private companies, government institutions, and nonprofit institutions have the capacity to provide much broader exposure for identity theft. These larger organizations often keep records of employees, customers, members, and owners, potentially exposing whole groups of potential targets simultaneously.

Not all identity theft is reported to the FTC; it is estimated that approximately 4% of the population of the United States, 12 million people, have been victimized by identity theft, resulting in some $12 billion in damages (Hille et al., 2015). Identity theft is also a global problem. In 2015 in the United Kingdom, incidents of identity theft grew by more than 49% despite enhanced governmental efforts to combat it (cifas, 2016). In fact, identity theft is the main complaint of consumers in industrialized nations and is the fastest-growing cyber crime (Harris, Propper, & Stout, 2014). In the United States, the only complaints that outnumber identity theft complaints regard debt collection and impostor scams (FTC, 2017).

Identity theft affects all ranges of targets including individual consumers, businesses, and government institutions. In a well-publicized hacking attack, Target stores fell victim because of lax security practices and policies (Riley & Pagliery, 2015). This attack compromised some 40 million consumers' payment information, including credit card, debit card, and personal identifying information.

At the time of the attack, it was the worst corporate cyber incident in United States history (Riley & Pagliery, 2015). Beyond the 40 million customers whose payment information was compromised, another 70 million had personal information stolen such as name, address, phone number, and other contact information. In addition to paying over $10 million in damages, Target paid for credit monitoring services for all those potentially exposed.

Similarly, the United States government has been the target of cyber attack and identity theft. In mid-2015, the United States Office of Personnel Management (OPM) experienced a security breach and fell victim to an identity theft attack (Naylor, 2016). The attack compromised an estimated four million federal personnel files. It later was revealed that another 20 million people's information was exposed as well.

The compromised information included more than just that of federal employees. Sensitive information was also exposed for contractors and family members of employees (Naylor, 2016). In addition to more-traditional

identifying data such as names and addresses, extremely sensitive and damaging information was also stolen such as social security numbers, dates of birth, and fingerprints. Similar to the Target attack, some theorize that access to the OPM system was gained by means of spear phishing attack on a vendor, which subsequently provided access to federal personnel records. The impact of these attacks was so severe that the serving OPM director was forced to resign.

Because of the rapid adoption of technology in all facets of life, identity theft is a crime that does not discriminate and is one of the fastest-growing cyber crimes (Farina, 2015; Prince, 2012). Growing technology adoption of devices like smart phones and connective media such as social networking sites (Instagram, Twitter, and Facebook) and instant messaging greatly accelerates the growth of identity theft and creates a field ripe with opportunity for miscreants (Computer Fraud & Security, 2016). More than 78% of people in the United States have social media profiles, a number that represents a growth rate of 5% from 2015 to 2016 (Statista, 2017).

These sites offer many connection points, and because of their social nature imply a level of trust that often prompts users to share personal information that can be used to facilitate social engineering attacks such as location, travel time, and information about family members (Ferrara, 2017). With such robust membership and enthusiastic participation, these sites represent a vast repository of personal information about people, making them a prime target for those seeking to commit identity theft.

The large mass of users with memberships on social media sites creates many options for finding identity theft targets. Recent technology changes for the sake of convenience exacerbate this issue. Many websites have taken to using Facebook as a central login and validation source to reduce a person's number of credentials and the number of times that customers must negotiate the sign-on process. Neolane (2017) found that more than 150 websites utilize Facebook as an alternative sign-on method.

Analyzing the 150 sites examined by Neolane (2017) provides interesting insight into the identity theft potential of stealing Facebook login credentials. The largest group of sites using Facebook for user authentication is media-based websites with a total of 68 sites. The next-largest group totaling 17 is ecommerce sites. The remaining groups are entertainment totaling 13, retail totaling 12, other totaling 11, consumer packaged goods totaling 6, automotive totaling 5, and nonprofit totaling 4.

One can easily intuit the wealth of information that could be gleaned from these sites were they compromised. Most account profiles gather basic identifying information such as name, address, and contact information. However, entertainment, retail, and ecommerce sites are likely to have payment and financial information as well. More tangentially, many password security questions involve items such a favorite movie or color, so even the more innocent-appearing sites could provide information to enable identity theft.

While this Facebook-login service is convenient for users and eliminates administrative churn by reducing the number of times that users must log in to separate websites, it also creates tremendous exposure regarding identity theft. Simply by stealing Facebook credentials, miscreants can access multiple sites and the confidential and private information stored in each site's repository. Further, binding these sites together creates a level of dependency that can weaken all of them. As of now, each site is only as secure as the site with the weakest security mechanisms (Stokes, 2014).

While Facebook is a billion-dollar company with massive technology resources, the other members of the chain are likely not as robust or sophisticated. Daisy-chaining accounts in this manner can be dangerous as it makes identity theft much easier to achieve for miscreants (Stokes, 2014). Once a miscreant gains a target's Facebook credentials, doors are opened to all connected accounts. However, even more frightening, the miscreant at that point has the means to establish new accounts with the victim's identity, greatly increasing potential exposure.

When users initiate the daisy-chain process and attach their Facebook account to another site or platform, there is an inherent assumption that information will be used for good and appropriate purposes (Stokes, 2014). However, that base assumption may not be correct. The site owners or creators may be miscreants themselves and may not have good intent. Further, miscreants could temporarily hijack the potentially-less-secure site for the purpose of stealing credentials. Both Target and the United States government were infiltrated because of poor security practices by partners (Weiss & Miller, 2015; Naylor, 2016).

In fact, social media sites also facilitate the sharing of corporate information (Ferrara, 2017). It is not uncommon for social media participants to announce items such as promotions, job changes, or significant work accomplishments on social media to inform family and friends of their status. However, many social media users do not customize their privacy settings upon joining a site. Many users joined social media sites such as Facebook years before privacy and cyber security were such public concerns. Those who do not actively manage

their privacy settings put themselves at risk for enabling social-engineering-based identity theft attacks (Taylor, 2017).

The technology boom of the past two decades has resulted in massive adoption of personal technology, which in turn has led to a massive aggregation of personal data on the Internet, leading to increased potential for identity theft (Lai, Li, & Hsieh, 2010; Yallapragada, Roe, & Toma, 2012). This adoption and daily use of technology for work, pleasure, and entertainment enables a broad spectrum of cyber crimes such as online scams, profile-cloning, and phishing-based attacks, which are all geared toward stealing people's identifying information and security credentials (Anderson, Durbin, & Salinger, 2008; Zhu, Caprenter, & Kulkarni, 2012). Once a miscreant gathers a sufficient amount of personal idenitifying information from various sources, they can conduct an identity theft attack (Lai et al., 2010; Yallapragada et al., 2012).

The damages incurred as a result of identity theft are difficult to pinpoint exactly, but the impact of the problem is staggering. Estimates place 2012 identity theft damages at almost $12 billion (Hille et al., 2015). Two years later, some 28.6 million victims in the United States were affected by identity theft, and $16 billion was stolen from consumers who participated in online shopping (Anderson, 2014). Demographic studies have found that several archetypes are more likely to fall victim to identity theft than others. Younger consumers, high-income consumers, and women are more likely to be victims of identity theft than other demographics (Anderson, 2014; Reyns & Henson, 2015). Reseachers have found that social and technology factors are the most significant determiners for potential identity theft (Prince, 2012).

2.12 Identity Theft Momentum

Some data suggest that identity theft may be decreasing. The FTC (2017) Consumer Sentinel Network Data Book for January – December 2016 shows that identity theft declined for consumers in 2016. Consumer identity theft complaints fell from 490,226 to 399,225. Figure 4 shows the trend of identity theft reports from 2001 to 2016 (FTC, 2017):

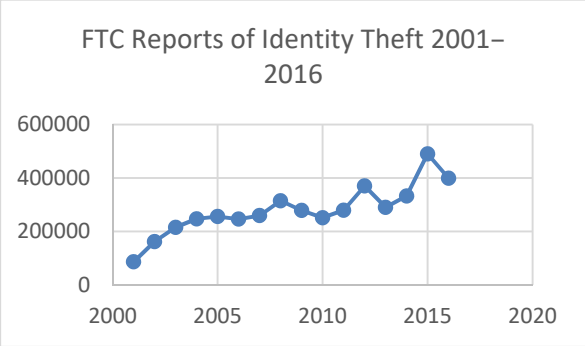

Figure 4. Chart of reports of identity theft to the FTC from 2001 to 2016

Adapted from FTC (2017).

While the downward movement in reports of identity theft is good to see, it is not necessarily indicative of a decline as the longer-term trend is generally upward.

However, some researchers do suggest that the number of incidents of identity theft may be declining (Pascal & Miller, 2015). In a report funded by LifeLock, Inc., the Javelin Strategy and Research Group found that there may be a downward trend in damages incurred by identity theft, citing a 3% decresase in victims and a $2 billion decrease in damages incurred. The authors of the report also stated, though, that although the numbers have changed, the magnitude of the problem has not (Pascal & Miller, 2015). This report's methodology, however, sent surveys to 5,000 consumers and analyzed their responses rather than documenting empirical data about losses. The Javelin Group also identified a variable limiting optimal visibility into identity theft: online identity theft versus physical identity theft such as when a wallet is stolen. The Javelin Group also attributed the reduction in damages to credit and identity monitoring services provided by companies such as LifeLock, Inc.—who funded the study.

The Javelin study has obvious potential weaknesses. First, Life Lock, Inc. funded the study (Pascal & Miller, 2015). This relationship creates potential opportunity for vested interest in the results. Second, the scope of

identity theft in the study was defined as using another person's identity for financial gain. This definition limits the range of identity theft to purely finance-based identity theft and specifically excludes idenitity theft for other purposes such as access to nonfinancial resources. Lastly, the sample for the study was likely a convenience sample, which many privately funded studies are prone to use, limiting the sample diversity.

2.13 Summary

There is no doubt that spear phishing is a significant problem that affects all aspects of society from personal to commercial to governmental stakeholders. Government statistics show that incidents of spear phishing and its associated problems, such as ransomware and identity theft, are increasing and causing tremendous amounts of damage worldwide. Researchers have spent considerable time and resources studying users who succumb to spear phishing and their demographic and psychographic profiles.

While this information is useful, it does not solve the issue. Even if it were possible to identify all those predisposed to falling for spear phishing attacks, it would be impractical if not impossible to isolate such a large part of the general population. Further, the problem is more complex than the existence of mere human susceptibility traits. Many factors exacerbate this problem such as the ubiquitous adoption of technology in everyday interactions (Computer Fraud & Security, 2016), the mass adoption of social media sites (Greenwald, 2016), and the growing sophistication of miscreants (Daly, 2009; Brewer, 2017; Thomas & Galligher, 2018).

A recent study showed that the vast majority of people, as many as 97%, is unable to accurately detect phishing attacks and that 20% of people who might be deemed proficient succumb to phishing attacks at least 10% of the time (McAfee, 2015). Given the magnitude of the problem, the significance of damage caused by this phenomenon, and the inability to isolate those susceptible to the issues, another alternative solution should be explored. Scholars, managers, and government leaders have called for more research and information to help combat spear phishing attacks and the resultant negative consequences such as ransomware and identity theft (Collier, 2017; FTC, 2017; Komatsu, Takagi, & Takemura, 2013; Sun & Lee, 2016). One method to help combat this problem that merits exploration is empowering users to resist spear phishing attacks.

3. Methodology

This exploratory, single, qualitative case study addressed the problem of spear phishing. Spear phishing is one of the most difficult challenges faced by IT departments. Spear phishing is the entry point for many intrusions and hacking activities such as ransomware and identity theft (Goel et al., 2017; Sjouwerman, 2015). The results of these attacks are devastating. Researchers have touted identity theft, for example, as the signature crime of the information age (Zaeem, Mnaoharan, Yang, & Barber, 2017). In 2013, more than 13 million people fell victim to identity theft and suffered some $18 billion in losses (Javelin Research and Strategy, 2014). Phishing attacks enable many different types of intrusion beyond identity theft—scholars have identified end users and employees as the most vulnerable point of entry for these attacks and have called for additional research to address this growing problem (Komatsu, et al., 2013; Sun & Lee, 2016).

The study employed semi-structured interviews with information security SMEs to explore the reasons that users fall victim to spear phishing attack and to identify techniques that could be used to prevent users from succumbing to phishing attacks. The data collected from the interviews were analyzed to identify patterns and common themes. The study results can be used to answer calls for research from scholars to expand current theories, such as TPB and PMT, that are used to predict and influence behavior (Ajzen, 2014; Floyd et al., 2000) and to provide the information required for practioners in the field to develop methods and tools to prepare users to resist spear phishing attacks.

3.1 Research Method and Design

This study was an exploratory, single, qualitative case study because it sought to answer a how or why question, and qualitative case studies best address how or why questions (Tetnowski, 2015; Yin, 2014). While quantitative research methods are ideal for addressing how much, where, how many, what, and how questions, quantitative research methods are not as effective as qualitative research methods at answering how or why questions (Baškarada, 2014). Moreover, qualitative research enables the opportunity for researchers to obtain rich, thick, and in-depth data (Cronin, 2014; Dasgupta, 2015). Case study methodology enables researchers to combine theoretical knowledge with insight from new empirical data to expand and validate theories (Duxbury, 2012; Yin, 2014). Case study research is especially effective for use in situations with limited knowledge about how or why behaviors, events, and actions occur or when current perspectives and insights are inadequate (Denham & Onwegbuzie, 2013; Yin, 2014).

This study explored the reasons why users succumb to spear phishing attacks, a phenomenon that is not well understood and a problem that has not been fully addressed by current literature and business practices (Lötter & Futcher, 2017). Spear phishing enables problems that are catastrophic in nature and have a huge global impact. As this problem continues to plague academic and business communities, more research is needed to help address this issue (Lötter & Futcher, 2017). A significant value proposition of this research is that it establishes a pool of data that can expand theories like TPB and PMT that predict behavior and influence users (Ajzen, 2014; Floyd et al., 2000).

Case study research was recommended for this study because of its effectiveness to address the research problem. Case study methodology uses empirical inquiry to gather information about limited situations focused on tangible real-life scenarios (Duxbury, 2014; Yin, 2014). Scholars recommend the use of case study design when the phenomenon to be studied has not been fully explored and the goal of research is to understand why the phenomenon is occurring (Duxbury 2012; Yin, 2014). Furthermore, case study methodology discovers how and why people make decisions (Barth & Thomas, 2012; Yin, 2014). Case study design was selected for this research because it is an effective method for conducting the study. The studied phenomenon is a real-life situation that is not fully understood and that has not been fully explored, and the research attempts to answer a how or why question (Dasgupta, 2015; Tetnowski, 2015; Yin, 2014).

Yin's (2014) protocol for case study research was utilized:

1. Create problem statement
2. Generate research questions
3. Create a case study approach and design
4. Prepare for the collection of data
5. Collect data
6. Analyze and evaluate data

Report the findings of the case study

A semi-structured interview process purposefully collected data (Robinson, 2014). SMEs were the subjects of the interviews based on demographic and psychographic segmentation. Study participants were chosen by means of criterion sampling (Robinson, 2014).

3.2 Population and Sample

Both theoretical and practical factors influence sample design in qualitative research (Robinson, 2014). This study used criterion sampling and purposeful data collection, which are recognized as standard for qualitative research (Robinson, 2014). Accordingly, it was essential to identify study participants who actually interact with the phenomenon being investigated (user interaction with spear phishing) and who have responsibility for security functions (preventing/combating spear phishing). Thus, study participants were security professionals who are responsible for end-user security at their organizations and who have specific responsibility for dealing with spear phishing attacks or have attained the CISSP certification, which validates five years of hands-on security experience. To further delineate the sample, study participants were based in Austin, Texas. All study participants conformed to these criteria, ensuring the appropriateness of the sample and the achievability of the research project.

Logic-based sampling is common in many studies. However, sample size is less relevant in single-case studies (Robinson, 2014; Yin, 2014). Recommendations for the sample size of a single-case study range from as little as 5 to less than 10 interview subjects (Mason, 2010; Robinson, 2014). A general recommendation is to work until one achieves saturation of the data. Data saturation occurs when the collection of new data no longer yields new information (Houghton, Casey, Shaw, & Murphy, 2013). Accordingly, this study conducted interviews until thematic data saturation was achieved—when three of the last five interviews provided no new data or insights (Mason, 2010; Robinson, 2014).

3.3 Materials and Instruments

Case study protocol was the instrument used in this study. Using case study protocol results in reliable research and provides a definitive template for the researcher to use during data collection (Yin, 2014). Semi-structured interviews were used in this case study focusing on a specific topic with a list of specifically developed interview questions (Rubin & Rubin, 2012). Semi-structured interviews are common in social science research to explore behavior (Bjerke & Ind, 2015). The interviews were conducted with information security SMEs who had either

obtained the CISSP certification, which validates security experience, or who have information system security as a primary role in their job duties.

Interview questions were open-ended and were developed based on a comprehensive literature review. These questions served as the basis for an interview guide. The interview guide was used to facilitate the interviews. Use of the interview guide ensured consistency of interviews while simultaneously allowing for fluid conversations so that rich, in-depth information could be obtained. The interview guide ensured that interviews were conducted in a timely and efficient manner (Rubin & Rubin, 2012; Yin, 2014).

The interview questions and interview guide were validated with a field test (Baxter & Jack, 2008). A small group of technology experts with similar backgrounds to interview subjects were asked to review the questions. The experts were asked to provide feedback on the language, wording, and interpretations of the interview questions. This feedback was used to refine the study questions.

Natural settings were used to conduct the interviews. Face-to face-interviews were conducted and enabled the ability to directly observe study subjects and view any nonverbal cues (Almutairi, Gardner, & McCarthy, 2014).

3.4 Data Collection and Analysis

Data gathering for the study consisted of a three-step process: (a) obtaining informed consents, (b) conducting semi-structured interviews, and (c) transcribing recorded interviews for analysis. The researcher approached candidates for participation in the study via email based on their participation in security user groups and referrals from other candidates. Semi-structured interviews are recommended to collect facts from interview participants (Rowley, 2012). Interview recording and transcription ensured accuracy and reliability of the data; the researcher defined concepts and relationships by converting the transcribed text to frequency distributions (Leedy & Ormond, 2015). NVivo® 11 for Windows software was used to perform content analysis to examine the context of frequency distributions and relationships by displaying data graphically, in accordance with Leedy's and Ormond's (2015) recommended procedures.

The semi-structured interview guides, questions, and framework were reviewed by other experienced qualitative researchers including the American Military University institutional review board to ensure the validity of the study methodology and approach. The collected data were verified by means of member-checking. Member-checking entails interview transcript review by study participants to ensure that all data, interpretations, and conclusions are accurate (Reay, 2014). The researcher performed member checks shortly after all data were transcribed from the interviews by either phone call or email.

4. Findings

4.1 Findings

The research questions for this study explored the traits of users that make them susceptible to spear phishing and what can be done to better enable users to resist spear phishing attacks. The implications for this study are organized by the themes that emerged from the interviews. Nine themes emerged from the study interviews: (a) lack of information literacy skills, (b) sophistication of miscreant attacks, (c) high-impact job roles, (d) transactional jobs with high volumes of email, (e) unfamiliarity with phishing, (e) confidence level, (f) training, (g) familiarity with phishing victims, and (h) testing proficiency.

Theme 1: Lack of information literacy skills. It is fairly easy to intuit that technology savvy better enables one to navigate dangers in cyber space. Strong information literacy skills reduce user vulnerability to spear phishing attacks (Wright & Marett, 2010). Users with strong computer skills are more proficient at analyzing messages and hyperlinks for dangerous anomalies. Users who possess high levels of technical acumen regarding web browsing, security, and email concepts such as spyware, cookies, viruses, and network security are also less susceptible to spear phishing attacks (Sheng et al., 2010).

These findings suggest that higher levels of information literacy and computer knowledge better empower users to resist spear phishing attacks. Based on these results, IT professionals and managers could work together to develop target training programs to increase information literacy skills and reduce the impact of spear phishing attacks (Caputo, et al., 2014).

Theme 2: Sophistication of miscreant attacks. The SMEs interviewed in the study strongly identified the sophistication of miscreant spear phishing attacks. The complexity and frequency of attacks have increased at alarming rates. In a survey in 2016, 76% of 500 cyber security professionals surveyed in 2016 reported that their organization had become a victim of phishing attack (Williams & Ashenden, 2017). According to Williams and Ashenden (2017), IT organizations are struggling to keep up.

The implication of this, then, is that the challenge of spear phishing is becoming even more robust. Consequently, users must be better prepared to resist the growingly sophisticated miscreant attacks. This challenge reinforces the need to improve information literacy skills regarding security, email, and web interactions (Sheng et al., 2010).

Theme 3: High-impact job roles. The SME interviews revealed that users in high-impact job roles who deal with sensitive data and who interact with company leadership are more susceptible to phishing attacks. These users often have access to sensitive corporate data and are a favorite target of miscreants for spear phishing attacks because they are used to sending sensitive data in a short timeframe (Greenwald, 2016; Landsman, 2016).

The implications of this theme are that this subset of users is a prime target for attack. Accordingly, they should be considered a special interest group and be better prepared for attacks. If attacks compromise these users, there is capacity for increased damage to the organization.

Theme 4: Transactional jobs with high volumes of email. Another theme that emerged from the study was that users in highly transactional jobs who process large amounts of email on a daily basis are more susceptible to spear phishing attack. Familiar and habitual use of email can make computer users more vulnerable to phishing attack (Vishwanath, 2015). These users should be identified as a category for special training and monitoring to reduce susceptibility to spear phishing attack.

Theme 5: Unfamiliarity with phishing. Several SMEs identified the theme of users being unfamiliar with phishing. Clearly, those who are unaware of phishing are powerless to defend against it. As the world has become more connected, there is still a significant amount of people who are unaware of phishing schemes and miscreant attacks, which is why 1 in 10 people open email attachments without knowing what they are clicking on (Aguilar, 2015). This group, like the previous groups mentioned, should be identified as special and provided with tools and training to resist spear phishing.

Theme 6: Confidence level. SMEs identified both low and high confidence levels as factors that can increase user susceptibility to spear phishing attacks. Users who are overconfident are more likely to click on phishing links and rely on antivirus software to protect them (Barry, 2017). Likewise, users with low confidence are likely to click on links to close the current transaction and move on to the next so that they don't appear behind in their work. This group should be identified as special, and processes and tools should be put in place to help enable them to resist spear phishing.

Theme 7: Training. The SMEs felt that training was a critical tool to enable users to resist spear phishing. However, many stated that training was sub-optimal, infrequent, or unengaging. This implies that training should be over-hauled to ensure that it is properly absorbed and embraced by users.

Theme 8: Familiarity with phishing victims. One of the strongest themes that emerged from the study interviews was that users who know victims of spear phishing or where who have been spear phishing victims themselves are more resistant to spear phishing attacks. The SMEs suggested that these users have more fear of damage from miscreants and are thus more vigilant to identify potential attacks and to be more suspicious of emails. Research has shown fear realization to be a positive motivator in generating protection response (Boss, et al., 2015). Making phishing and its negative effects more real to users is an effective mechanism for making users more aware of spear phishing and participating in security training to prevent spear phishing.

Theme 9: Testing proficiency. SMEs identified testing proficiency as a tool that can be useful in preparing users to resist spear phishing. One SME engaged an outside service to test user proficiency on a monthly basis. Testing strategies can be effective, especially if users know they will be tested regularly; however, they can also yield unpredictable results such as users sharing the content of test messages with others inside and outside the company (Kohgadai, 2018). Testing is a tool that should be considered part of a spear phishing prevention plan.

5. Discussion

This study was a single exploratory case study. The researcher collected data from seven security SMEs in the Austin area. The research used an interview guide to conduct semi-structured interviews comprising open-ended questions (Yin, 2014). Each participant in the study was an adult with a primary job role of information system security. The study focused on exploring methods to empower users to resist spear phishing attacks.

The interview guide consisted of nine open-ended questions. The researcher used the interview guide to conduct timely, consistent, and efficient interviews (Rubin & Rubin, 2012; Yin, 2014). The interviews provided coverage to achieve the purpose of the study. The researcher presented the study questions to experienced researchers and the thesis advisor to ensure the validity of the questions (Jacob & Furgeson, 2012). The researcher used member checks to ensure the collected data were rich and valid (Torrance, 2012).

The researcher transcribed and imported the interviews into NVivo® 11 for Windows software. The software helped identify nine unique themes by coding responses with similar characteristics (Azeem & Salfi, 2012). The researcher ensured reliability in the study by carefully conducting interviews, recording interview sessions, and transcribing interview recordings (Azeem & Salfi, 2012).

Information security managers in the field can use the findings from this study to craft effective security programs to empower users to resist spear phishing. The traits identified in this study can be used to segment users into groups to better understand their unique qualities and needs regarding security support and training. This will enable the development of efficient screening and training programs that increase spear phishing awareness, provide spear phishing detection skills and email analysis skills, and create a realization of the damaging effects of spear phishing to decrease spear phishing incidents (Jensen et al., 2017 Komatsu et al., 2013; Kumaraguru, et al. , 2010; Sun & Lee, 2016).

The findings of this study contribute to the body of knowledge and literature regarding spear phishing by providing insight into the traits of users that make them both more vulnerable and more resilient to spear phishing techniques, as well as insight into effective methods for training users (Komatsu et al., 2013; Sun & Lee, 2016). The study findings can help refine and expand on theories that predict behavior in information security such as TPB (Ajzen, 2014) and PMT (Floyd et al., 2000). Lastly, the study provided recommendations for future research to validate the study results and to use the study results to seed further qualitative research.

5.1 Recommendations

This study identified themes that provide a basis for recommendations for current practice as well as future research. The findings in this study support isolated findings of other research and security literature (Aguilar, 2015; Barry, 2017; Boss et al., 2015; Caputo et al., 2014; Greenwald, 2016; Landsman, 2016; Sheng et al., 2010; Vishwanath, 2015; Williams & Ashenden, 2017; Wright & Marett, 2010). This qualitative case study used a small sample, and findings may not be generalizable to other situations or locales. The following paragraphs present recommendations for practice and future research.

Recommendations for practice. The first recommendation for practice is that IT security managers should work with business managers to segment employees into groups in a manner similar to the way that businesses segment customers. Segmenting is a powerful tool that helps divide people into distinct groups to better understand their needs and traits that can help predict behavior (Soloman, 2013). Segmentation should be considered in the following areas:

- Level of information literacy competence
- High-impact job roles
- Transactional roles with high volumes of email
- Those unfamiliar with phishing
- Those with high levels of confidence
- Those with low levels of confidence

Identifying these at-risk groups provides a mechanism for businesses to categorize employees. Once these categories are established, business and IT managers can work to determine more focused screening and training programs to help prevent spear phishing attacks from being successful.

After the appropriate user segments are identified, the next recommendation is for firms to develop training for each identified segment. Training should contain real-life examples that highlight the seriousness of the spear phishing problem and the impact of the resultant damage, such as identity theft and ransomware. Training should use real case studies, along with actual incidents that have occurred within the company and personal incidents that have happened to other employees. Sharing these actual and personal examples will result in a strong realization of the dangerous impact of spear phishing and will evoke a more personal protection response, which has been proven to increase vigilance and self-protection response— which can result in increased security proficiency (Boss et al., 2015)

5.2 Recommendations for Future Research

The first recommendation for future research is to explore other locations. The researcher conducted this study in Austin, Texas. Similar studies should be conducted in other areas of the United States to validate these patterns and observations. This study could also be replicated in other countries.

The next recommendation for how researchers can use the findings from this study is to seed quantitative research (Cronin, 2014; Duxbury, 2012; Yin, 2014). Quantitative studies could explore the themes identified in this study to better understand their effects on preparing users to resist spear phishing, to improve training programs, and to improve security processes. Future researchers should also explore utilizing PMT to improve security training and user resistance to spear phishing attacks, as researchers have called for additional research to combat spear phishing (Komatsu, Takagi, & Takemura, 2013; Sun & Lee, 2016).

6. Limitations of the Study

There were several limitations for the study. First, case study research has inherent limitations such as difficult and laborious execution, a weak basis for academic generalization, and a potential lack of rigor (Ridder, 2017; Yin, 2014). Case study research can suffer from a lack of rigor for several reasons, such as the researcher allowing bias to creep into the study, a lack of discipline of the researcher, or failure to accurately capture and document information from interviews (Yin, 2014). The researcher mitigated these limitations in this study by diligently conducting the research, as well as creating and following a case study protocol for the study. A succinct and clear interview guide was designed for and used in the study to guide the interview process (Thomas, 2017b). Recording and transcribing interviews ensured accuracy, and member checks ensured the validity of the rich data gathered (Birt, Scott, Cavers, Campbell, & Walter, 2016).

6.1 Delimitations of the Study

The major delimitations of this study were the demographics used to select study subject population. Study subjects were located in Austin, Texas and were deemed SMEs in information system security by either having earned the Certified Information Systems Security Professional (CISSP) certification or being primarily responsible for security functions within their IT departments.

References

Aguilar, M. (2015). *The number of people who fall for phishing emails is staggering*. Retrieved February 18, 2018, from GIZMODO: https://gizmodo.com/the-number-of-people-who-fall-for-phishing-emails-is-st-1697725476

Ajzen, I. (2014). The theory of planned behaviour is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, & Arujo-Soares. *Health Physchology Review, 9*, 131-137. https://doi.org/10.4054/DemRes.2013.29.8

Allen, C. (2017). *Cyber-terrorism: The next logical threat to come from IS*. Retrieved November 13, 2017, from https://www.scmagazineuk.com/cyber-terrorism-the-next-logical-threat-to-come-from-is/article/675965/

Almutairi, A. F., Gardner, G. E., & McCarthy, A. (2014). Practical guidance for the use of a pattern-matching technique in case-study research: A case presentation. *Nursing & Health Sciences, 16*(2), 239-244. https://doi.org/10.1111/nhs.12096

Alperovitch, D. (2016). *Bears in the midst: Intrusion into the Democratic National Committee.* Retrieved Janurary 21, 2018, from Crowd Strike: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. Retrieved from https://misq.org

Anderson, G. (2014). *Identity theft: Who's at risk?* Retrieved January 22, 2018, from https://www.aarp.org/research/topics/economics/info-2014/identity-theft-incidence-risk-behaviors.html

Anderson, K., Durbin, E., & Salinger, M. (2008). Identity theft. *Journal of Economic Perspectives, 22*(2), 171-192. https://doi.org/10.1108/13590791211190704

Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and meet. Philosophical Transactions of the Royal Society of London A: Mathematical. *Physical and Engineering Sciences, 367*(1898), 2717-2727. https://doi.org/10.1098/rsta.2009.0027

Azeem, M., & Salfi, N. (2012). Usuage of NVIVO software for qualitative data analysis. *Academic Research International, 2*(1), 262-266. Retrieved from http://www.journals.savap.org.pk

Barry, C. (2017). *Can your security system overcome user confidence?* Retrieved February 18, 2018, from https://blog.barracuda.com/2017/06/28/can-your-security-system-overcome-user-confidence/

Barth, M., &Thomas, I. (2012). A multi-dimensional approach to consumer motivation: Exploring economic,

hedonic, and normative consumption goals. *Journal of Consumer Marketing, 33*(1), 75-84. https://doi.org/10.1108/JCM-08-2014-1091

Baškarada, S. (2014). Qualitative Case-study guidelines. *The Qualitative Report, 19*, 1-18. Retrieved from http://www.nove.edu/QR

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementatiton for novice researchers. *The Qualitative Report, 13*(4), 544-559. Retrieved from http://nsuworks.nova.edu/tqr_home/

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher, 20*(2), 40-43. https://doi.org/10.7748/nr2012.11.20.2.40.c9442

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1802-1811. https://doi.org/10.1177/1049732316654870

Bjerke, R., & Ind, N. (2015). The influence of aesthetic invesments on employees: An investigation of arts' impact on employees. *EuroMed Journal of Business, 10*(2), 214-233. https://doi.org/10.1108/EMJB-09-2014-0029

Bleau, H. (2017). *2017 Global fraud and cybercrime forecast*. Retrieved from RSA: https://www.rsa.com/en-us/resources/2017-global-fraud-and-cybercrime-forecast

Bobko, P., Barelka, A., Hirshfield, L., & Lyons, J. (2014). Invited article: The construct of suspicion and how it can benefit theories and models in organizational science. *Journal of Business Psychology, 29*(3), 335-342. https://doi.org/10.1007/s10869-014-9360-y

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864. Retrieved from https://misq.org

Brewer, R. (2017). Ransomware attacks: detection, prevention, and cure. *Network Security, 9,* 5-9. http://dx.doi.org.ezproxy.utica.edu/10.1016/S1353-4858(16)30086-1

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

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy, 12*(1), 28-38. https://doi.org/10.1109/MSP.2013.106

cifas. (2016). *Fraudscape 2016*. Retrieved from https://www.cifas.org.uk/research_and_reports

Clarke, R. A., & Knake, R. K. (2010). *The next threat to national security and what to do about it.* Pymble, Australia: HarperCollins Publishers.

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ, 189*(22), 786-787. https://doi.org/10.1503/cmaj.1095434

Computer Fraud & Security. (2016). Identity theft rises sharply as fraudsters target social media. *Computer Fraud & Security, 7*, 1-3. https://doi.org/10.1016/S1361-3723(16)30048-3

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. https://doi.org/10.7748/nr.21.5.19.e1240

CSO. (2012, February 28). *CSO's ultimate guide to social engineering.* Retrieved January 21, 2018, from https://www.csoonline.com/article/2130996/identity-access/cso-s-ultimate-guide-to-social-engineering.html

Daly, M. (2009, November 4). The advanced persistent threat. Retrieved January 21, 2018, from http://static.usenix.org/event/lisa09/tech/slides/daly.pdf

Darwish, A., El Zarka, A., & Aloul, F. (2013). *Towards understanding phishing victims' profile.* Retrieved January 21, 2018, from psu.edu: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.310.8972&rep=rep1&type=pdf

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision: The Journal of Business, 19*(2), 147-160. https://doi.org/10.1177/0972262915575661

De Leeuw, A., Valois, P., Ajzen, I., & Schmidt, P. (2015). Using the theory of planned behavior to identify key beliefs underlying pro-environmental behavior in high school students: Implication for educational

interventions. *Environmental Psychology, 42*, 128-138. https://doi.org/10.1177/147/1470593114558530

Denham, M. A., & Onwegbuzie, A. J. (2013). Beyond words: Using nonverbal communication data in research to enhance thick description and interpretation. *International Journal of Qualitative Methods, 1*, 670-696. https://doi.org/10.1177/160940691301200137

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security,* (10), 5-8. https://doi.org/10.1016/S1361-3723(16)30079-3

DOJ. (2018). *Idenitity theft.* Retrieved January 21, 2018, from Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Duxbury, T. (2012). Towards more case study research in entrepreneurship. *Technology Innovation Management Review, 2*(3), 9-17. Retrieved from http://www.timereview.ca

El-Din, R., Cairns, P., & Clark, J. (2015). The human factor in mobile phishing. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 4*, 53-65. https://doi.org/10.4018/978-1-4666-8345-7.ch004

Farina, K. (2015). Cyber crime: Identity theft. *International Encyclopedia of the Social and Behavioral Sciences,* 633-637. https://doi.org/10.1016/B978-0-08-097086-8.45054-3

FBI. (2005). *CSI/FBI Computer Crime and Security Survey.* Retrieved from http://www.wheresthepapger.org/FBIccs2005.pdf

FBI. (2018, 2018). *Cyber crime.* Retrieved February 16, 2018, from FBI.gov: https://www.fbi.gov/investigate/cyber

Ferrara, J. (2017). *Social engineering: How social media is compounding the threat.* Retrieved January 22, 2018, from https://www.scmagazineuk.com/social-engineering-how-social-media-is-compounding-the-threat/article/668589/

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Psychology, 30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

FTC. (2013). *Consumer Sentinel Network Data Book.* Retrieved from https://www.huffingtonpost.com/2012/02/28/identity-theft-cost-americans-152-billion-2011-ftc_n_1307485.html

FTC. (2015). *Consumer Setntinel Network Data Book for January-December 2014.* Retrieved from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2014

FTC. (2017). *Consumer Sentinel Network Data Book 2016.* Retrieved January 22, 2018, from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

Ghosh, S. (2017). *The massive 'Petya' cyber attack has hit 64 countries so far and there's no kill switch.* Retrieved November 28, 2017, from http://www.businessinsider.com/petya-cyberattack-hit-64-countries-no-kill-switch-2017-6

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association of Information Systems, 18*(1), 22-44. Retrieved from http://aisel.aisnet.org/jais/

Greenwald, J. (2016). *Employers face growing risk in tax season: 'Spear phishing'.* Retrieved from http://www.businessinsurance.com

Halevi, T., Memon, N., & Nov, O. (2015). *Spear phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear phishing attacks.* Retrieved January 21, 2018, from Social Sciences Research Network: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report, 17*(2), 510-517. Retrieved from http://www.nova.edu/ssss

Harris, E., Propper, N., & Stout, H. (2014). *A sneaky path into Target customer's wallets.* Retrieved January 21, 2018, from New York Times: https://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). ndividual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review, 40*(2), 265-281.

https://doi.org/10.1108/OIR-04-2015-0106

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. https://doi.org/10/1016/j.dss.2009.02.005

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19. https://doi.org/10.1016/j.intmar.2014.10.001

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*(4), 12-17. https://doi.org/10.7748/nr2013.03.20.4.12.e326

IRS. (2017). *Dangerous W-2 phishing scam evolving; targeting schools, restaurants, hospitals, tribal groups and others.* Retrieved from https://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

Jacob, S., & Furgeson, P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report, 17*(6), 1-10. Retrieved from http://www.nova.edu/ssss

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100. https://doi.org/10.1145/1290958.1290968

Javelin Research and Strategy. (2014). Identity fraud report: card data breaches and inadequate consumer password habits fuel disturbing fraud trends. *Pleasanton, CA: Javelin Strategy and Research.* Retrieved from https://www.javelinstrategy.com/coverage-area/2014-identity-fraud-report-card-data-breaches-and-inadequate-consumer-password-habits

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

KnowBe4. (2017). *AIDS Trojan or PC Cyborg Ransomware.* Retrieved November 28, 2017, from https://www.knowbe4.com/aids-trojan

Kohgadai, A. (2018). *Top phishing test tools and simulators.* Retrieved February 18, 2018, from https://www.skyhighnetworks.com/cloud-security-blog/top-phishing-test-tools-and-simulators/

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security. *Information Management & Computer Security, 21*(1), 5-15. https://doi.org/10.1108/09685221311314383

Kumaraguru, K., Sheng, S., Acquisiti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fail. *ACM Trainsactions on Internet Technology (TOIT), 10*(2), 2-30. https://doi.org/10.1145/1754393.1754396

Kumaraguru, P., Cranshaw, J., Acquisiti, A., Cranor, L., Hong, J., Blair, M., & Pham, T. (2009). *School of phish: A real-world evaluation of anti-phishing training.* Retrieved January 21, 2018, fromhttps://www.cs.cmu.edu/~jasonh/publications/soups2009-school-of-phish-final.pdf

Lai, F., Li, D., & Hsieh, C. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847. https://doi.org/10.1016/jcose.2010.08.001

Landesman, T. (2016, March 31). 55 companies and counting - W-2 spear phishing attacks continue to increase. Retrieved January 21, 2018, from https://blog.cloudmark.com/2016/03/31/55-companies-and-counting-w-2-spear-phishing-attacks-continue-to-increase/

Lastdrager, E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(9). https://doi.org/10.1186/s40163-014-0009-y

Leedy, P. D., & Ormond, J. E. (2015). *Practical research: Planning and design* (11th ed.). Boston: Pearson.

Lelii, S. (2017). *WannaCry ransomware attacks shows value of data backups.* Retrieved from http://searchdatabackup.techtarget.com/news/450418934/WannaCry-ransomware-attack-shows-value-of-data-backups

Lipton, E., Sanger, D., & Shane, S. (2016, December 13). *The perfect weapon: How Russian cyber power invaded the U.S.* Retrieved January 21, 2018, from

https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Longstaff, T. (1989). *Information about the PC CYBORG (AIDS) trojan horse.* Retrieved from http://www.securityfocus.com/advisories/700

Lötter, A., & Futcher, L. (2017). A framework to assist email users in the identification of phishing attacks. *Information & Computer Security, 23*(4), 370-381. https://doi.org/10.1108/

Majauskas, G. (2009). *Nortel Antivirus - How to remove.* Retrieved November 28, 2017, fromhttps://www.2-viruses.com/remove-nortel-antivirus

Manes, C. (2017). *The 10 worst ransomware attacks that ever happened.* Retrieved January 5, 2018, from https://techtalk.gfi.com/the-10-worst-ransomware-attacks-that-ever-happened/

Mansfield-Devine, S. (2016). Ransomeware: Taking business hostage. *Network Security*, (10), 8-17. Retrieved from http://www.sciencedirect.com/journal/network-security

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research, 11*(3), 1-19.

McAfee. (2015). *97% of people globally unable to correctly identify phishing emails.* Retrieved January 21, 2018, from https://www.mcafee.com/us/about/news/2015/q2/20150512-01.aspx

Mitnick, K. (2017). *Who has your data? Hackers are getting bolder. Here's how to fight back.* Retrieved from https://www.aarp.org/money/scams-fraud/info-2017/fraud-protection-identity-theft.html

Naylor, B. (2016). *One year after OPM data breach, what has the government learned?* Retrieved from http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned

Neolane. (2017). *Analysis of 150 websites using Facebook login.* Retrieved fromhttp://www.slideshare.net/Neolane/analysis-of-150-websites-using-facebook-login

Pascal, A., & Miller, S. (2015). *2015 identity fraud: Protecting vulnerable populations.* Retrieved January 22, 2018, from https://www.javelinstrategy.com/brochure/347

PhishMe. (2016). *Enterprise Phishing Susceptibility and Resiliency Report.* Leesburg: PhishMe. Retrieved from https://phishme.com/enterprise-phishing-susceptibility-report

Prince, B. (2012). *Americans rate cyber-security as hot issue in presidential election: Survey.* Retrieved January 21, 2018, from http://www.eweek.com/security/americans-rate-cyber-security-as-hot-issue-in-presidential-election-survey

Reay, T. (2014). Publishing qualitative research. *Family Business Review, 27*(2), 95-102. https://doi.org/10.1177/0894486514529209

Reyns, B., & Henson, B. (2015). The theif with a thousand faces and the victim with none: Identifying determinant for online identity theft victimization with routine activity theory. *International Journal of Offender Therapty and Comparative Criminology, 60*(10), 1119-1139. https://doi.org/10.1177/0306624X15572861

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-21. Retrieved from http://www.usimr.org/

Richwine, L. (2014). *Cyber attack could cost Sony studio as much as $100 million.* Retrieved December 20, 2017, from https://www.reuters.com/article/us-sony-cybersecurity-costs/cyber-attack-could-cost-sony-studio-as-much-as-100-million-idUSKBN0JN2L020141209

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research, 10*(2), 281-305.

Riley, C., & Pagliery, J. (2015). *Target will pay hack victims $10 million.* Retrieved from http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/

Robinson, O. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25-41. https://doi.org/10.1080.17480887.2013.801543

Rowley, J. (2012). Conducting research interviews. *Management Research Review, 35*(3/4), 260-271. https://doi.org/10.1108/0140917121210154

Rubin, H. J., & Rubin, I. S. (2012). Qualitative interviewing: The art of hearing data (3rd ed.). Thousand Oaks:

Sage Publications.

Savage, K., Coogan, K., & Lau, H. (2015). The evolution of ransomware. Retrieved November 28, 2017, from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.* Retrieved January 21, 2018, from http://lorrie.cranor.org/pubs/pap1162-sheng.pdf

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. https://doi.org/10.1108.09685220010371394

Sjouwerman, S. (2015). Confronting 'spear phishing' etc. *Privacy Journal, 41*(7), 3-4. Retrieved from http://www.privacyjournal.net

Soloman, M. R. (2013). *Consumer behavior*. Boston: Pearson.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security, 24*(2), 124-133. https://doi.org/10106/j.cose.2004.07.001

Stokes, N. (2014). *Should you use Facebook or Google to log in to other sites?* Retrieved from http://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/

Sun, J. C., & Lee, K. (2016). Which teaching strategy is better for enhancing anti-phishing learning motivation and achievement? The concept maps on tablet PCs or worksheets. *Educational Technology & and Society, 19*(4), 87-99. Retrieved from http://www.ifets.info/

Symantec. (2016). *Ransomeware and Business 2016.* Retrieved November 28, 2017, from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Symantec. (2017). *Trojan Gpcoder.* Retrieved November 28, 2017, from https://www.symantec.com/security_response/writeup.jsp?docid=2005-052215-5723-99

Symantec. (2018). *2017 Internets security threat report.* Retrieved January 21, 2018, from https://www.symantec.com/security-center/threat-report

Taylor, B. (2017). *Social media privacy guide.* Retrieved January 22, 2018, from https://www.bestvpn.com/social-media-privacy-guide/

Tetnowsky, J. (2015). Qualitative case study research design. *Perspective on Fluency & Fluency Disorders, 25*(1), 39-45. https://doi.org/10.1044/ffd25.1.39

Thomas, J. E. (2017a). Combating ransomware with traditional backup. https://doi.org/10.13140/RG.2.2.15403.13603

Thomas, J. E. (2017b). Exploring buyer motivation to improve management, marketing, sales, and finance practices in the martial arts industry. https://doi.org/10.5539/ijms.v9n2p12

Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science, 11*(1), 14-25. https://doi.org/10.5539/cis.v11n1p14

Torrance, H. (2012). Triangulation, respondent validation, and democratic participation in mixed methods research. *Journal of Mixed Methods Research, 54*(2), 111-123. https://doi.org/10.1016/j.jadohealth.2013.10.173

Turner, D. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report, 15*(3).

USPS Office of Inspector General. (2015). Information security awareness training and phishing. Retrieved January 21, 2018, from https://www.uspsoig.gov/sites/default/files/document-library-files/2015/IT-AR-16-001.pdf

Verizon. (2016). 2016 data breach investigations report. Retrieved January 21, 2018, from https://www.google.com/search?q=2016+Data+Breach+Investigations+Report&ie=utf-8&oe=utf-8&client=firefox-b-1-ab

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of

a phishing attack. *Journal of Computer Mediated Communication, 20*(5). https://doi.org/10.1111/jcc4.12126

Vishwanath, A., Harrison, B., & Ng, Y. (2016, February 10). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Harrison, B., Chen, R., Wang, J., & Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information process model. *Decision Support System, 51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Weiss, E., & Miller, R. (2015). *The Target and other financial data breaches: Frequently asked questions.* Retrieved January 21, 2018, from https://fas.org/sgp/crs/misc/R43496.pdf

Williams, E., & Ashenden, D. (2017). *Phishing scams are becoming ever more sophisticated - and firms are struggling to keep up.* Retrieved February 18, 2018, from https://theconversation.com/phishing-scams-are-becoming-ever-more-sophisticated-and-firms-are-struggling-to-keep-up-73934

Wright, R., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273-303. doi:10.2753/mis0742-1222270111

Wueest, C. (2016). *Financial threats 2015.* Retrieved January 21, 2018, fromhttps://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/financial-threats-15-en.pdf

Yallapragada, R., Roe, W., & Toma, A. (2012). Accounting fraud, and white-collar crimes in the United States. *Journal of Business Case Studies*, 187-191. https://doi.org/10.19030/jbcs.v8i2.6806

Yin, R. K. (2014). *Case-study research: Design and methods* (5th ed.). London: Sage.

Zaeem, R., Mnaoharan, M., Yang, Y., & Barber, K. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security, 65*, 50-63. http://dx.doi.org/10/1016/j.cose.2016.11.02

Zhu, F., Caprenter, S., & Kulkarni, A. (2012). Understanding identity exposure in pervasive computing environments. *Pervasive and Mobile Computing, 8*(5), 777-794. https://doi.org/10.1016/j.pmcj.2011.06.007

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).