Employees' behavior in phishing attacks: what individual, organizational and technological factors matter?

Article (Accepted Version)

Shahbaznezhad, Hamidreza, Kolini, Farzan and Rashidirad, Mona (2020) Employees' behavior in phishing attacks: what individual, organizational and technological factors matter? Journal of Computer Information Systems. pp. 1-12. ISSN 0887-4417

This version is available from Sussex Research Online: <http://sro.sussex.ac.uk/id/eprint/93462/>

This document is made available in accordance with publisher policies and may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher's version. Please see the URL above for details on accessing the published version.

Copyright and reuse:

Sussex Research Online is a digital repository of the research output of the University.

Copyright and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable, the material made available in SRO has been checked for eligibility before being made available.

Copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational, or not-for-profit purposes without prior permission or charge, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Employees' behavior in phishing attacks: What individual, organizational and technological factors matter?

Abstract

Phishing, as a social engineering attack has become an increasing threat to organizations in cyberspace. To prevent this, a well-designed continuous security training and educational program needs to be established and enforced in organizations. Prior studies have focused on phishing attack from a limited view of technology countermeasure, email's characteristic, information processing, and securing individual's behaviors to tackle existing gaps. In this research, we developed a theoretical model of factors that influence users in the clicking of phishing emails from a broader Socio-Technical perspective. We applied Protection Motivation Theory (PMT) and habit theory for investigating individual factors, Theory of Planned Behavior (TPB) and Deterrence Theory for investigating organizational and technological factors accordingly. The findings revealed habit and protective countermeasure positively affect clicking on phishing emails, whereas, no effect of the procedural countermeasures was evident. The results of this study can be used to design phishing simulation exercise and embedded training for vulnerable employees.

Keywords:

Phishing attacks, Protection Motivation Theory (PMT), Socio-Technical perspective, email security policy, Theory of Planned Behavior (TPB).

1. Introduction

Information security and cybersecurity are amongst the biggest concerns in the organizational and societal context. Organizations and individuals substantially invest in security safeguards to protect the integrity, availability, and confidentiality of information assets. However, recent studies confirmed that these safeguards are not adequate to provide the ultimate protection of sensitive and confidential information.¹ According to Verizon Data Breach Investigation Report (DBIR),² over 30 percent of breaches are caused by phishing attacks and reported that the cost of ransomware is estimated over \$8 billion globally. Phishing attack, as a social engineering technique is designed to bypass technical countermeasures by using emails, social networks, or search engine poisoning and mobile apps.³ Phishing attacks exploit the target's cognitive biases and motivate them to rely on their heuristics behaviors and persuade targets to act by creating senses of urgency, fear of loss, or importance. Phishing emails are often crafted carefully to convince individuals to visit a bogus website, which can lead to a harvest of sensitive information (e.g., login credential, credit card numbers), installation of malware, ransomware, or remote access tool.⁴

Although technical countermeasures such as anti-phishing and spamming tools (e.g., SPF, DKIM and DMARC), email malware detection and data loss prevention (DLP) are deployed to mitigate the risk of phishing attacks, using these technologies to detect phishing attacks remains a challenging problem. This is not least because they often require human intervention to analyze and distinguish between phishing and legitimate emails. Success in the battle against phishing attacks can be achieved while organizations invest in both technological and socio-organizational functions and capabilities.⁵ Since the focus of phishing attacks shifts towards individuals and organizational resources, employee's compliance with email security policies and requirements

has been considered as a key socio-technical capability for organizations. Organizations often deploy phishing attack simulation exercises as a means to identify vulnerable employees and provide them with required phishing training to increase their organizational awareness against commonly used phishing tactics, techniques and procedures (TTPs). However, employees sometimes fail to apply their knowledge and awareness on phishing adequately.⁶ Some organizations also develop an email security policy and standard operating procedures (SOPs) to provide employees with required guidelines to ensure that email security requirements are achieved while utilizing information system (IS) resources.⁷ Hence, understanding the socio-technical antecedents to employee's compliance with the organization's email security policy and requirements is deterministic.

Employee's non-compliance behaviors have been sufficiently scrutinized through the lenses of psychology, criminology, and health belief theories. The pertinent literature examines IS misuse behaviors through deterrence and punishment,^{8,9} rational decisions^{5,10} and neutralization theories.^{7,11} There is another strand of studies which applies a meta-analysis of the relevant literature to identify key antecedents of employee's security policies compliance from different theoretical lenses. Based on their findings, training and awareness program could be useful to convince employees of the values of policies. However, security training and awareness program, including email security training, should apply theory-informed approaches that foster security competencies as a means to bolster security compliance in an organization.

Therefore, this study aims to extend the extant knowledge about employee's compliance with email security policy by identifying influential factors in email security training and awareness programs, including phishing attack simulation with embedded phishing training. To achieve this aim, our study addresses the following research questions:

1. What are technological, organizational and individual factors that influence employee's intention towards phishing attacks?
2. What is the role of socio-technical factors in shaping employee's intention towards compliance with email security policy?
3. How can organizations better train and educate employees by incorporating socio-technical factors into email security training program (e.g., phishing attack simulation exercise)?

Drawing on the Socio-Technical theory,¹² we posit that an employee's intention towards clicking on a phishing email and therefore, compliance with email security policy is shaped by the technological, individual and organizational factors. We integrated the Protection Motivation Theory (PMT) model with habit to measure past and automatic behaviors. We also investigated the role of organizational norm and procedures as organizational factors. Finally, technological countermeasures such as preventive and detective controls are used as technological factors that influence employee's intention towards clicking on a phishing email.

2. Literature review

Email technology is an integral part of daily business and commercial communications. The total number of daily business and customer emails was expected to exceed 293 billion in 2019.¹³ According to the Verizon DBIR,² over 30 percent of breaches involved phishing-spoofing attacks that attempt to mimic legitimate webpages or websites. Consequently, it is important that email security countermeasures are adequately implemented. Email security countermeasures apply a combination of technological, organizational, individual, and procedural requirements to protect against the adverse impact of phishing attacks. However, the implementation of these countermeasures is a difficult and complicated task for many organizations. Since users often fail

to distinguish emails and fall prey to phishing attacks, phishing emails are designed to bypass technological controls and exploit human cognitive biases.

Extant literature has collectively investigated the phishing attacks from different perspectives. From an individual's psychological and behavioral perspective, factors such as information carelessness,⁶ individual differences,¹⁴ information processing,¹⁵ and experiential and dispositional character,¹⁶ have been explored. From an organizational viewpoint, the impact of phishing attacks has been assessed in terms of organizational cost,¹⁷ financial loss,¹⁸ and the severity of organizational risk.¹⁹ In the area of technical countermeasures, researchers have adopted several protective and detective tools to filter out phishing emails that contain malicious content. These tools mainly use machine learning, anomaly detection, text mining and profile matching.³ Although there has been an intense debate about the technical countermeasure, there is a consensus among the researchers and practitioners on the security training. In this respect, increasing awareness through educational program has been considered as a key countermeasure to stop phishing attacks.²⁰ There are various training solutions that aim to teach end-users on how to identify phishing attempts and reduce the chance of victimization. For example, some researchers have developed some graphical cartoons to teach employees on phishing attacks.²¹ As another example, an anti-phishing game –“Anti-Phishing Phil” has been designed and used by the researchers to address good habits behaviors and inform users of the common types of phishing threat.²² Some other researchers have proposed phishing attack simulation to mimic real phishing attacks and assess the overall awareness levels of the subjects and include embedded training materials.²¹

Organizations often aim for a continuous phishing awareness and training campaigns by conducting continuous phishing simulation exercises to identify vulnerable employees and provide

them with required training. However, only well-designed security and educational programs are found to be effective enough to improve the user's ability to stop phishing attacks.²³ Thus, this research aims to investigate why individuals are susceptible to phishing attacks. We will examine how individuals avoid malicious phishing attacks by avoidance motivation behavior, prior educational knowledge and/or IT safeguards. We also intend to examine the impact of habitual automatic behaviors and shame on email phishing attacks. The results of this study can contribute to both theory and practice through identifying the influential factors in designing email simulation campaigns and training programs for vulnerable employees.

3. Theoretical foundation

To investigate the influential factors on the employees' reaction to phishing attacks, we need to find out the main areas that affect the employees' intention. Socio-Technical Theory¹³ suggests that there should be a fit between the technical subsystem and the social subsystem, which together make up an organization. The technical subsystem comprises the devices, tools and techniques required to improve the economic performance of the organization. The social subsystem includes the employees, customers, suppliers, knowledge, skills, attitudes, values, needs, rules and regulations. These all administrate the relation of people, and organizational processes and procedures to the organizations' technical subsystems.

Adopting the Socio-Technical approach enables us to explain technological counterfeits and social factors, including individual and organizational factors. To better articulate the socio subsystem in this study, we have considered two groups of individual and organizational factors. In order to explain individual and organizational factors, we referred to two theories accordingly, namely The Protection Motivation Theory (PMT)²⁴ and the Theory of Planned Behavior (TPB).²⁵

These theories have been widely employed and integrated with other theories in the relevant literature (e.g., see ref. 5). For example, Ifinedo¹ integrated TPB and PMT theories in information security compliance research. Likewise, in this research, we take behavior-intention approach to examine phishing attacks in an organizational context.

As for technological factors, we incorporate the Deterrence Theory to explain the security control that monitors employees who click on phishing to prevent or detect phishing. These theories are briefly described as follows.

3.1 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), developed by Rogers²⁵ to clarify fear appeals, is considered as one of the most powerful explanatory theories in exploring individual's intention for protective actions.²⁶ PMT has been widely employed in the IS literature to investigate user's behaviors regarding the security issues arising from security threats.²⁷ PMT explains the threat and coping appraisals. Threat appraisal is about an individual's assessment of the level of danger posed by a threatening event, such as phishing attacks.^{25,27} Threat appraisal includes of perceived vulnerability and perceived severity. The coping appraisal is an individual's assessment of the ability of the person to cope with and avert the potential loss or damage related to the threat.²⁸ Coping appraisals reflect self-efficacy, response efficacy and response cost.²⁵ In this study, we consider threat and coping appraisal factors are associated with adaptive, maladaptive behaviors that may influence users who are targeted for phishing email. From social psychology, the adaptive or maladaptive user behavior will influence user's attitude towards processing of information in phishing email.²⁸ In the adopted socio-technical approach, we employed this theory to explain

individual factors, which might affect users to cope or victimized of phishing attacks, to address the perceived consequences.

3.2 Theory of Planned Behavior (TPB)

The TPB describes an individual's intention to perform a given behavior.²⁶ Relying on TPB, the intention of performing some behaviors can be explained by the attitudes toward the behavior, subjective norms, and perceived behavioral control, which together invoke the actual behavior.²⁹ Drawing on the TPB,²⁶ we posit that an employee's intention toward clicking on phishing emails is influenced by subjective norms, perceived behavioral control and attitude toward compliance. In this research, we considered the subjective norms in the category of organizational cues that are pushed to employees by the organizational environment. Attitude towards a behavior can be shaped by rewards or sanction that is associated with a particular behavior. Hence, threat appraisal and coping appraisal factors in PMT can be used as the estimation of the outcomes contributes to the attitude related to the person's subjective understanding of the outcome of behavior.³⁰ Also, this research considers the role of procedural countermeasures in an employee's reaction on the phishing emails. The objective of creating information security procedural countermeasures is to establish security policies to make employees aware of risks related to miscellaneous emails and to educate them about their roles and responsibilities concerning those risks.

3.3 Habit Theory

In contrast to the deliberately rational behavior, habit refers to non-intentional automatic behavior that individuals may bring to IS usage.³¹ Habit Theory argues that many actions occur without any conscious decision to act, as individuals are used to perform some actions repeatedly

and regularly.³² Since the action of clicking on phishing emails can be triggered by automatic behavior tendencies developed during the history of using email on daily business operations, we include habit construct in our research framework (see Figure 1) as a predictor of intention towards clicking on a phishing email.

3.4 Deterrence Theory

Deterrence theory explains how people are motivated to obtain pleasure and avoid pain. The certainty (likelihood), celerity (swiftness), and severity (amount) of punishment are explained in this theory. In the context of IS security, this theory illustrates that the user awareness of security controls and countermeasures (i.e. monitoring and detective controls) impacts on the user perception of certainty and severity of sanctions associated with maladaptive behaviors of users fell on an phishing email.³³ This theory can be applied to address which security countermeasures or processes would be effective on user's intention whom deal with phishing and suspicious emails on a daily business as usual operations. Using Deterrence theory would enable us to investigate the underlying factors of security countermeasures that impact on user's intention to analyze and detect phishing emails in alignment with organizational security policies and training programs.

4. Research hypotheses and framework

Drawing on Socio-Technical Theory, Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Habit Theory and Deterrence Theory, we have developed our research framework as illustrated in Figure 1. The framework depicts the factors that influence intention towards non-compliance with email security policy and phishing attacks. These factors are classified into three

groups of individual, organizational and technological factors, which are discussed in the following sections.

----Insert Figure 1 about here----

4.1 Individual factors

The individual factors are proposed in consistence with prior studies (e.g., see ref. 10) which examine automatic or subconscious behavior (habit) in addition to intentional behavior (see PMT) related to decision making about the phishing attacks. We have slightly modified our framework to examine the impact of informal sanctions and shame that may influence users for not being victim of phishing attacks.³⁴ According to PMT, having information about a threat invokes a cognitive process in individuals that appraises positive or negative behavioral response. Thus, identifying phishing emails can be considered as an adaptive response, while being a victim of phishing attack is regarded as a maladaptive response. The maladaptive response invokes factors such as perceived vulnerability, severity, rewards, and shame in individual employees, which ultimately decreases the probability of maladaptive behaviors.^{11,28} **Vulnerability** in the research framework refers to the employee's assessment of whether their organization exposes to phishing attacks if no action is taken to prevent them. **Severity** denotes the negative impact of phishing email in an organization. **Rewards** promote an extrinsic physical or psychological pleasure or peer approval that may motivate the probability of maladaptive behavior. Therefore, we conceptualize rewards as saving time by not assessing email adequately to identify phishing emails. In this study, **shame** refers to a feeling of guilt or embarrassment if others know that an employee has clicked on a phishing email.³⁴ Hence, we hypothesized that:

H1a. Perceived vulnerability negatively affects employee's intention towards clicking on a phishing email.

H1b. Perceived severity negatively affects employee's intention towards clicking on a phishing email.

H1c. Perceived rewards positively affect employee's intention towards clicking in a phishing email.

H1d. Perceived shame negatively affect employee's intention towards clicking in a phishing email.

The adaptive response in PMT promotes compliance behaviors towards email phishing attack. In this research, **Response efficacy** denotes the employees' perception of the benefit of identifying a phishing email. **Self-efficacy** denotes to employees' belief that they can successfully identify a phishing email.

Finally, **response cost** addresses the inconvenienced incurred by clicking on a phishing email. Therefore, it is hypothesized that:

H1e. Response efficacy negatively affects employee's intention towards clicking on a phishing email.

H1f. Self-efficacy negatively affects employee's intention towards clicking on a phishing email.

H1g. Response cost negatively affects employee's intention towards clicking on a phishing email.

In contrast to intentional behavior, a **habit** is a form of routinized behavior¹⁰ that reflects automatic behavior intentions that have been developed during the history of an individual.³¹ Habit theory demonstrates that employee's actions occur without the conscious decision of the action and they often re-perform as individuals are accustomed to the actions. Hence, we argue that since

employees are dealing with emails daily and most emails received in organizations are genuine or innocuous, clicking on emails contents including links has become a habitual behavior. Thus, automatic habitual behaviors have a positive impact on clicking in phishing emails.

H1h. Habit positively affects employee's intention towards clicking on a phishing email.

4.2 Organizational factors

Theory of planned behaviors has been extensively used in information security literature to examine non-compliance behaviors with information security policy.^{1,5} Most of the extant IS studies have proposed a positive impact of normative on individual behavior towards compliance with information Security policy.¹²

Hence, we argue that the organizational **subjective norms and normative beliefs** have a positive impact on the employees to act with more due-diligence before clicking to suspicious phishing emails. Also, prior studies have revealed that **procedural countermeasures**, including information security standards, policies and guidelines have a positive impact on educating and uplifting security awareness among employees.⁵ Hence, we hypothesized that:

H2a. Subjective norms and normative beliefs negatively affect employee's intention towards clicking on phishing emails.

H2b. Procedural countermeasures negatively affect employee's intention towards clicking on phishing emails.

4.3 Technological factors

Technical controls and countermeasures often have a pivotal role in identifying security threats in organizations. **Detective countermeasures** refer to a monitoring capability that could track and

audit users' activities, including clicking on phishing emails. Deterrence research (e.g., see ref. 33) has posited that monitoring and surveillance functions increase sanction for non-compliance behavior. In contrast, **Preventive countermeasures** refer to protective controls, such as email proxy, anti-malware and anti-phishing technologies that are implemented by organizations to block employees' access to phishing emails. These technologies assure that emails received by employees are most likely to be genuine or harmless. Thus, they may increase automatic habitual behaviors among employees in regards to detecting phishing email as they assume that security controls will detect phishing emails before being received. Therefore, we hypothesize that:

H3a. Preventive countermeasures positively affect employee's intention towards clicking on a phishing email.

H3b. Detective countermeasures negatively affect employee's intention towards clicking on a phishing email.

5. Research Methodology

5.1. Domain identification

The conceptual framework developed in this study (see Figure 1) consists of 13 constructs and 66 latent variables that helps us to understand the employee's intention towards clicking on phishing emails. The latent variables which are so-called indicators are necessary for determining the outcome of each construct. The constructs and indicators in this study are all derived from previous studies (e.g., see ref. 10,11,35) that are validated from its point of application and the necessary of outcome. We measured each research construct (illustrated in Figure 1) with question items adapted from previously validated scales, but slightly moderated to better fit to the context of our study (See the Appendix). All items were measured on a 7-point Likert scale. We assessed

our research framework and the corresponding research hypotheses by using a hypothetical scenario method, so-called vignette method.³⁵

The constructs for individual factors that are relevant to automatic or subconscious behaviors towards phishing include: Perceived Vulnerability (H1a), Perceived Severity (H1b), Rewards (H1c), Perceived Shame (H1d), Response Efficacy (H1e), Self-efficacy (H1f), Response Cost (H1g), and Habit (H1h). Each construct is measured through a set of indicators that directly relate to the core outcome of each construct.

The construct Perceived vulnerability (H1a) has four latent variables (H1a1-H1a4) for measuring the security threat imposed by clicking on phishing emails (from ref. 10,35). To measure the impact of phishing attacks on organization and individuals, we extracted and modified four indicators (H1b1-H1b4) from Boss et al.³⁵ and Warkentin et al.³⁶ to assess the construct Perceived Severity (H1b). Five indicators (H1c1-H1c5) of the construct Rewards (H1c) proposed by Bulgurcu et al.⁵ and Vance et al.¹⁰ applied to measure the reward of non-compliance with information security policies. The construct Perceived Shame (H1d) consisted of six indicators (H1d1-H1d6) for measuring the impact of shame on individuals being subject of phishing emails (by ref. 11). The fifth individual factor of Response Efficacy (H1e) was measured through five indicators (H1e1-H1e5), adjusted from Boss et al.³⁵ and Vance et al.¹⁰ to assess individual responses to phishing attacks. The four indicators (H1f1-H1f4) of the construct Self-Efficacy (H1f) were all extracted and modified from Vance et al.¹⁰ and Warkentin et al.³⁶ to assess the coping strategy in responding to phishing email. The construct Response Cost (H1g) which was intended to measure the cost of compliance with information security policies (from ref. 10) consists of five indicators (H1g1-H1g5). The final individual factor of Habit (H1h) which includes seven indicators (H1h1-

H1h7) was measured through the items suggested by Vance et al.¹⁰ to assess automatic behaviors in response to phishing emails.

The constructs for organizational factors are related to organizational behaviors, norms and culture that may influence individual responses to phishing emails. The organizational factors consist of Subjective Norms (H2a) and Procedural Countermeasures (H2b). We applied four indicators (H2a1-H2a4) to conceptualize Subjective Norms (H2a), all derived from Ifinedo¹ for measuring the role of organizational culture and norms in information security compliance and employee's responses to phishing emails. The second organizational construct of Procedural Construct (H2b) consists of five indicators (H2b1-H2b5) for measuring the role of organizational processes and operations (i.e., standard operation procedures, standards, security training and awareness programme) regarding phishing emails (by ref. 33).

The constructs for technological factors are related to existing detective and preventive security and technology controls that may influence employee's intention in responding to phishing emails. Five indicators (H3a1-H3a5) proposed by Hovav and D'Arcy³³ were used to conceptualize Preventive Countermeasures (H3) for measuring the employee's perception about preventive security measures in response to phishing emails. The construct Detective Countermeasures (H4a) consists of five indicators (H4a1-H4a5) for measuring of the detective security controls that are implemented in organizations (from ref. 8). Finally, our dependent construct of Intention Towards Clicking on Phishing Email (Ia1) is used to measure an individual employee's intention on clicking and responding to phishing email, which consists of four indicators (Ia1-Ia4) (from ref. 5,10).

5.2. Instrument development and pre-test

In order to have a better understanding and readability of the questionnaire, the survey's items were firstly reviewed by a panel of experts from academia and industry. We adapted the approach proposed by Straub and Welke⁹ to review the questionnaire in pre-test phase. To do so, the designed survey was reviewed by 16 experts, including nine academics in information systems and computer sciences and seven professionals from industry with research background through using open-ended discussions. We initially approached the participants by email and then had consecutive meetings with them to reach a consensus on the theoretical and practical development of the survey. This review was performed to make subsequent modifications to the questions that may not be clear and partially vague. The selected latent variables in this study were mostly easily measurable and this provided a better understanding to the respondents.

Following Straub and Welke⁹, in the second step, the revised questionnaire was distributed online to a number of MSc students who had experiences in research survey methods and cybersecurity topic. In this step, 18 responses were received suggesting comments on the wording and length of the questions. The responses were used to further improve the survey's structure and presentation and make it easier to follow by non-expert participants.

5.3. Data collection and Instrument Test

After conducting the pre-test, in the third step, an exploratory study was performed in two consulting organizations in New Zealand. To do so, an online survey was distributed, of which 142 anonymous responses (58% response rate) were attained. The organizations' employees were firstly asked about their demographics (see Table 1). This was then followed by a set of questions about their organizations' requirements with respect to information security policies and phishing

emails. Those employees who were unaware of email phishing and organization's information security policy were excluded from this study.

----Insert Table 1 about here ----

Of 164 respondents, 22 participants responded that they are completely unaware of information security policies and phishing emails, so they were excluded as of uncompleted questionnaires. This left us with a sample of 142 appropriate questionnaires (a usable response rate of 36 percent) which were included in data analysis. The adequacy of the sample size was investigated by running factor analysis. The value was found to be 0.82, which indicated that the sample size is enough for performing the analysis.

----Insert Table 2 about here ----

Based on the 142 responses, the validity and reliability of the measurement items were carefully examined. To do so, we performed different reliability and validity tests. To verify reliability, two tests of indicator reliability and internal consistency reliability were assessed. To do so, we selected to apply Cronbach's alpha and composite reliability value accordingly. Both values were above the threshold of 0.7 to be accepted (see the details in Table 2). To ensure validity, first, the convergent validity was ascertained by assessing the factor loadings and calculating the variance extracted. A practical rule of thumb was used to determine if the factor loading is greater than 0.5 for a construct. As can be seen in Table 2, all loadings were above 0.5 and mostly over 0.7. Second, the discriminant validity of the items was assessed by computing the correlations between all validated constructs (see Table 3). The results confirmed that the square correlation value of each construct was over 0.9 and correlations between all pairs of constructs were below the recommended threshold value of 0.90. In simple term, the values in the diagonal of the correlation

of constructs matrix were greater than the corresponding off-diagonal correlations of the construct to their latent variables, thus the discriminant validity of the research constructs was ensured.

---Insert Table 3 about here ---

Taking all the afore-mentioned results, it is evident that the measures of all research constructs were sufficiently reliable and valid for further analysis. As a result of this stage, no measurement items of the constructs was removed from the questionnaire. Thus, in the next stage, we estimated the structural model and tested the research hypotheses.

6. Analyses and results

We tested the research framework and the research hypotheses by employing the component-based Partial Least Squares (PLS) method of Structural Equation Modeling (SEM). PLS method examines the conceptual model and its structural paths by ignoring other covariance that is not stated in the model.³⁷ This approach is suitable for estimating the proposed relationships within the research framework. To assess the research hypotheses and relevant measurement scales we used Smart-PLS 3. SmartPLS is one of the widely used software modules for PLS-SEM by both academics and practitioners.³⁸ The constructs in the model are all reflective and we used bootstrapping resampling method for analysis. The results are presented in Table 4.

---Insert Table 4 about here ---

The standardized coefficients calculated for the path model are based on one-tailed t-tests. As demonstrated in Table 4, except H1d, H1f and H2b all other proposed hypotheses are supported at a minimum of $p < 0.001$. Thus, while the individual factors of perceived vulnerability, perceived severity, rewards, response efficacy, response cost and habit significantly impact on the intention towards clicking on phishing emails, shame (H2d) and self-efficacy (H2b) are found to be unimportantly influential towards this intention. In terms of organizational factors, we found out

that in contrast to Procedural countermeasures (H2b), subjective norms and normative beliefs have a significantly negative effect on employee's intention towards clicking on phishing emails. Finally, the results reveal that both technological factors of Preventive countermeasures and detective countermeasures are highly influential on our investigated dependent variable. In overall, the results reveal that about 46% of the variance (R^2) is explained for the intention of clicking on phishing emails.

7. Discussion, implications and limitations

This study investigated three main classes of individual, organizational and technological factors on users' intention towards clicking on a phishing email. Based on the data collected from 142 users and using PLS to analyze the data, the proposed research framework and the research hypotheses (except H1d, H1f and H2b) were all verified.

This study makes significant theoretical contributions to the emerging body of knowledge on the behavioral, technological, and organizational concerns of information security. First, the extant literature has mainly identified that individual factors, rooted in PMT and habit Theory, explain the users' intention on a certain cybersecurity behavior. This study offers a robust theoretical explanation and empirical support on the impact of a comprehensive set of habit and motivational factors which influence users' behavior towards phishing attacks. Second, this study empirically investigates the role of the organizational factors, including subjective norms and procedural countermeasures in the context of phishing attacks. We proposed that the impact of subjective norms on intention towards clicking on phishing emails is stronger than the impact of procedural countermeasures. Moreover, while prior research (e.g., see ref. 36) has discussed the importance of security policies and standards in driving the systematic compliance for the employees, we have

noted that these policies and guidelines are not adequate to invoke behavioral change in employees dealing with phishing emails. Thus, we suggest that the requirements of email security policies should be embedded into organizational training structure, such as email training programs to ensure that all employees adapt themselves with security countermeasures and requirements.

Third, our study investigates the role of technological countermeasures in shaping employee's attitude towards cybersecurity challenges. Our findings indicate that technical preventive and detective countermeasures significantly influence the employee's intention for paying extra attention on suspicious emails. Consistent to prior studies, we suggest that detective controls have a significant impact on shaping accepted security behaviors. However, our findings indicate that preventive countermeasures such as anti-phishing tools and email proxy have a pivotal role in detecting phishing email, as phishing attacks have become more sophisticated to bypass privative security countermeasures. Hence, it is incumbent on employees to apply additional due-diligence to investigate any suspicious emails. Finally, given some of the prior findings related to the preventive or detective countermeasures in the non-technical context, we thought it is important to investigate the role of these countermeasures in the technological context. We have revealed that supportive technology plays a key role in explaining the employees' behavior in handling phishing emails, thus, it is suggested to be included in any relevant future research.

Additionally, the results of our study offer practical implications for cyber-security practitioners. The findings provide evidence of the significant individual, organizational and technological factors that influence employee's intention to not sink in the ocean of emails. Since all these three perspectives need to be considered by cybersecurity professionals in changing an employee's behavior in facing suspicious emails, we suggest managers and practitioners to offer some information security awareness programs⁵ and emphasize on all aspects of phishing attacks

recognized in this research. Indeed, security practitioners should aim such information security awareness programs to inform users about intrinsic and extrinsic factors which can influence their behavior. Therefore, employees can be more vigilante to understand how cybersecurity criminals can exploit employee's perception from different individual/motivational, organizational, and technological perspectives. Employees may need to know about the existing security arsenals alongside with the security risks that could be exploited by malicious attackers.

This study has a number of limitations. One of the main ones is related to the sampling and method of data collection. We collected relatively a small data set from employees of two consulting organizations in New Zealand. While this could potentially bring some unwanted errors in the results, we tried to have a heterogeneous sample from each organization to represent participants from different age, gender and educational levels. The result was very similar across the age, gender and education and does not have any significant impact on the model fit. This demonstrates a relative insensitivity of the results to the demographics of the participants. For greater assurance of the invariability of the results, we suggest future research to further enrich our research findings through collecting a larger sample from different industries in different regions/countries to generalize the research findings and assess whether employee's intention with respect to cybersecurity attacks differ in different contexts.

References

-
- ¹ Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 2012; 31(1):83-95.

-
- ² Verizon. Data breach investigation report. USA: Verizon; 2020 [accessed 2020 July 8].
<https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>.
- ³ Aleroud A., Zhou L. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*. 2017; 68(7):160-196.
- ⁴ Arachchilage NAG, Love S, Beznosov K. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*. 2016; 60(7):185-197.
- ⁵ Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*. 2010; 34(3):523-548.
- ⁶ Workman M. A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*. 2008; 59(4):662-674.
- ⁷ Willison R, Warkentin M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*. 2013; 37(1):1-20.
- ⁸ D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*. 2009; 20(1):79-98.
- ⁹ Straub DW, Welke RJ. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*. 1998; 22(4):441-469.

-
- ¹⁰ Vance A, Siponen M, Pahnla S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*. 2012; 49(3-4):190-198.
- ¹¹ Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*. 2010; 34(3):487-502.
- ¹² Bostrom RPH, Heinen JS. MIS problems and failures: a socio-technical perspective. *MIS Quarterly*. 1977; 1(3):17-32.
- ¹³ Radicati Group Inc. Email statistics report, 2017-2021. Palo Alto (CA): Radicati; 2017 [Accessed 2019 Dec. 31]. <https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf>.
- ¹⁴ Vishwanath A, Herath T, Chen R, Wang J, Rao R. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*. 2011; 51(3):576-586.
- ¹⁵ Luo X, Zhang J. How do consumer buzz and traffic in social media marketing predict the value of the firm? *Journal of Management Information Systems*. 2013; 30(2):213-238.
- ¹⁶ Wright RT, Marett K. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*. 2010; 27(1):273-303.
- ¹⁷ Jakobsson M, Myers S. Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Hoboken. New Jersey (USA): John Wiley & Sons; 2006.

-
- ¹⁸ Singh N. Online frauds in banks with phishing. *The Journal of Internet Banking and Commerce*. 2007; 12(2):1-27.
- ¹⁹ Chen X, Bose I, Leung ACM, Guo C. Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*. 2011; 50(4):662-672.
- ²⁰ Jansson K, Solms RV. Phishing for phishing awareness. *Behaviour & Information Technology*. 2013; 32(6):584-593.
- ²¹ Srikwan S, Jakobsson M. Using cartoons to teach internet security. *Cryptologia*. 2008; 32(2):137-154.
- ²² Davinson N, Sillence E. It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*. 2010; 26(6):1739-1747.
- ²³ Kumaraguru P, Cranshaw J, Acquisti A, Cranor L, Hong J, Blair MA, Pham T. School of phish: A real-world evaluation of anti-phishing training. Paper presented at: 5th Symposium on Usable Privacy and Security; 2009 July 15-17; Mountain View (CA).
- ²⁴ Rogers RW. 1983. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In: Cacioppo JT, Petty R. Editors, *Social psychophysiology: A sourcebook*. New York: Guilford Press.
- ²⁵ Ajzen I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. 1991; 50(2):179-211.
- ²⁶ Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*. 2010; 34(3):613-643.

-
- ²⁷ Woon I, Tan GW, Low R. A protection motivation theory approach to home wireless security. Paper presented at: Twenty-Sixth International Conference on Information Systems; 2005 Dec. 11-14; Las Vegas, NV.
- ²⁸ Vishwanath A, Harrison B, Ng YJ. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*. 2018; 45(8):1146-1166.
- ²⁹ Armitage CJ, Conner MT. Efficacy of the theory of planned behaviour: A meta-analytical review. *British Journal of Social Psychology*. 2001; 40(4):471-499.
- ³⁰ Ajzen I. 1985. From intentions to actions: A theory of planned behavior. In Kuhl J, Beckmann J. Editors, *Action control: From Cognition to Behavior*. London (UK): Springer.
- ³¹ Limayem M, Hirt SG. Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*. 2003; 4(1):65-97.
- ³² Goh T-T, Xin Z, Jin D. Habit formation in social media consumption: a case of political engagement, *Behaviour & Information Technology*. 2019; 38(3):273-288.
- ³³ Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*. 2012; 49(2):99-110.
- ³⁴ Piquero NL, Tibbetts SG, Blankenship M.B. Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior*. 2005; 26(2):159-188.

-
- ³⁵ Weber J. Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly*. 1992; 2(2):137-160.
- ³⁶ Warkentin M, Johnston AC, Shropshire J, Barnett WD. Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*. 2016; 92(12):25-35.
- ³⁷ Straub D, Boudreau MC, Gefen D. Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*. 2004; 13(1):380-427.
- ³⁸ Wong KKK. Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*. 2013; 24(1):1-32.

Figure 1: Theoretical framework

Table 1. Profiles of responding participants

	Frequency	Percentage
Gender		
Men	92	65
Women	50	35
Age		
18-24	57	42
25-34	55	39
35-44	16	11
Over 44	7	5
Knowledge of IT		
1 (Very Low)	0	0
2	3	2
3	14	10
4	27	19
5	59	42
6	29	20
7 (Very High)	10	7
Email check per day (Times)		
1-3	24	17
4-6	51	36
7-10	27	19
11-20	24	17
More than 20	16	11
Work or personal email		
Work	111	78
Personal	31	22
Highest level of education		
Less than high school	1	1
High school/College degree	14	10
Undergraduate degree	98	69
Postgraduate degree	29	20
	Mean	STD
Years of Internet usage	16.73	6.14
The length of service at the organization	6.61	6.81
	Frequency	Percentage
Has your employer established information Security?		
Yes	142	100
No	0	0

To what extent are you aware of phishing email requirements /obligations addressed by the information security policy of your organization?		
1 (Completely Unaware)	0	0
2	0	0
3	14	10
4	30	21
5	36	25
6	28	20
7 (Completely aware)	34	24

Table 2- Determination of AVE, composite reliability and Cronbach's alpha value after bootstrapping

Constructs	Indicator	Factor Loading	AVE	Composite reliability	Cronbach's alpha
Perceived Vulnerability	H1a1	0.73	0.74	0.72	0.87
	H1a2	0.77			
	H1a3	0.91			
	H1a4	0.84			
Perceived Severity	H1b1	0.72	0.57	0.70	0.77
	H1b2	0.87			
	H1b3	0.90			
	H1b4	0.88			
Rewards	H1c1	0.80	0.56	0.83	0.75
	H1c2	0.89			
	H1c3	0.92			
	H1c4	0.86			
	H1c5	0.85			
Shame	H1d1	0.72	0.64	0.81	0.77
	H1d2	0.80			
	H1d3	0.80			
	H1d4	0.91			
	H1d5	0.73			
	H1d6	0.77			
Response Efficacy	H1e1	0.83	0.67	0.84	0.88
	H1e2	0.90			
	H1e3	0.84			
	H1e4	0.71			
	H1e5	0.74			
Self Efficacy	H1f1	0.91	0.76	0.77	0.90
	H1f2	0.80			
	H1f3	0.80			
	H1f4	0.77			
Response Cost	H1g1	0.74	0.77	0.83	0.94
	H1g2	0.76			
	H1g3	0.81			
	H1g4	0.87			

	H1g5	0.92			
Habit	H1h1	0.78	0.74	0.83	0.82
	H1h2	0.90			
	H1h3	0.75			
	H1h4	0.91			
	H1h5	0.82			
	H1h6	0.71			
	H1h7	0.75			
Subjective Norms	H2a1	0.80	0.69	0.85	0.71
	H2a2	0.81			
	H2a3	0.70			
	H2a4	0.71			
Procedural Countermeasures	H2b1	0.85	0.68	0.74	0.80
	H2b2	0.87			
	H2b3	0.78			
	H2b4	0.83			
	H2b5	0.91			
	H2b6	0.77			
	H2b7	0.71			
Preventive Countermeasures	H3a1	0.73	0.74	0.76	0.81
	H3a2	0.88			
	H3a3	0.86			
	H3a4	0.90			
	H3a5	0.76			
Detective Countermeasures	H3b1	0.81	0.75	0.76	0.75
	H3b2	0.88			
	H3b3	0.87			
	H3b4	0.85			
	H3b5	0.71			
Intention Towards Clicking on Phishing Emails	Ia1	0.87	0.61	0.70	0.85
	Ia2	0.90			
	Ia3	0.89			
	Ia4	0.85			
	Ia5	0.73			

Table 3: correlation analysis

	Perceived Vulnerability	Perceived Severity	Rewards	Shame	Response Efficacy	Self Efficacy	Response Cost	Habit	Subjective Norms	Procedural Countermeasures	Preventive Countermeasures	Detective Countermeasures	Intention Towards Clicking on Phishing Emails
Perceived Vulnerability	0.93												
Perceived Severity	0.53	0.94											
Rewards	0.76	0.69	0.96										
Shame	0.78	0.81	0.64	0.93									
Response Efficacy	0.85	0.88	0.55	0.52	0.94								
Self Efficacy	0.79	0.72	0.82	0.82	0.88	0.93							
Response Cost	0.86	0.81	0.76	0.84	0.71	0.84	0.91						
Habit	0.64	0.87	0.63	0.82	0.64	0.77	0.87	0.94					
Subjective Norms	0.52	0.88	0.59	0.71	0.87	0.59	0.57	0.76	0.93				
Procedural Countermeasures	0.75	0.88	0.63	0.63	0.67	0.67	0.80	0.78	0.79	0.92			
Preventive Countermeasures	0.61	0.85	0.66	0.81	0.78	0.65	0.70	0.87	0.66	0.54	0.94		
Detective Countermeasures	0.79	0.80	0.63	0.81	0.73	0.70	0.62	0.71	0.63	0.76	0.67	0.91	
Intention Towards Clicking on Phishing Emails	0.68	0.60	0.87	0.51	0.73	0.51	0.82	0.70	0.63	0.55	0.81	0.83	0.91

Table 4- Hypotheses and t-values

Hypothesis	t – values	Supported (one-tail)	p-value
H1a	4.36	Supported	p < .001
H1b	2.75	Supported	p < .050
H1c	5.68	Supported	p < .050
H1d	1.23	Not supported	p < .200
H1e	3.09	Supported	p < .001
H1f	1.58	Not supported	p < .150
H1g	5.96	Supported	p < .001
H1h	4.14	Supported	p < .001
H2a	5.01	Supported	p < .001
H2b	1.46	Not supported	p < .200
H3a	5.37	Supported	p < .001
H3b	3.33	Supported	p < .001

Appendix- Scenarios and questionnaire

Scenario 1- Violation: clicking on a phishing email

Niles is working on a project that requires access to the organization's customer details and confidential financial information. His organization has provided him with sufficient training on identifying and reporting of phishing emails. However, Niles is going on a business trip and would like to apply clients' data and financial information for his presentation slides. Niles checked his email at the airport and found out that there is an email from the organization's service desk requiring him to click on a link and change his password immediately due to a security incident. He clicked on the link quickly and entered his old and new password to ensure that he can access the organization's file when he arrived at his destination.

Scenario 2- Violation: Reporting of a phishing email

Gina is a low-level manager in an insurance organization where she was recently hired. Her organization has a strong email security policy that requires stringent compliance with email security requirements. Gina has a client-facing role, which requires her to send and receive emails to and from clients on a daily basis. Recently, Gina discovered a phishing email that was crafted from a trusted client. Gina called the client and informed them about the phishing email. However, due to her busy workload, she forgot to contact the organization's Information Security department and report the phishing email. Gina knows that email security policy mandates reporting of phishing emails. However, since she has not clicked on the email and deleted the email, she does not think that the security risk is high enough to report the case to the Information Security department.

Questionnaire:

Perceived vulnerability

- I could be subjected to an information security threat, if I would do what [the scenario character] did.
- My organization could be subjected to information security threat, if I did what [the scenario character] did.
- An information security problem could occur, if I did what [the scenario character] did.
- I am unlikely to lose sensitive data, if I did what [the scenario character] did.

Perceived severity

- If I would do what [the scenario character] did, there would be serious information security problems for my organization.
- If I would do what [the scenario character] did, serious information security problems would result.
- An information security breach in my organization would be a serious problem for me.
- Loosing data would be unlikely to cause a major problem.

Rewards

- If I would do what [the scenario character] did, I would save work time and perform my tasks.
- If I would do what [the scenario character] did, I would save time.
- Non-compliance with the information security policies saves work time.
- My pay raises and/or promotions depend on whether I comply with the requirements of the information security policies.

-
- I will be given monetary and non-monetary rewards, if I comply with the requirements of the information security policies.

Shame

- If I would do what [the scenario character] did, I would be ashamed to see my co-workers knew that I had violated the organization's email security policy.
- If I would do what [the scenario character] did, I would be ashamed to see others knew that I had violated the organization's email security policy.
- If I would do what [the scenario character] did, I would be ashamed to see my managers knew that I had violated the organization's email security policy.
- I would have problem if I felt ashamed that my co-workers knew that I did what [the scenario character] did.
- I would have problem if I felt ashamed that my managers knew that I did what [the scenario character] did.
- I would have problem if I felt ashamed that others knew that I did what [the scenario character] did.

Response efficacy

- Complying with email security policy in our organization keeps cybersecurity breaches down.
- If I comply with email security policy, cybersecurity breaches are scarce.
- Careful compliance with email security policy helps to avoid cybersecurity problems.
- Anti-malware software works for protection against phishing attacks.
- Anti-malware software is efficient for protection against phishing attacks.

Self-efficacy

-
- I can comply with email security policy by myself.
 - Doing the opposite of what the [the scenario character] did would be difficult for me to do.
 - At this moment, I could identify and report phishing email, if there was no one around to tell me what to do.
 - At this moment, I could identify and report phishing email, if I could call someone for help if I got stuck.

Response cost

- Complying with email security policy inconveniences my work.
- There are too many overheads associated with complying with email security policy.
- Enabling phishing email detection measures in my organization is/would be time consuming.
- The cost of implementing recommended email security controls is more than its benefit.
- The impact of the organization's email security control in my work is lower than the benefit.

Habit

- Complying with email security policy is something I do automatically.
- Complying with email security policy is something I do without having to consciously remembering it.
- Complying with email security policy is something that makes me feel weird if I do not do it.
- Complying with email security policy is something that belongs to my (daily, weekly, monthly) routine.
- Complying with email security policy is something that I start doing before realizing I am doing it.
- Complying with email security policy is something that I have no need to think about doing it.

-
- Complying with email security policy is something that I would find hard not to do it.

Subjective norm

- My boss thinks that I should follow the organization's email security policy.
- My colleagues think that I should follow the organization's email security policy.
- My organization's IT department pressures me to follow the organization's email security policy.
- My subordinates think I should follow the organization's email security policy.

Procedural countermeasures

- My organization has specific guidelines that describe acceptable security requirements for the use of email.
- My organization has established rules of behavior for use of email.
- My organization provides training to help employees improve their awareness of email security issues.
- My organization has a formal policy that enforces employees to report phishing emails that they receive.
- In my organization, employees are briefed on the consequences of opening the phishing email and click on the relevant Internet link.
- In my organization, employees are briefed on the consequences of not reporting phishing incidents.
- My organization educates employees on their email security responsibilities.

Preventive countermeasures

- I believe that my organization implements security controls to prevent phishing emails.

-
- I believe that my organization implements preventive controls to ensure that it remains secured even though employees click on phishing emails.
 - I believe that my organization has preventive security controls to protect the network and my computer.
 - I believe that my organization has preventive security controls against stealing or deleting organizational information.
 - I believe that my organization conducts periodic audits to identify weakness in preventive security controls.

Detective countermeasures

- I believe that employees' computing activities are monitored by my organization.
- I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized task.
- I believe that my organization actively monitors the content of employees' email messages.
- I believe that my organization reviews log of employees computing activities on a regular basis.
- I believe that my organization conducts periodic audits to identify weakness in detective security controls.

Intention to click on a phishing email

- I would act in the same way as [the scenario character] did, if I was in the same situation.
- The chance that I would do what [the scenario character] did in the described scenario is low.
- I intend to comply with the requirements of the email security policy of my organization in the future.

-
- I intend to protect information and technology resources according to the requirements of the email security policy of my organization in the future.
 - I intend to carry out my responsibilities prescribed in the email security policy of my organization when I use organizational email in the future.