IADIS International Journal on Computer Science and Information Systems
Vol. 13, No. 2, pp. 93-108
ISSN: 1646-3692

EVALUATING USER VULNERABILITIES VS PHISHER SKILLS IN SPEAR PHISHING

Mathew Nicho[1], Hussein Fakhry[1] and Uche Egbue[2]
[1]College of Technological Innovation, Zayed University, Dubai, UAE
[2]School of Computing and Digital Media, Robert Gordon University, United Kingdom

ABSTRACT

Spear phishing emails pose great danger to employees of organizations due to the inherent weakness of the employees in identifying the threat from spear phishing cues, as well as the spear phisher's skill in crafting contextually convincing emails. This raises the main question of which construct (user vulnerabilities or phisher skills) has a greater influence on the vulnerable user. Researchers have provided enough evidence of user vulnerabilities, namely the desire for monetary gain, curiosity of the computer user, carelessness on the part of the user, the trust placed in the purported sender by the user, and a lack of awareness on the part of the computer user. However, there is a lack of research on the magnitude of each of these factors in influencing an unsuspecting user to fall for a phishing or spear phishing attack which we explored in this paper. While user vulnerabilities pose major risk, the effect of the spear phisher's ability in skillfully crafting convincing emails (using fear appeals, urgency of action, and email contextualization) to trap even skillful IT security personnel is an area that needs to be explored. Therefore, we explored the relationships between the two major constructs namely 'user vulnerabilities' and 'email contextualization', through the theory of planned behavior with the objective to find out the major factors that lead to computer users biting the phishers' bait. In this theoretical version of the paper, we provided the resulting two constructs that needed to be tested.

KEYWORDS

Spear phishing, User Vulnerabilities, Email Contextualization

1. INTRODUCTION

Spear phishing attacks form not only an effective attack vector to infiltrate companies and organizations (Gascon, Ullrich, Stritter, & Rieck, 2018), but also pose real challenge in terms of detection and mitigation (Thomas, 2018). In this respect, multiple human factors as well as the ability of the spear phisher to contextualize emails have been identified as causal factors that contribute to human error in spear phishing attacks. Phishers exploit these cognitive limitations by employing visual deception to spoof legitimate email messages or websites (Carnegie Mellon University, 2014). Successful emails employ psychological weapons of influence and relevant life domains (Oliveira et al., 2017). As spear phishing attacks are executed by coordinated human actions rather than automated pieces of code (Jasek, Kolarik, & Vymola, 2013) targeting people (Julisch, 2013), the attacker's point of entry into network systems using email as an attack vector remains a vulnerable point of network to date. Security policies, no matter how stringently they are implemented, cannot prevent certain human behavioral patterns while accessing their emails, thus making them vulnerable to an attack. Therefore, despite the advances made in information security, human factors remain a critical element in the security of systems for at least three possible reasons: 1) they are a vulnerable link, 2) they are the only factor that exercises initiatives, and 3) they are the factor that transcends all the other elements of the entire system (Adeka, Shepherd, & Abd-Alhameed, 2013). Consequently, end users in the workplace have been termed as 'the weakest link' in information systems security (Paans, & Herschberg, 1987; Guo, Yuan, Archer, & Connelly, 2011).

With 92.4% of malware being delivered via email (Verizon Inc., 2018), 42% of IT Security professionals consider spear phishing to be amongst one of the top 3 cyberattack concerns (Das, 2018). Ironically, in a global study conducted on 19000 respondents in 2015, 97 percent of consumers could not correctly identify phishing scam emails (Paganini, 2018). In this respect, spear phishing is considered to be the preliminary stage of an Advanced Persistent Threat (APT) attack to create a point of entry into the organization (Vayansky, & Kumar, 2018). The years 2011 through 2015 have witnessed aggressive growth in phishing attacks globally (Anti Phishing Working Group, 2017). Subsequently, a growth rate of 250% between October 2015 and March 2016 has been reported with more than 20 million new malwares deployed by hackers to facilitate these attacks (Bradley, 2016). In the same vein, Kaspersky Labs reported to have received over 30.8 million phishing alerts on its anti-phishing mechanism in the 2nd quarter of 2015 (Dalasta, 2016). The notoriety of phishing attacks is now alarming as the above statistics have confirmed a disturbing trend that online users are becoming more vulnerable to the attack. High-profile cases of attacks using spear phishing have increasingly come to the public awareness in the last decade. These include Operation Aurora, and those against the International Monetary Fund, Oak Ridge National Laboratory in the US and the French foreign ministry (Tankard, 2011).

Social engineering tools that include spear phishing have been used to successfully penetrate information systems of Google, RSA, and New York Times (Krombholz, Hobel, Huber, & Weippl, 2015). While users occasionally find it difficult to differentiate between a genuine URL and a fake one in a spear phishing attack (Dhamija, Tygar, & Hearst, 2006; Stembert, Padmos, Bargh, Choenni, & Jansen, 2015), phishers leverage this ability to deceive even security aware IT personnel. Successful spear phishing emails apply psychological principles of influence that exploit common human heuristics that are often beneficial in simplifying decision-making, but can also result in misrepresentation, and can lead to deception (Oliveira et al., 2017). Furthermore, the spear phisher creates contextually convincing emails (Nicho, Fakhry, & Egbue, 2018) using 'creative persuasion' strategies such as urgency and authoritativeness (Rajivan, & Gonzalez, 2018). This narrows down to two constructs namely 'user vulnerabilities' and 'email contextualization'. In this respect we aim to find out the answer to the research question: "Which of the two factors has a greater influence on computer users to fall victim to spear phishing email attacks? As each of these two constructs incorporate multiple variables, we also aim to understand the relative influence of each of the variables in the constructs; and the correlation of the variables with each other. An empirical answer to the research question can assist organizations in developing and implementing appropriate IT control mechanisms to prevent and mitigate the incidence of spear phishing attacks for their employees.

The research question therefore clearly focuses on the end users in the workplace, who have been termed as “the weakest link” in IS security (Paans, & Herschberg, 1987; Guo et al., 2011), since every information security breach incident involves some element of human error (Verizon Inc., 2014). Therefore, human factors are critical elements in the security system for at least three possible reasons; they are the weakest link, they are the factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system (Adeka, Shepherd, & Abd-Alhameed, 2013). Hence, a behavioral approach to identify the independent variables can provide deep insights into the problem.

The remainder of the paper is structured as follows. Section two provides an understanding of spear phishing along with its multiple attack methodologies. Section three focuses on the problem from a behavioral perspective to identify the theoretical lens. Section four delves into the reasons why computer users fall for spear phishing attacks. Section five outlines the research model and the methodology, followed by conclusion and future directions from this project.

2. SPEAR PHISHING

Phishing emails are sent with malicious intent that attempt to exploit recipients’ weaknesses and trick them into sharing sensitive personal or organizational information (Hong, 2012; Butavicius, Parsons, Pattinson, & McCormac, 2016). However, spear phishing makes use of emails that contain contextual information, carefully harvested through profiling and reconnaissance, to trick carefully chosen targets into revealing sensitive information (Han, & Shen, 2016). The use of contextual information improves the hackers’ chances of gaining the recipients’ confidence with malicious correspondence to lure them into parting with sensitive information (Stembert et al., 2015). The use of deception by hackers deploying spear phishing (Jagatic, Johnson, Jakobsson, & Menczer, 2007) is preceded by intensive data mining to gather information from social networking sites to win the confidence of the victims to lure them into clicking on the links (Nelson, Lin, Chen, Iglesias, & Li, 2016). Spear phishing is characterized by intensive preparation to adapt or engineer the corresponding email to capture the victim’s interest (Stembert et al., 2015). Consequently, spear phishing targets a specific individual or an organization using personalization and customization to distract the target’s attention from certain safety measures, to achieve a high success rate (Alam, & El-Khatib, 2016). In this type of attack, the adversary accesses inside information or specific relevant information about their intended target and uses this information to impersonate trusted relationships through the means of well-formatted fake email messages (Caputo, Pfleeger, Freeman, & Johnson, 2014). However simple it may seem, it is a complex targeted attack where the hacker gathers specific information about the intended target and uses it to initiate sophisticated and genuine correspondence before the attack is carried out to compromise the target’s confidential information (Dewan, Kashyap, & Kumaraguru, 2014).

In spear phishing attacks, hackers use various means to establish a single point of entry into an individual's computer or an organization's network system to carry out their malicious acts by means of infiltrating targeted network systems (Lin, Tien, Chen, Tien, & Pao, 2015). In this respect, email continues to be the preferred mechanism of attack deployed in spear phishing among the three major types of spear phishing attack vectors, namely email, URL spoofing and water holing (Fette, Sadeh, & Tomasic, 2007; Stembert et al., 2015). Due to the persistent nature of spear phishing, it continues to be successful such that hackers can effectively carry out attacks initiating users to unwillingly breach information security policies (Abraham, & Chengalur-Smith, 2010). While the paper focuses on spear phishing, we use these two terms (phishing and spear phishing) interchangeably in this paper.

3. MODELLING VULNERABILITIES IN USER BEHAVIOUR

Modelling user vulnerabilities has gained significance since, out of the 156 million phishing emails (a key aspect of the spear phishing) sent every day to global internet users, 16 million of them make it through email filters, 8 million emails are opened, 800,000 links are clicked, and 80,000 fall for the scam and get their computer infected, which results in loss of personal identity and information (Johnson, 2016). Since most human behavior is goal oriented (Ajzen, 1985), the objective of the computer user when confronted with the decision about opening a suspicious or genuine email can vary ranging from financial gain to acquiring new information ['curiosity' has been defined as a desire to evoke the senses to acquire new information (Litman, 2005)], which in turn can lead to policy violation (from an organizational perspective). Therefore, actions are controlled by intentions whereby human social behavior can best be described as following well formulated plans (Ajzen, 1985). Spear phishing thrives because hackers take advantage of human psychology to exploit their weaknesses and deceive them into achieving their fraudulent desires (Parmar, 2012), as these emails are embedded with electronic deception and disguised to appear to come from individuals or organizations with which the victim is familiar (Han, & Shen, 2016).

The theory of planned behavior (TPB) (Ajzen, & Fishbein, 1980) has been used to explain security policy violations by computer users (Bulgurcu, Cavusoglu, & Benbasat, 2010; Sommestad, Karlzén, & Hallberg, 2017). The TPB, which is an extension of the theory of reasoned action, explains an individual's intention to perform a given behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010). According to the TPB (Ajzen, 1991), human behavior is guided by three kinds of considerations, namely 'attitude' towards the behavior, 'subjective norms', and 'perceived behavioral control'. The theory, however, merely points to a host of possible background factors that may influence the beliefs people hold such as personality and broader life values (Ajzen, 2011). Likewise, perceived behavioral control refers to people's perception of the ease or difficulty of performing the behavior of interest, while subjective norms are concerned with the likelihood that important referent individuals or groups approve or disapprove of performing a given behavior. While the three factors (*attitudes, subjective norms,* and *perceived behavioral control*) account for user vulnerabilities, we added another construct, namely email contextualization, since this is a major factor that even trained security personnel can overlook.

In this respect, we aim to understand inherent spear phishing user vulnerability variables by understanding the relationships between these and the awareness of spear phishing (ASP) contextual cues through the TPB. The TPB is an extension of the theory of reasoned action (Fishbein, & Ajzen 1975; Ajzen, & Fishbein, 1980) that explains an individual's intention to perform a given behavior. The TPB suggests that the intention to perform various kinds of behaviors can be predicted with high accuracy from attitudes toward the behavior, subjective norms, and perceived behavioral control, and that these intentions, together with perceived behavioral control, account for a considerable amount of variance in the actual behavior (Ajzen, 1991). Organizations deploy technological means to protect their information and technology resources, but they also rely on their employees. Employees who use the information and technology resources of their organizations assume certain roles in the organization and are responsible for safeguarding (protecting) those resources, so we are interested in knowing the predominant factors that drive an employee to perform those roles and meet their responsibilities. Subsequently, this assists organizations in understanding the antecedents or factors that influence a computer user's decision to click on an email (genuine or spam) through the TPB. The TPB considers behavioral intention as an indication of an individual's readiness to perform an action. In this respect, a computer user's act of opening and clicking a link or downloading an attachment that is not genuine is used as the dependent variable in the study. We begin this by adopting the three main constructs of the TPB which are attitude, subjective norms, and perceived behavioral control. However, we added two more constructs (urgency and fear, and email contextualization) from the phisher's context where emails can be customized and contextualized based on the intended target's mental disposition.

4. INFLUENCING FACTORS IN SPEAR PHISHING ATTACKS

Spear phishing victims fall for the phisher's bait due to intrinsic factors that are inherent in the victim based on experience and learning, as well as external factors (such as the ability of the spear phisher to expertly craft a spear phishing email). Therefore, when confronted with a spear phishing scenario, humans are often influenced by their mind-sets as well as their decision-making capabilities (Stembert et al., 2015), since spear phishing attacks are structured in such a way as to make their victims believe in the authenticity of the email based on the nature of the information it contains (Han, & Shen, 2016).

4.1 User Vulnerabilities in Spear Phishing

The success rate of spear phishing attacks is quite high because the information included in the email content exploits humans' emotional responses to fear, greed, sense of urgency, curiosity, trusted personal relationships and standard business correspondence (Kim, Shin, Kim, & Lee, 2011a). In this respect, urgency is a contributing factor in spear phishing users' vulnerability when they receive emails that require an urgent response as this may put the victims under unnecessary pressure preventing them from making rational decisions prior to responding to the email (Aggarwal, Kumar, & Sudarsan, 2014).

Attitudes (curiosity and carelessness): Social engineering methods that are used in phishing target human behavior attributes namely curiosity, fear of the unknown or losing something (as when responding to popup windows), ignorance and carelessness (Bere, Bhunu-Shava, Gamundani, & Nhamu, 2015). Furthermore, the high rate of mobile devices in use today also makes users respond to their emails without analyzing them properly while accessing these devices on the go (Parmar, 2012). While spear phishers make mistakes in crafting a cloned site or a phishing site, computer users are more likely to ignore such mistakes (Aburrous, Hossain, Dahal, & Thabtah, 2010). When users out of curiosity respond to ‘false negative emails’, which are emails from unknown senders that contain innocuous looking sentences such as those asking about the health of the recipient or just a simple “how are you?”, the actual attack is carried out without the victim being aware (Aggarwal, Kumar, & Sudarsan, 2014). Therefore, while human carelessness is a critical vulnerability factor in phishing attacks, little empirical research has studied behaviors associated with information carelessness and the ways that people exploit this vulnerability (Workman, 2008). Based on this evidence, we postulate the following hypothesis.

H1: Attitudes comprising of curiosity and carelessness are a contributing factor in influencing users to fall for spear phishing attacks.

Subjective norms (trust, and financial benefit): Spear phishing emails could assume the form of ‘greed’ or a ‘promise of financial benefits’ to lure their victims to provide sensitive information like the potential to access a very large amount of money, stacked away in an account and requiring the victim’s cooperation to transfer the money to a safe haven (Aggarwal, Kumar, & Sudarsan, 2014). Since, ‘trust’ is a typical personality trait of people who are deceived by targeted e-mails (Torii, Morinaga, Yoshioka, Terada, & Unno, 2014), phishers exploit these trusts to compromise targets (Huang, Tan, & Liu, 2009). Human behavior attributes such as trust, the desire to be helpful, wishing to get something for nothing, are aimed at manipulating humans or software into divulging confidential information about the targeted network (Bere et al., 2015). Phishers constantly use psychology behind their emails that displays greed or trust (Vayansky, & Kumar, 2018). Based on this, the resulting hypothesis is postulated.

H2: Subjective norms comprising of trust in the sender complemented with financial gain positively influences users to fall for spear phishing attacks.

Perceived behavioral control (Lack of awareness) User’s carelessness together with a lack of knowledge in differentiating between spoofed and genuine websites leads users to fall victims to such attacks (Zhang, Ren, & Jiang, 2016). In this respect, lack of awareness of phishing is a major factor for most compromises (Banerjee, & Pandey, 2010; Gupta, Arachchilage, & Psannis, 2018). Subsequently, the user’s inability to differentiate between a genuine email and a phishing email from the words contained in the subject and body of an email, respectively, will generally contribute to the reasons why humans fall for spear phishing attacks (Hong, 2012). The above justifications give rise to the hypothesis.

H3: Perceived behavioral control is a contributing factor in user vulnerabilities related to spear phishing.

4.2 Hacker’s Skills in Email Contextualization

The hacker’s ability to contextualize the email is a relevant factor that needs to be taken into consideration. Spear phishing emails are structured in such a way to make their victims believe in the authenticity of the email based on the nature of information it contains (Han, & Shen, 2016). Such emails pose a serious threat because the expected reaction of the victim in the face of such threat is not usually covered and/or controlled by an organization’s information security policy, thereby leaving potential breach in the organization’s security at the mercy of the user’s discretion (Garera, Provos, Chew, & Rubin, 2007). However, implementing multilevel technical security layers to protect the network (Krombholz et al., 2015) is inadequate to prevent the organization’s members of staff from relating with the outside public and therefore unknowingly from being in contact with potential hackers (Caldwell, 2013).

Urgency and fear appeal: A spear phishing email could be easily identified by some of the following contents of an email: a sense of urgency to take action, spelling errors or bad grammar, invoking a sense of fear/greed or emotional response, link text/source address mismatch, lack of consistency in the name/address of the source, and/or email out of context when matched with one’s expectation (Caldwell, 2013). However, the question of why the email passes through under the very eyes of unsuspecting computer users can partly be ascertained by observing the methods deployed by spear phishers in crafting the email. Because handling phishing emails is not a primary task for a user, users are often forced to make rapid decisions about the email based on straightforward cues found in the email like ‘urgency’ which may interfere with the user’s ability to detect deception (Burns, Durcikova, & Jenkins, 2012). In this respect, the following hypothesis is postulated.

H4: Urgency and fear appeal embedded in the email by phishers is a contributing factor leading to users falling victim to phishing attacks

Email contextualization: Hackers indulge in URL spoofing mainly to obfuscate their identity, and to exploit the confidence people have in trusted websites thus hiding the sender’s real source address (Patel & Luo, 2007). In this respect, hackers spoof the URL or IP address of an existing website and come up with a malicious URL that looks like a genuine URL to the targeted victim (Kim, Jeong, Kim, & So, 2011b). This, however, eludes the eyes of unsuspecting victims regardless of their training in security awareness (Soni, Firake, & Meshram, 2011). Consequently, users occasionally find it difficult to differentiate between a genuine URL and a fake one when they are under a spear phishing attack because they tend to only take a quick glance at the URL with a presumption that it is legitimate (Dhamija, Tygar, & Hearst, 2006; Stembert et al., 2015). By this time, the targeted victim(s) has already clicked on the malicious URL where it will then point them to the hacker's site instead of the legitimate one they had desired to visit (Fette, Sadeh, & Tomasic, 2007). In this respect, spear phishing attacks not only lure naïve victims into giving out sensitive information to hackers, but also exploit or trick technically knowledgeable users (Khonji, Iraqi, & Jones, 2011). While user vulnerabilities can greatly affect the success of a spear phishing email, the contextual factors built into the spear phishing email also add to the success of a spear phishing email. Based on these arguments, the following hypothesis is presented.

H5: Email contextualization by phishers is a contributing factor leading to users falling victim to phishing attacks

Table 1. Variables affecting users' likelihood to fall victim to spear phishing email attacks

Constructs	Vulnerabilities	References
´	Financial benefit/ desire for monetary gain	(Aggarwal, Kumar, & Sudarsan, 2014; Bere et al., 2015; Sahu & Dubey, 2014; Vayansky & Kumar, 2018; Zhou, Zhang, Xiao, Wang, & Lin, W. 2014; Oliveira et al., 2017)
	Curiosity	(Aggarwal, Kumar, & Sudarsan, 2014; Bere et al., 2015; Cho, Cam, & Oltramari, 2016; Fette, Sadeh, Tomasic, 2007; Wash & Cooper, 2018; O'Kane, Sezer, & Carlin, 2018)
	Carelessness	(Aburrous et al, 2010; Bere et al., 2015; Chiew, Chang, & Tiong, 2015; Kearney & Kruger, 2013; Laszka, Lou, & Vorobeychik, 2016; Miyamoto, Hazeyama, & Kadobayashi, 2005; Nagalingam, Narayana Samy, Ahmad, Maarop, & Ibrahim, R. 2015; Parmar, 2012; Workman, 2008; Wright & Marett, 2010; Zhang, Ren, & Jiang, 2016; Zhou et al., 2014)
	Trust in the sender	(Alseadoon, Othman, Foo, & Chan, 2013; Bere et al., 2015; Cho, Cam, & Oltramari, 2016; Harrison, Vishwanath, & Rao, 2016; Huang, Tan, & Liu, 2009; Ivaturi, & Janczewski, 2012; Komatsu, Takagi, & Takemura, 2013; Patel & Luo, 2007; Romanov, Semenov, Mazhelis, & Veijalainen, J. 2017; Vayansky & Kumar, 2018)
	Lack of awareness; ignorance	(Bann, Singh, & Samsudin, 2015; Caputo et al., 2014; Chiew, Chang, & Tiong, 2015; Gupta, Arachchilage, & Psannis, 2018; Ismail, Singh, Mustaffa, Keikhosrokiani, & Zulkefli, 2017; Janet, Mitchell, Robert, & Bradley, 2008; Rot & Olszewski, 2017; Soni, Firake, & Meshram, 2011; Zhang, Ren, & Jiang, 2016)
Email Contextualization	Urgency	(Burns, Durcikova, & Jenkins, 2012; Caldwell, 2013; Ivaturi, & Janczewski, 2012; Kearney, & Kruger, 2013; Nagalingam et al., 2015; Smutz, & Stavrou, 2012; Vayansky, & Kumar, 2018; Wang, Herath, Chen, Vishwanath, & Rao, 2012)
	Fear appeal	(Bere et al., 2015; Gupta, Arachchilage, & Psannis, 2018; Kim et al., 2011b; Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015)
	Email characteristics	(Dhamija, Tygar, & Hearst, 2006; Han, & Shen, 2016; Khonji, Iraqi, & Jones, 2011; Kim et al., 2011b; Patel, & Luo, 2007; Soni, Firake, & Meshram, 2011)

Spear phishing user vulnerabilities gleaned from the literature are summarized in table 1 which attempts to theoretically answer the research question raised in section 1. Hence, users' inherent attitudes while dealing with emails as well as awareness of spear phishing email cues impacts upon users' decision in making a true positive or true negative decision regarding genuine and malicious emails. However, the direct and indirect roles of attitudes and awareness of spear phishing cues on a users' email behavior have not yet been studied.

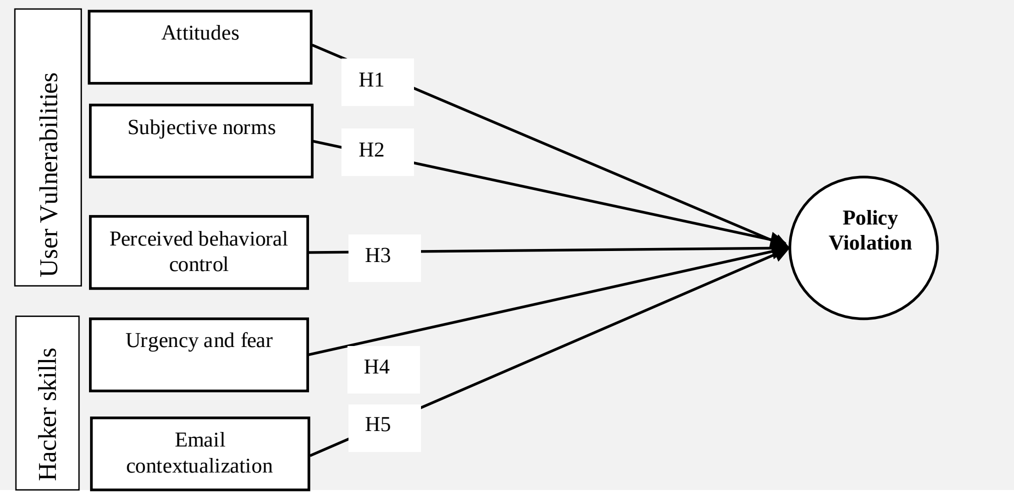

Figure 1. Spear phishing behavioral model (SPB) illustrating the constructs that influence computer users' likelihood to fall victim to spear phishing email attacks

We, therefore, integrate the variables in the constructs into the modified TBP as illustrated in figure 1 through our spear phishing behavioral model (SPB) where attitudes, subjective norm, perceived behavioral control, urgency and fear, and email contextualization form the independent variables that affect the dependent variable policy violation. While the subsequent section outlines the research design, the empirical research is planned in the subsequent phase of this project.

5. RESEARCH DESIGN

Since the aim of the model is to find out the effect of these independent variables on the dependent variable, structural equation modeling (SEM) can be used as it uses distinct types of models to depict relationships among observed variables, with the same basic goal of providing a quantitative test of a theoretical model hypothesized by the researcher (Schumacker, & Lomax, 2016). SEM, which is a combination of factor analysis and regression or path analysis, is a general statistical modeling technique widely used in the behavioral science (Hox and Bechger, 1998).

Multiple regression analysis has been used to test a hypothesis whereby Moon and Kim (2001) extended the TAM to find out the effect of perceived playfulness, perceived ease of use, perceived usefulness, attitudes, and intention to use (independent variables), on the actual usage of the internet (dependent variable). In this respect, we plan to run separate regressions on each of the dependent variables. This is how a multiple regression model looks like when represented as a path model. Regression analysis can be viewed as a simple form of SEM where the researcher proposes a theoretical model (with independent and dependent variables) to evaluates its fit to the data. In this respect, goodness of fit of the model is evaluated in terms of R^2 tests and individual regression parameters, which also considers the variance and covariance. Figure 2 transforms the model (figure 1) into a multiple regression model. Here, the six variables result in 6 x 6 variance/covariance matrix, 15 unique covariance, and 21 (15 + 6) data points. Hence, the estimation of the following parameters is called for:

1. The variances and covariances of the five independent variables (15)
2. The regression coefficient (05)
3. The error variance (01)

Total = 21

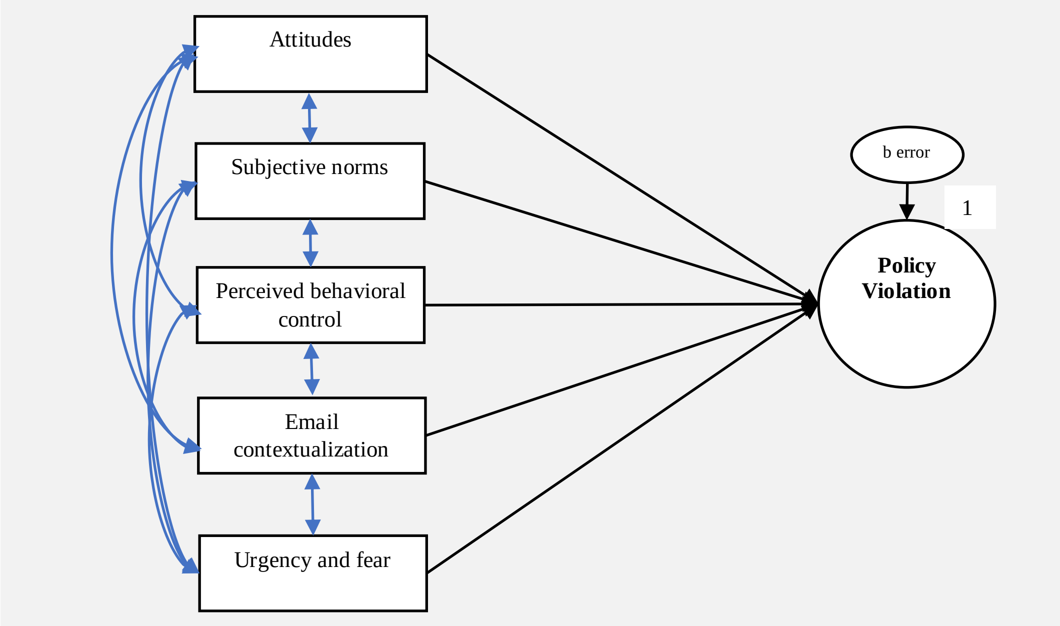

Figure 2. SBP model using multiple regression

The preparation of the attack simulation process involves crafting a spear phishing email with a link, designing a specially hosted website (using a free sub-domain web hosting platform) for the link, a reward-based questionnaire to entice the victim for a reward, and a subsequent link where the respondents are directed to an online questionnaire (figure 3). The content of the email is designed to emulate a self-explanatory email like the ones hackers normally use to lure their potential victims into falling for spear phishing attacks. The link leads to the website which simulates an online product testing survey site. The respondents then participate willingly in the purported product testing survey and by extension, complete the research questionnaire to enable the researcher to obtain unbiased data for analysis on the topic of the study.

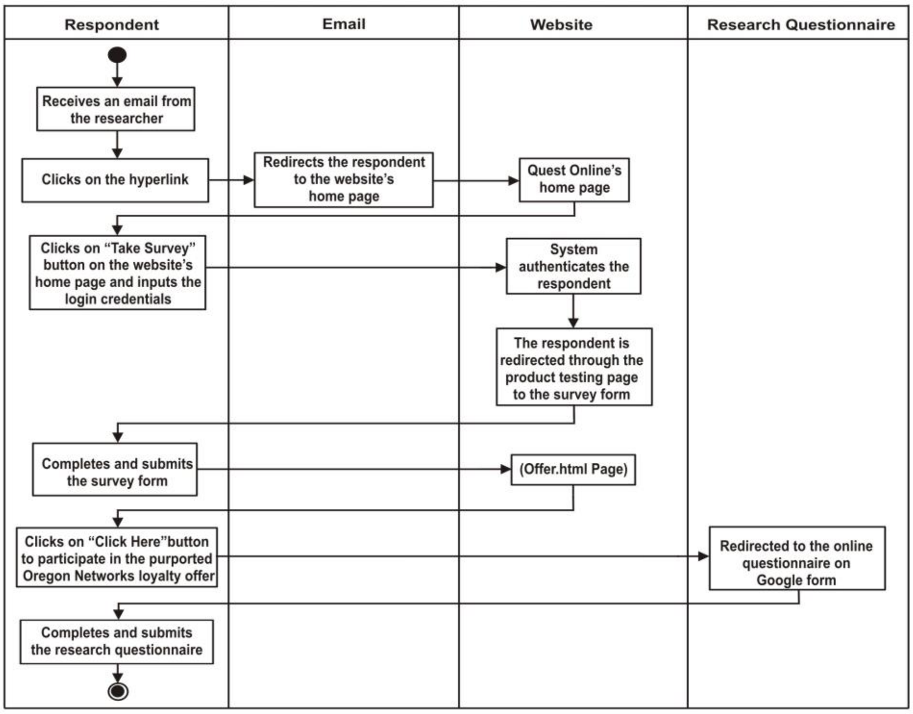
Respondent
Email
Website
Research Questionnaire
Receives an email from the researcher
Clicks on the hyperlink
Redirects the respondent to the website's home page
Quest Online's home page
Clicks on "Take Survey" button on the website's home page and inputs the login credentials
System authenticates the respondent
The respondent is redirected through the product testing page to the survey form
Completes and submits the survey form
(Offer.html Page)
Clicks on "Click Here"button to participate in the purported Oregon Networks loyalty offer
Redirected to the online questionnaire on Google form
Completes and submits the research questionnaire

Figure 3. Diagram of the process flow chart

6. CONCLUSION

Existing research has shown the predominance of two major factors that can influence a computer user's likelihood of falling for spear phishing attacks, namely user vulnerabilities (inherent in the user) and the skills of the spear phisher in crafting a 'genuine looking' spear phishing email. While researchers have provided evidence about these two influencing factors, the question of which one of these constructs is more effective in influencing the victim remains unanswered. Furthermore, which of the variables inherent in these factors contribute most to spear phishing attacks remains unanswered. Since, the TBD model has been used by researchers to predict factors that influence an employee's intention to comply with organizational policies, we used this theory as a theoretical lens to observe the factors that have a greater influence on an unsuspecting user's propensity to fall victim to a phishing or spear phishing attack. In the subsequent phase of the project, we shall attempt to test the two constructs (along with the five factors) through five hypotheses using the SEM technique, as used widely in behavioral science. The study is not without its limitations. First, due to ethical considerations, we simulated spear phishing emails, which is in fact different from reality. Second the interaction between the components (attitudes, subjective norm, and perceived behavioral control) in the original TPB model is outside the scope of this study since we assume that the correlation will be within permissible limits to do regression analysis. Two avenues for future research stem from this study. First, it would be interesting to explore and evaluate the relative effect of technical controls versus non-technical phishing related organizational control/policy on organizational users. Organizations widely use email filters, policies, awareness program to protect organizational users. However, a comprehensive list of these countermeasures needs to be explored along with their relative weights. Second, a study on building a comprehensive taxonomy of phishing attack vectors is required, which will greatly elucidate the nature of threat, the technical and non-technical nature of each threat. Both these studies can identify appropriate combination of technical and non-technical countermeasures that can be applied to the corresponding spear phishing threat vector.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). An Overview of Social Engineering Malware: Trends, Tactics, and Implications. *Technology in Society, 32*(3), 183-196.

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent Phishing Detection System for E-Banking Using Fuzzy Data Mining. *Expert Systems with Applications, 37*(12), 7913-7921.

Adeka, M., Shepherd, S., & Abd-Alhameed, R. (2013). Resolving the Password Security Purgatory in The Contexts of Technology, Security and Human Factors. In *Proceedings of the International Conference of Computer Applications Technology (ICCAT), 2013.*

Aggarwal, S., Kumar, V., & Sudarsan, S. (2014). *Identification and detection of phishing emails using natural language processing techniques.* In *Proceedings of the 7th International Conference on Security of Information and Networks.*

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior *Action Control* (pp. 11-39): Springer, Berlin.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Ajzen, I. (2011). The Theory of Planned Behavior: Reactions and Reflections. *Psychology & Health, 26*(9), 1113-1127.

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice Hall.

Alam, S., & El-Khatib, K. (2016). *Phishing Susceptibility Detection through Social Media Analytics.* In *Proceedings of the 9th International Conference on Security of Information and Networks*.

Alseadoon, I. M., Othman, M. F. I., Foo, E., & Chan, T. (2013). *Typology of Phishing Email Victims Based on their Behavioral Response.* In *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, Illinois.

Anti-Phishing Working Group. (2017). Global Phishing Survey 2016. Retrieved from https://www.antiphishing.org/apwg-news-center/

Banerjee, C., & Pandey, S. (2010). Research on Software Security Awareness: Problems and Prospects. *ACM SIGSOFT Software Engineering Notes, 35*(5), 1-5.

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science, 72*, 129-136.

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). How Advanced Persistent Threats Exploit Humans. *International Journal of Computer Science Issues (IJCSI), 12*(6), 170.

Bradley, S. (2016). How to Use Analytics to Enhance Security. *Risk Management, 63*(7), 14.

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.

Burns, M. B., Durcikova, A., & Jenkins, J. L. (2012). On Not Falling for Phish: Examining Multiple Stages of Protective Behavior of Information System End-Users. In *Proceedings of the Thirty Third International Conference on Information Systems*, Orlando.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). *Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails.* In *Proceedings of the Australasian Conference on Information Systems,* Adelaide.

Caldwell, T. (2013). Spear-Phishing: How to Spot and Mitigate the Menace. *Computer Fraud & Security, 2013*(1), 11-16.

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.

Carnegie Mellon University. (2014). Unintentional Insider Threats: Social Engineering. Retrieved from https://www.researchgate.net/profile/Jeremy_Strozer/publication/265906952_Analysis_of_Unintentional_Insider_Threats_Deriving_from_Social_Engineering_Exploits/links/551297cb0cf268a4aaea9285/Analysis-of-Unintentional-Insider-Threats-Deriving-from-Social-Engineering-Exploits.pdf

Chiew, K. L., Chang, E. H., & Tiong, W. K. (2015). Utilization of Website Logo for Phishing Detection. *Computers & Security, 54,* 16-26.

Cho, J.-H., Cam, H., & Oltramari, A. (2016). Effect of Personality Traits on Trust and Risk to Phishing Vulnerability: Modeling and Analysis. In *Proceedings of the 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),* San Diego, USA.

Dalasta, D. (2016). Phishing Data: Attack Statistics. Retrieved from http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-data-attack-statistics

Das, R. (2018). The Trends in Spear Phishing Attacks. Retrieved from https://resources.infosecinstitute.com/the-trends-in-spear-phishing-attacks/#gref

Dewan, P., Kashyap, A., & Kumaraguru, P. (2014). Analyzing Social and Stylometric Features to Identify Spear Phishing Emails. In *Proceedings of 2014 APWG Symposium on Electronic Crime Research (eCrime),* Birmingham. UK.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, Montreal, Canada.

Fette, I., Sadeh, N., & Tomasic, A. (2007). *Learning to detect phishing emails.* Proceedings of the 16th international conference on World Wide Web.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading: MA: Addison-Wesley.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A Framework for Detection and Measurement of Phishing Attacks. In *Proceedings of the 2007 ACM workshop on Recurring Malcode*, Alexandria, VA, USA.

Gascon, H., Ullrich, S., Stritter, B., & Rieck, K. (2018). Reading Between the Lines: Content-Agnostic Detection of Spear-Phishing Emails. In *Proceedings of* the *International Symposium on Research in Attacks, Intrusions, and Defenses* (pp. 69-91). Heraklion, Crete, Greece, Springer.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Non-Malicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending Against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. *Telecommunication Systems, 67*(2), 247-267.

Han, Y., & Shen, Y. (2016). Accurate Spear Phishing Campaign Attribution and Early Detection. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, Pisa, Italy.

Harrison, B., Vishwanath, A., & Rao, R. (2016). *A User-Centered Approach to Phishing Susceptibility: The Role of a Suspicious Personality in Protecting Against Phishing.* In *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS),* Hawaii.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM, 55*(1), 74-81.

Hox, J. J., & Bechger, T. M. (1998). An Introduction to Structural Equation Modeling. *Family Science Review, 11*, 354-373.

Huang, H., Tan, J., & Liu, L. (2009). Countermeasure Techniques for Deceptive Phishing Attack. In *Proceedings of the International Conference on New Trends in Information and Service Science (NISS'09)*, Beijing, China.

Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science, 124*, 656-663.

Ivaturi, K., & Janczewski, L. J. (2012). Effects of Information Seeking Modes on Users' Online Social Engineering Vulnerabilities. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Ho Chi Minh City, Vietnam.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Janet, L., Mitchell, D. B. A., Robert, B., & Bradley, K. (2008). Analysis of Student Vulnerabilities to Phishing. In *Proceedings of the Americas Conference on Information Systems* (*AMCIS 2008),* Toronto, Canada.

Jasek, R., Kolarik, M., & Vymola, T. (2013). *APT Detection System Using Honeypots.* In *Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13)*, Valencia, Spain.

Johnson, L. (2016). 3 Ways to Protect Against Phishing Attacks in 2016. Retrieved from http://blog.pcisecuritystandards.org/3-ways-to-protect-against-phishing-attacks-in-2016

Julisch, K. (2013). Understanding and Overcoming Cyber Security Anti-Patterns. *Computer Networks, 57*(10), 2206-2211.

Kearney, W. D., & Kruger, H. A. (2013). Phishing and Organizational Learning. In Proceedings of the IFIP International Information Security Conference, Auckland, New Zealand.

Khonji, M., Iraqi, Y., & Jones, A. (2011). Mitigation of Spear Phishing Attacks: A Content-Based Authorship Identification Framework. In *Proceedings of the 2011 International Internet Technology and Secured Transactions (ICITST)*, Abu Dhabi, UAE.

Kim, G., Shin, B., Kim, K. K., & Lee, H. G. (2011a). IT Capabilities, Process-Oriented Dynamic Capabilities, and Firm Financial Performance. *Journal of the Association for Information Systems, 12*(7), 487-517.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011b). The Dark Side of The Internet: Attacks, Costs and Responses. *Information systems, 36*(3), 675-705.

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human Aspects of Information Security: An Empirical Study of Intentional Versus Actual Behavior. *Information Management & Computer Security, 21*(1), 5-15.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and applications, 22,* 113-122.

Laszka, A., Lou, J., & Vorobeychik, Y. (2016). Multi-Defender Strategic Filtering Against Spear-Phishing Attacks. In Proceedings of the thirtieth AAAI Conference on Artificial Intelligence (AAAI-16), Phoenix. Arizona.

Lin, C. H., Tien, C. W., Chen, C. W., Tien, C. W., & Pao, H. K. (2015). Efficient Spear-Phishing Threat Detection Using Hypervisor Monitor. In *Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST).*

Litman, J. (2005). Curiosity and The Pleasures of Learning: Wanting and Liking New Information. *Cognition & Emotion, 19*(6), 793-814.

Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2005). SPS: A Simple Filtering Algorithm to Thwart Phishing Attacks. In *Proceedings of the Asian Internet Engineering Conference*, Bangkok, Thailand.

Moon, J.-W., & Kim, Y.-G. (2001). Extending the TAM for a World-Wide-Web context. *Information & Management, 38*(4), 217-230.

Nagalingam, V., Narayana Samy, G., Ahmad, R., Maarop, N., & Ibrahim, R. (2015). Identifying the Level of User Awareness and Factors on Phishing Attempt Among Students. *Advanced Science Letters, 21*(10), 3243-3247.

Nelson, J., Lin, X., Chen, C., Iglesias, J., & Li, J. J. (2016). Social Engineering for Security Attacks. In *Proceeding of the 3rd Multidisciplinary International Social Networks Conference on Social Informatics 2016*, Data Science 2016, NJ, USA.

Nicho, M., Fakhry, H., & Egbue, U. (2018). *When Spear Phishers Craft Contextually Convincing Emails*. In *Proceedings of the International Conferences WWW/Internet 2018 and Applied Computing 2018*, Budapest, Hungary.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of Ransomware. *IET Networks*, 7(5), 321-327.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... & Ebner, N. (2017). Dissecting Spear Phishing Emails for Older Vs Young Adults: On The Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility To Phishing. *In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver, USA.

Paans, I. R., & Herschberg, I. S. (1987). Computer Security: The Long Road Ahead. *Computers & Security, 6*(5), 403-416.

Paganini, P. (2018). New Intel Security study shows that 97% of people can’t identify phishing emails. Retrieved from https://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html

Parmar, B. (2012). Protecting Against Spear-Phishing. *Computer Fraud & Security, 2012*(1), 8-11.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The Design of Phishing Studies: Challenges for Researchers. *Computers & Security, 52,* 194-206.

Patel, D., & Luo, X. (2007). Take a Close Look at Phishing. In *Proceedings of the 4th Annual Conference on Information Security Curriculum Development,* Kennesaw, GA, USA.

Rajivan, P., & Gonzalez, C. (2018). Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology, 9*, 135.

Romanov, A., Semenov, A., Mazhelis, O., & Veijalainen, J. (2017). Detection of Fake Profiles in Social Media. In *Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017),* Porto, Portugal.

Rot, A., & Olszewski, B. (2017). Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. In *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems*, Prague, Czech Republic.

Sahu, K. R., & Dubey, J. (2014). A Survey on Phishing Attacks. *International Journal of Computer Applications, 88*(10).

Schumacker, R. E., & Lomax, R. G. (2016). *A Beginner's Guide to Structural Equation Modeling* (4th ed.). New York: Routledge.

Smutz, C., & Stavrou, A. (2012). Malicious PDF Detection Using Metadata and Structural Features. In *Proceedings of the 28th Annual Computer Security Applications Conference,* Orlando, Florida

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 1-10.

Soni, P., Firake, S., & Meshram, B. (2011). *A phishing analysis of web-based systems.* In *Proceedings of 2011 International Conference on Communication, Computing & Security*, Odisha, India.

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015). A study of preventing email (spear) phishing by enabling human intelligence. In *Proceedings at the European Intelligence and Security Informatics Conference (EISIC), 2015.*

Tankard, C. (2011). Persistent Threats and How to Monitor and Deter Them. *Network Security* (August), 16-19.

Thomas, J. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management, Vol. 13 (6).*

Torii, S., Morinaga, M., Yoshioka, T., Terada, T., & Unno, Y. (2014). Multi-Layered Defense Against Advanced Persistent Threats (APT). *FUJITSU Sci. Tech. J, 50*(1), 52-59.

Vayansky, I., & Kumar, S. (2018). Phishing Challenges and Solutions. *Computer Fraud & Security, 2018*(1), 15-20.

Verizon Inc. (2014). 2014 Data Breach Investigations Report. Retrieved from www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Verizon Inc. (2018). Verizon Data Breach Investigation Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication, 55*(4), 345-362.

Wash, R., & Cooper, M. M. (2018). Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (p. 492). ACM.

Workman, M. (2008). Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems, 27*(1), 273-303.

Zhang, W., Ren, H., & Jiang, Q. (2016). Application of Feature Engineering for Phishing Detection. *IEICE TRANSACTIONS on Information and Systems*, 99(4), 1062-1070.

Zhou, Y., Zhang, Y., Xiao, J., Wang, Y., & Lin, W. (2014). Visual Similarity Based Anti-Phishing with the Combination of Local and Global Features. In *Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and* Communications (TrustCom), New York; USA.