Telematics and Informatics 48 (2020) 101343

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Why do users not report spear phishing emails?

Youngsun Kwak[a], Seyoung Lee[b,*], Amanda Damiano[c], Arun Vishwanath[d]

[a] Program in Interactive Contents, Inter-Department Program, Graduate School, Inha University, Republic of Korea
[b] Department of Media and Communication, Sungkyunkwan University, Republic of Korea
[c] Department of Communication, Marist College, United States
[d] Avant Research Group (ARG), LLC, United State

ARTICLE INFO

Keywords:
Spear phishing emails
Self-efficacy
Negative outcomes
Self-monitoring
Cyber risk beliefs

ABSTRACT

Cyber security training programs encourage users to report suspicious spear phishing emails, and most antiphishing software provide interfaces to assist in the reporting. Evidence, however, suggests that reporting is scarce. This research examined why this is the case. To this end, Social Cognitive Theory (SCT) was used to examine the influence of the triadic factors of perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring, on individuals' likelihood of reporting spear phishing emails. Based on recent research on phishing victims, the present study also incorporated cyber risk beliefs (CRBs) into the SCT framework. The model, tested using survey data (N = 386), revealed that the likelihood of reporting spear phishing emails is increased by perceived self-efficacy, expected negative outcomes, and cyber security self-monitoring. Furthermore, the CRBs directly influenced the three SCT factors and indirectly the individuals' likelihood of reporting spear phishing emails. The findings add to our understanding of SCT and the science of cyber security.

1. Introduction

Spear phishing, the fraudulent practice of sending emails with malware hidden behind hyperlinks and attachments that appear to come from legitimate sources (e.g., a trusted and well-known company), is the most common method of attack used by hackers today (Vishwanath, 2016a; Vade Secure, 2018). Most cyber security experts consider phishing attacks as one of the most prominent modes of the Nigeran email scam or advance-fee fraud types, wherein spear phishing seems to be its more sophisticated form: it involves emails that appear to come from trusted sources, having specific individuals or departments within organizations as targets ("KnowBe4," n.d.). Spear phishing is responsible for a wide variety of breaches, from the infamous Sony Pictures Entertainment hack to the Democratic National Committee (DNC) servers hack that roiled Hilary Clinton's presidential campaign (Vishwanath, 2016b). The same method has also been associated to attacks on industrial control systems, espionage, and terrorism, making it one of the most pressing cyber security problems that society currently faces.

Today, the most widely implemented user-focused intervention is concerned with training individuals to increase their security awareness. Major training programs emphasize reporting; they encourage users to report suspected spear phishing emails to an incident response team, usually the help desk of the information technology (IT) department. The effectiveness of user training to increase security awareness is demonstrated in the substantial decrease in the rate of clicking on malicious links embedded in phishing emails by 64%, as reported by a survey of 377 IT practitioners in the U.S. (Ponemon Institute, 2015). Similarly, Caputo et al.

* Corresponding author at: Department of Media and Communication, Sungkyunkwan University, Seoul, Republic of Korea.
E-mail address: gethemane@skku.edu (S. Lee).

https://doi.org/10.1016/j.tele.2020.101343
Received 17 August 2019; Received in revised form 31 December 2019; Accepted 5 January 2020
Available online 08 January 2020
0736-5853/

(2014) found that the rate of clicking on phishing links decreased by approximately 63% after training in their study, which was designed to measure the effectiveness of the antiphishing education against simulated spear phishing emails with the sample of 1,395 workers from an organization based in Washington DC.

The effectiveness, however, is limited by the failure or ignorance in complying with policies recommended in security awareness trainings (Caputo et al., 2014; Siponen et al., 2014; Tsai et al., 2016) as well as relapse to habitual patterns of email use (Vishwanath, 2015). Considering the forgoing issues, the reasons of the vulnerability of individuals in terms of phishing emails were explored in the literature on the matter. Prior research has uncovered that certain types of message cues containing authority, urgency, or social proof persuasion techniques are involved in the most effective and successful phishing attempts (Butavicius et al, 2016; Vishwanath et al., 2011; Wang et al., 2012; Williams et al., 2018). Another line of research focused on the individual differences such as personality traits and cognitive information processing of the victims of phishing attempts. On the one hand, it was found that conscientiousness has a positive effect on the victim's response to phishing emails. On the other hand, cyber risk perception and the level of suspicion, aroused by Cyber Risk Beliefs (CRBs) and systematic information processing have a negative effect on the victim's vulnerability to phishing (Halevi et al., 2015; Vishwanath et al., 2016; Williams et al., 2017).

In terms of reporting suspicious emails, evidence suggests that users seldom report. For instance, in a simulated phishing test for 1,000 target users, 20.3% of the target population clicked on a link embedded in a phishing email and only 7.4% of them reported it to the help desk, as per the phishing campaign assessment conducted in 2018 by the Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS). It also showed that the ratio of reports-to-clicks was only 0.68. A similar finding was addressed in the 2019 Data Breach Investigations Report (DBIR) conducted by Verizon. In a simulated phishing email test, approximately half of the phishing victims reported it a few weeks later (Verizon, 2019). The tendency of underreporting is also visible in other types of cybercrimes such as data breaches in businesses. According to a news article (CSO, 2019), the Internet Crime Complaint Center (IC3) of the FBI in the U.S. released data showing that only 15% of business cybercrime victims reported their respective incidents to law enforcement in 2018, and only 28% of cyberattacks against businesses in the UK were reported to the police in 2016.

The general idea here is that reporting makes early detection possible and allows the IT of the company to inform others of an attack before it spreads. To make reporting easy, many antiphishing toolbars and programs provide a convenient mechanism (e.g., PhishMe Reporter installer, an email add-on software that provides a one-stop direct link to report a suspected email). Moreover, Google Chrome, a web browser, provides a security warning to its users when downloading suspicious Portal Document Format files (Krol et al., 2012). Though there are many benefits of reporting phishing emails and significant resources have been expended in security training and maintaining incident response teams, most users opt to not report spear phishing emails. The goal of the study, therefore, is to answer the question: *Why do more users not report spear phishing emails?*

To understand why people consciously choose not to perform a behavior, this study adopts a leading theory of human agency, the Social Cognitive Theory (SCT) (Bandura, 1986, 1997). SCT explicates the motivational mechanisms that drive human action. Its central thesis, supported by almost three decades of empirical research, is that people's behavioral intentions are shaped by the triadic interactions among their self-efficacy, the outcomes they expect from the intended behavior, and their self-monitoring or ability to observe, judge, and enact behaviors that support the performance of the intended action. From a spear phishing-reporting standpoint, these constructs translate to the following: users' self-efficacy toward reporting spear phishing emails and performing supportive behaviors that safeguard against phishing victimization; the expected outcomes from reporting suspected spear phishing emails; and their attentive application of online cyber safety standards that indicates their conscious monitoring of actions, which could prevent their victimization through spear phishing.

Our choice of SCT's framework is because cognitive processes, particularly the different types of information processing that users engage and their motivations, have been the focus of much of the research on spear phishing victimization (Vishwanath et al., 2011; Wang et al., 2012). In addition, constructs such as computer self-efficacy and self-monitoring, derived from SCT, are often evoked to explain why people fall victim to phishing (Rhee et al., 2009; Vishwanath et al., 2011), making the framework well-suited for this investigation.

Additionally, recent research on cyber security has identified a new construct, Cyber Risk Beliefs (CRBs), defined as users' perceptions about the inherent risks of their online actions (Vishwanath et al., 2016, 2017). Research has shown that high CRBs play a pivotal role in determining whether people fall victim to spear phishing by motivating them to expend more cognitive resources toward assessing the veracity of emails. Thus, another goal of our research is to examine whether CRBs can serve as a scope condition in SCT, indirectly motivating individual willingness to report suspected spear phishing emails, by directly influencing the triadic factors in SCT. Our hypothesis is rooted in the idea that if CRBs could influence information processing decisions within a context, it could also influence the broader cognitive processes—self-efficacy, self-monitoring, outcome expectations—which according to SCT, ultimately motivate human action.

Support for our hypothesis would extend the SCT whilst also expanding our understanding of the role of CRBs in shaping users' spear phishing email reporting behavior. With this goal in mind, we examined whether users' CRBs could influence their self-efficacy toward performing behaviors that safeguard against spear phishing victimization, their perceptions of the outcomes from reporting suspected spear phishing emails, and their self-monitoring of their cyber safety behaviors.

We begin the next section with an overview of the research model and hypotheses, followed by the methods, measures, analysis, results, and discussion in subsequent sections.

2. Theoretical premise

2.1. The social cognitive motivational processes

SCT (Bandura, 1986, 1989, 1997, 1998) explicates the motivational mechanisms that lead to and support human action. The theory characterizes human behavior as agentic, meaning that human behavior is motivated and regulated by self-influence and not just by the inner forces of personality or external forces of environmental events. In other words, people influence their own circumstances and are not just products of it. In SCT, people form behavioral intentions by monitoring their current behaviors against prospective actions, assessing their own adequacies and capabilities, and evaluating the relative positive and negative outcomes from the intended actions. Thus, human actions are self-directed outcomes of forethought, metacognition, and prior behavior that iteratively influence, inspire, or discourage prospective behavior.

In SCT, the stage of forethought involves examining outcome expectations, which is the assessment of the expected negative or positive results of the prospective behavior (LaRose et al., 2003). Metacognition involves the constructs of self-efficacy, defined as the individuals' confidence in performing a behavior (Vishwanath et al., 2011; Wang et al., 2012). Finally, self-monitoring involves the ability to observe and calibrate one's enactment of an intended behavior or perform ancillary behaviors related to or supportive of the prospective action (Rhee et al., 2009).

The focal intended action in the present study is the likelihood of reporting a spear phishing email. Within this context, the primary outcome expectation is determining whether the user foresees some negative outcome from reporting. The sole focus on estimating negative experiences is for two reasons. First, most phishing reporting portals are unidirectional, where a user reports a suspected email to a help-desk in-box and usually never receives any direct feedback. As a case in point, even the Internet Crime Complaint Center (IC3), the cybercrime reporting online portal setup by the FBI, does not provide any direct feedback to individuals who report. Thus, people seldom receive any positive feedback for reporting or foresee any direct benefit from reporting. Second, when it comes to human behavior, fear of negative outcomes, rather than the hope for positive ones, is almost always stronger drivers of performance (Maddux and Rogers, 1983). As such, people are far more likely to avoid engaging in a behavior for fear of recrimination, embarrassment, or shame. This makes negative outcomes more salient in cognition and a more important consideration from a measurement perspective.

Further, in any behavioral context, self-efficacy is generally narrowly defined, but delineating its broader influences allows for a better understanding of the true motivations behind behavior (Bandura and Cervone, 1983). For instance, in a public health study on the motivations behind leading a healthy lifestyle, the self-efficacy in terms of achieving a healthy lifestyle might be the product of the second-order influences of maintaining a food diary and following through with a regular exercise regimen. Measuring such second-order influences not only gives us a richer understanding of the factors motivating self-confidence but also allows us to identify the factors that play more important roles in motivating positive lifestyle changes. For this reason, within the spear phishing reporting context, we focused on perceived self-efficacy toward performing antiphishing behaviors as the first-order and second-order construct of efficacy toward reporting and toward performing generally safe cyberspace safe actions.

Furthermore, in SCT, self-monitoring translates to the individuals' attentive enactment of safe cyber actions, which directly indicates the degree of conscious calibration of cyber behaviors and points to how well individuals can observe, judge, and correct their cyber safety behaviors (LaRose et al., 2003; Rhee et al., 2009). Finally, because forethought, the estimation of outcomes, and metacognition are all fundamentally the outcome of cognitive processes, we also examined whether users' CRBs, which have been shown to motivate directly users' phishing related cognitive processing, also influence these SCT-based constructs, and indirectly influence the likelihood of spear phishing reporting.

Fig. 1 presents an overview of the research model. The relational paths between the various constructs in the model are based on decades of research on SCT as well as recent research on spear phishing. These, along with the hypotheses, are sequentially examined.

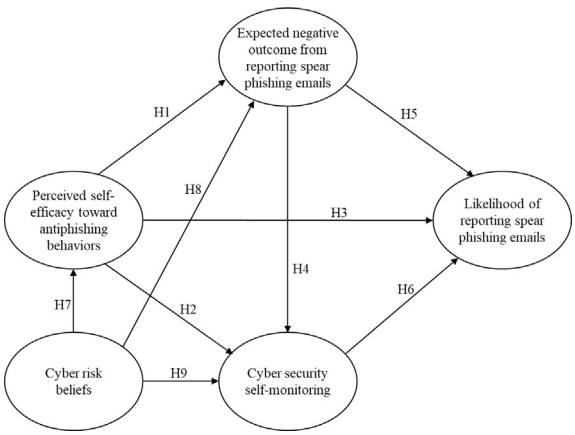


Fig. 1. Research model based on the Social Cognitive Theory and recent research on spear phishing.

2.2. The influence of self-efficacy on spear phishing reporting

In SCT, self-efficacy (i.e., people's confidence in the ability to perform a behavior) is considered one of the most important motivators of behavior (Bandura, 2006). Self-efficacy motivates behavior directly by providing a sense of confidence in continuing an action. It also motivates behavior indirectly by influencing the cognitive and affective assessments about the behavior as well as one's actual performance of behavior or actions that support the intended behavior. For instance, people who have high confidence in their ability to lose weight might be more particularly concerned about suffering health issues due to their body weight (negative outcome expectations), which often has a stronger motivating influence than positive outcome expectation, such as looking good or fitting in one's clothes. Awareness of different approaches to weight loss and the past performance of supportive behaviors, such as running or maintaining a food diary, might provide the ability to calibrate actions (high self-monitoring); this could then lead to successful weight loss and serve as the impetus to persist with efforts even when they seem ineffective. Thus, self-efficacy influences the types of outcomes people expect from a behavior as well as their self-monitoring of behaviors, ultimately leading to the desired outcome.

Extending this to the cyber security standpoint, previous studies have found that self-efficacy plays its role in motivating cyber security behaviors both directly and indirectly through outcome expectations or self-monitoring. For example, Vishwanath et al. (2011) identified that perceived self-efficacy in knowledge regarding email use and email-based phishing attempts negatively influences the likelihood of responding to a phishing email. In a similar vein, Wang et al. (2017) found that an individual with high self-confidence in the ability of detecting a phishing email shows stronger intention to adopt coping behaviors such as thoughtfully analyzing cues presented in an email to determine its legitimacy. Moreover, regarding the relationship between self-efficacy and self-monitoring, Rhee et al. (2009) found that self-efficacy in information security influences not only the use of security protection software but also security conscious care such as not sharing sensitive information via email or using passwords that are difficult to guess.

Based on the previous studies, therefore, we expect self-confidence in antiphishing behaviors to influence users' willingness to report suspected spear phishing emails. We also expect users with high security self-efficacy to be better calibrated for understanding the value of reporting through the conscious enactment of cyber safe behaviors. Thus, users with high security self-efficacy are expected to exhibit higher monitoring (i.e., higher security awareness and engagement in cyber safe behaviors). For this reason, it is also expected that users with high self-efficacy are more concerned about the negative outcomes from reporting, such as the outcomes from reporting a legitimate email falsely or reporting too many such emails—actions that would undermine the users' personal view of their own competency and erode their sense of efficacy overtime. When a person possessing a higher level of self-efficacy based on personal standards or challenging goals expects negative self-evaluative outcomes of performance, they put intense effort in goal attainment; whereas individuals with a lower level of self-efficacy and with self-doubt give up or avoid performing further.

Hypothesis 1. Perceived self-efficacy toward antiphishing behaviors will have a significantly positive relationship with expected negative outcomes from reporting spear phishing emails.

Hypothesis 2. Perceived self-efficacy toward antiphishing behaviors will have a significantly positive relationship with cyber security self-monitoring.

Hypothesis 3. Perceived self-efficacy toward antiphishing behaviors will have a significantly positive relationship with the likelihood of reporting spear phishing emails.

2.3. The influence of outcome expectations on spear phishing reporting

In SCT, the anticipated self-evaluative outcomes from any intended behavior are also important motivators of its performance. Generally, when it comes to expected negative outcomes—which, as explained earlier, are of greater interest in the phishing-reporting context—self-monitoring serves as an adaptive counter-balance measure. The reason is that the fear of negative outcomes gives rise to a sense of threat that undermines people's self-worth in coping; most people increase self-monitoring of actions to decrease the likelihood of the negative event (Bandura, 1986; Dijkstra and Buunk, 2008; Dijkstra et al., 1999). For instance, if someone driving cross country is informed of bad weather conditions along the way (a potential negative outcome), they would enhance the care (their self-monitoring) with which they drove their vehicle (the performance of the behavior). Such careful driving would be influenced by their belief in their ability to drive carefully as well as the belief that such care would improve their safety (self-efficacy). Analogously, negative outcomes from spear phishing reporting (e.g., fear, embarrassment, or being subjected to ridicule) is expected to increase the monitoring of behaviors that help assure the likelihood of reporting. Furthermore, because high self-monitoring and high self-efficacy are expected to serve as a buffer against the actualization of negative outcomes, our research model posits that expected negative outcomes from reporting would also continue to influence reporting positively.

Hypothesis 4. Expected negative outcomes from reporting spear phishing emails will have a positive relationship with cyber security self-monitoring.

Hypothesis 5. Expected negative outcomes from reporting spear phishing emails will have a positive relationship with the likelihood of reporting spear phishing emails.

2.4. The influence of self-monitoring on spear phishing reporting

In SCT, people's self-monitoring mechanisms make them regulate their behaviors to achieve desired goals. Self-regulation operates through three sub processes: self-observation, self-judgment, and self-reaction. Self-observation of actions provides people with an analysis of their behaviors. Such analysis enables people to judge the adequacy of their performed behaviors based on their personal standards. Their self-reaction to this assessment then leads to course-corrections that help achieve the desired goal (Bandura, 1989). In the current research context, enhanced self-monitoring of one's cyber security behaviors, for instance, by giving consistent attention to different cyber safety considerations while online, is expected to result in better self-diagnosis and better coping strategies against any setbacks encountered while performing cyber security behaviors. It is also expected to lead to better awareness and understanding of the value of reporting, which is also a cyber safety behavior. Hence, the research posits the following:

Hypothesis 6. Cyber security self-monitoring will have a positive relationship with the likelihood of reporting spear phishing emails.

2.5. Cyber risk beliefs

People's perceptions of online risk, their CRBs, have been shown by recent research to be an indirect predictor of their overall susceptibility to phishing attacks (Vishwanath et al., 2016). High CRBs decrease susceptibility to spear phishing by motivating systematic processing, which, in-turn, influences the amount of suspicion emails arouse. In contrast, low CRBs increase susceptibility by increasing the users' reliance on heuristics. Thus, the level of CRBs serves as an exogenous trigger of cognitive mindfulness.

The social-cognitive motivational mechanisms of self-efficacy, self-monitoring, and self-reactive outcome expectations are at their core also cognitive processes that control the performance of human behavior. They are also recursively influenced by each other and external environmental stimuli, such as other people's reactions to media influences that iteratively shape behavior. Within these processes, one can imagine more contextualized cognitive sub-processes. For instance, people might acquire a heuristic on the sophistication of spear phishing from a news story that might influence confidence in their own ability (cyber security self-efficacy) in detecting such attacks or in the quality of their own judgments and the effectiveness of their self-monitoring abilities. Thus, constructs that might influence cognitive processes might also influence the motivational mechanisms proposed by the SCT. Here, CRBs is of particular interest because it has already been shown to enhance the cognitive resources users are willing to deploy in assessing the legitimacy of suspected spear phishing emails. We, therefore, expect people with high CRBs to be more mindful about online risk, which then translates to more control or regulation of online actions, more concern about the negative outcomes from reporting, and a better assessment of their abilities or confidence in dealing with security issues, including reporting spear phishing emails. Hence, this research poses the following hypotheses:

Hypothesis 7. Cyber risk beliefs will have a positive relationship with perceived self-efficacy toward antiphishing behaviors.

Hypothesis 8. Cyber risk beliefs will have a positive relationship with expected negative outcomes from reporting spear phishing emails.

Hypothesis 9. Cyber risk beliefs will have a positive relationship with cyber security self-monitoring.

3. Method

3.1. Data

The research model was tested using a sample of undergraduate college students from a large northeastern university in the U.S. Participants received one hour of research credit for completing the survey. The population of undergraduates is appropriate because college students are one of the most vulnerable populations with regard to phishing attempts (Sheng et al., 2010). Research has shown that college students are specifically targeted by many phishing attacks, and universities spend a significant amount of resources in protecting students from phishing threats (Vishwanath et al., 2016).

3.2. Participants

Four hundred and thirteen students participated in the online survey, which was approved by the Social and Behavioral Sciences Institutional Review Board. After removing incomplete responses, the study comprised of 386 (148 women and 238 men) samples.

3.3. Measures

We first measured the respondents' ability to detect spear phishing emails by using a spear phishing quiz designed by Intel Security (2015). The test presented three spear phishing and three legitimate emails in random order and respondents were asked to identify whether the emails were spear phishing or legitimate.

For testing the model, we measured five key variables that consist of the proposed research model utilizing multiple items: (1) perceived self-efficacy toward antiphishing behaviors; (2) expected negative outcomes from reporting spear phishing emails; (3) cyber security self-monitoring; (4) CRBs; and (5) likelihood of reporting spear phishing emails.

Perceived self-efficacy toward antiphishing behaviors was measured using two subconstructs: perceived self-efficacy toward reporting spear phishing emails and perceived self-efficacy toward cyber security behaviors. Perceived self-efficacy toward reporting spear phishing emails was measured using five items (e.g., I feel confident that I could quickly retrieve accurate contact information of who to report spear phishing emails to) created on the basis of the recommendations of "Phishing.org" (n.d.) on actions that people should take when they receive suspicious phishing emails. Perceived self-efficacy toward cyber security behaviors was measured with four items (e.g., I am very confident of my ability to recognize malware infections) adopted from Amo (2016). Each of the items was assessed on a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*.

Expected negative outcomes from reporting spear phishing emails, defined as concern for mishandling of reports of spear phishing emails, was measured using seven items (e.g., reporting spear phishing emails could result in IT staff ridiculing me if I misreport) using a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*. For this study, the items were developed from findings of previous studies on online knowledge sharing motivations (Ardichvili et al., 2003; Preece et al., 2004; Wendelken et al., 2014).

Cyber security self-monitoring was measured using three items (e.g., I change my password frequently) derived from qualitative studies in the domain of cyber or information security (Furnell, 2008; Furnell et al., 2008; Talib et al., 2010). All responses were scored on a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*.

CRBs was assessed using six items (e.g., I believe the risk of getting infected by spyware, malware, or a virus is a lot less when you open a .pdf [Adobe PDF] file than when you use a .doc [Microsoft word or other Office] type document) retrieved from the study of Vishwanath et al. (2016). All six items were scored on a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*.

Likelihood of reporting spear phishing emails was measured using three items (e.g., I make an effort to find a phone number of University of [Name of University] IT department to report it as a spear phishing email) developed by the researchers of the present study. Respondents were asked to answer the items starting with a vignette question (i.e., when receiving a suspicious email that appears to come from University of [Name of University] asking you to go to a specific web link or respond with your personal details, which of these do you do?). Overall, the items captured behavioral intent, intensity, and effort. Respondents rated the items on a 7-point Likert type scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*.

3.4. Validity and reliability test

Prior to testing the validity and reliability of the five constructs via structural equation modeling (SEM), we examined the statistical assumption of SEM which held that all observed variables should follow a normal distribution using kurtosis and skewness. The assumption of normal distribution is generally met if absolute values of skewness and kurtosis are less than 3 and 10, respectively (Kline, 2011). The results indicated that all observed variables did not deviate from normal distribution, because the skewness and kurtosis indexes did not exceed the standards. Therefore, the statistical assumption of SEM was met.

We assessed the factorial validity and reliability of the five variables that consist of the proposed research model with confirmatory factor analysis (CFA) and Cronbach's alpha using AMOS 20.0 and SPSS 20.0 programs. According to the guidelines suggested by Hu and Bentler (1999), the comparative fit index (CFI), the normed fit index (NFI), the standard root mean square residual (SRMR), and the root mean square error of approximation (RMSEA) were utilized to evaluate the model fit of the proposed model. In general, a good fit is achieved with a high CFI and NFI (greater than 0.95) and a low SRMR and RMSEA (less than 0.05). The internal consistency of the measure is generally considered acceptable if the value of Cronbach's alpha is greater than 0.7 (Kline, 2013).

First, we performed a second-order CFA to confirm the factor structure of perceived self-efficacy toward antiphishing behaviors. One item with correlated error from each of perceived self-efficacy toward reporting spear phishing emails (i.e., I feel confident that I could figure out when to report spear phishing emails) and perceived self-efficacy toward cyber security behaviors (i.e., I am very confident in my ability to identify a secure URL) was dropped. Thus, a total of seven items yielded the two-factor structure with acceptable fit indices of $\chi^2 = 13.48$, $df = 13$, $p = .411$, $\chi^2/df = 1.04$, CFI = 1.00, NFI = 0.99, SRMR = 0.02, and RMSEA = 0.01 (90% CI = 0.00, 0.05). The two subfactors of the perceived self-efficacy toward antiphishing behaviors had a satisfactory level of internal consistency (perceived self-efficacy toward reporting spear phishing emails: Cronbach's alpha = 0.92 and perceived self-efficacy toward cyber security behaviors: Cronbach's alpha = 0.88).

Next, we conducted a first-order CFA for the five latent constructs to confirm the validity of the overall factor structure. Four items from expected negative outcomes from reporting spear phishing emails (i.e., reporting spear phishing emails is useless because IT staff will probably just dismiss my report, rendering my efforts wasted; reporting spear phishing emails will not elicit any response from IT staff; I don't think my reporting will really make a difference; and someone might have already reported a spear phishing email, so I probably don't need to report it) and two items from CRBs (i.e., a lot less on a mobile device [phone or tablet using mobile OS] than on a computer; and a lot less on Facebook/social media messages than traditional emails) were dropped due to highly correlated errors. After dropping the items, the first-order CFA yielded good fit indices of $\chi^2 = 305.16$, $df = 158$, $p < .001$, $\chi^2/df = 1.93$, CFI = 0.97, NFI = 0.94, SRMR = 0.04, and RMSEA = 0.05 (90% CI = 0.04, 0.06). The expected negative outcomes from reporting spear phishing emails (Cronbach's alpha = 0.83), cyber security self-monitoring (Cronbach's alpha = 0.80), CRBs (Cronbach's alpha = 0.85), and the likelihood of reporting spear phishing emails (Cronbach's alpha = 0.96) had a satisfactory level of internal consistency.

4. Results

4.1. Descriptive statistics

The findings from the quiz assessing the ability to detect spear phishing emails indicated the following: 8.8% of respondents identified one email correctly; 24% identified two correctly, 31% identified three correctly, 21% identified four correctly, 12% identified five correctly, and only 1.8% correctly identified all six emails. These results are consistent with Intel's 2015 findings of the test conducted using 19,000 respondents from 144 countries.

Participants' responses to the items regarding intent to report spear phishing emails (measured on a 7-point response scale) suggested that, on average, they had a relatively low likelihood of reporting spear phishing emails ($M = 3.11$, $SD = 1.50$). For the SCT variables, respondents were moderately confident as reflected in their perceived self-efficacy toward antiphishing behaviors ($M = 4.05$, $SD = 1.21$), their perceived self-efficacy toward reporting spear phishing emails ($M = 4.03$, $SD = 1.36$), and their perceived self-efficacy toward cyber security behaviors ($M = 4.08$, $SD = 1.35$). Respondents, however, had slightly lower overall expected negative outcomes from reporting spear phishing emails ($M = 3.46$, $SD = 1.24$) and lower overall cyber security self-monitoring ($M = 3.97$, $SD = 1.32$). Finally, the participants' CRBs ($M = 3.79$, $SD = 1.17$) indicated that they were moderately sensitive to cyber risks.

4.2. Evaluation of the research model

The overall fit of the research model was evaluated using SEM with maximum likelihood (ML) estimation. Goodness of fit was assessed using a combination of six fit indices: chi-square (χ^2), chi-square/degree of freedom (χ^2/df), comparative fit index (CFI), normed fit index (NFI), standard root mean square residual (SRMR), and root-mean-square error of approximation (RMSEA).

The proposed model resulted in a good fit: $\chi^2 = 292.27$, $df = 158$, $p < .001$, $\chi^2/df = 1.85$, CFI = 0.97, NFI = 0.95, SRMR = 0.04, and RMSEA = 0.05. The hypothesized model explained 29% of the total variance in likelihood of reporting spear phishing emails. Table 1 indicates the zero-order correlations among the variables in the proposed research model.

4.3. Hypotheses testing

Fig. 2 indicates the research model with the structural paths and their standardized path coefficients (β).

Hypotheses 1, 2 and 3 suggested that perceived self-efficacy toward antiphishing behaviors would have significantly positive influences on expected negative outcomes from reporting spear phishing emails, cyber security self-monitoring, and the likelihood of reporting spear phishing emails. As shown in Fig. 2, the path coefficients from perceived self-efficacy toward antiphishing behaviors to expected negative outcomes from reporting spear phishing emails ($\beta = 0.21$, $p < .001$), from perceived self-efficacy toward antiphishing behaviors to cyber security self-monitoring ($\beta = 0.44$, $p < .001$), and from perceived self-efficacy toward antiphishing behaviors to likelihood of reporting spear phishing emails ($\beta = 0.14$, $p < .05$) were statistically significant. Thus, the data supported Hypotheses 1, 2, and 3.

Hypotheses 4 and 5 posited positive influences of expected negative outcomes from reporting spear phishing emails on cyber security self-monitoring and likelihood of reporting spear phishing emails. The path coefficient from expected negative outcomes from reporting spear phishing emails to cyber security self-monitoring was significant ($\beta = 0.18$, $p < .01$). The path coefficient from expected negative outcomes from reporting spear phishing emails to likelihood of reporting spear phishing emails was also significant ($\beta = 0.30$, $p < .001$). Therefore, Hypotheses 4 and 5 were also supported by the data.

Hypothesis 6 suggested that cyber security self-monitoring would positively influence likelihood of reporting spear phishing emails. The path coefficient from cyber security self-monitoring to likelihood of reporting spear phishing emails was significantly positive ($\beta = 0.25$, $p < .001$), thereby indicating that Hypothesis 6 is also supported.

Hypotheses 7, 8, and 9 predicted that CRBs would have significantly positive influences on perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring. The path coefficients from CRBs to perceived self-efficacy toward antiphishing behaviors ($\beta = 0.16$, $p < .05$) and from CRBs to expected negative outcomes from reporting spear phishing emails ($\beta = 0.46$, $p < .001$) were significant. The path coefficient from CRBs to cyber security self-monitoring was also marginally significant ($\beta = 0.12$, $p < .10$). Hence, Hypotheses 7, 8, and 9 were also supported by the data.

Table 1
Zero-order correlations among the variables in the proposed research model.

	1	2	3	4	5	6
1. Perceived self-efficacy toward reporting spear phishing emails	1.00					
2. Perceived self-efficacy toward cyber security behaviors	0.59**	1.00				
3. Expected negative outcomes from reporting spear phishing emails	0.19**	0.22**	1.00			
4. Cyber security self-monitoring	0.35**	0.36**	0.32**	1.00		
5. Cyber risk beliefs	0.13**	0.08	0.40**	0.20**	1.00	
6. Likelihood of reporting spear phishing emails	0.27**	0.26**	0.37**	0.39**	0.28**	1.00

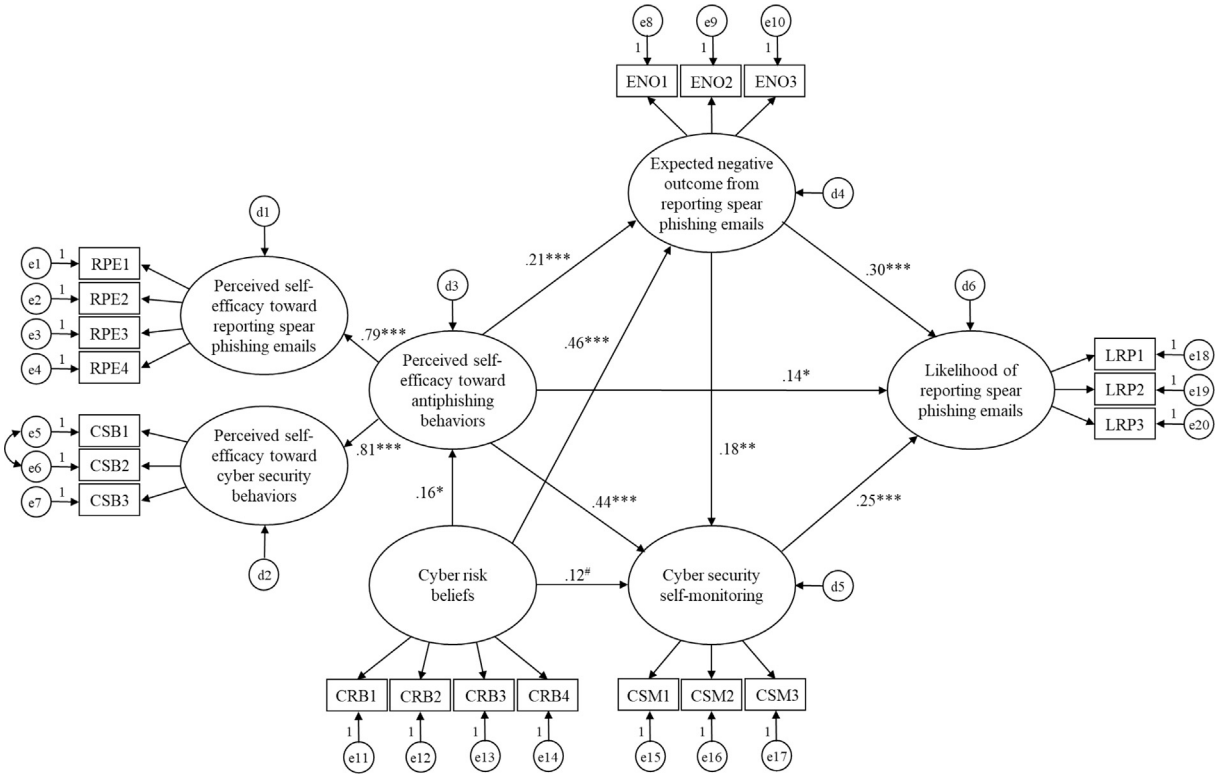


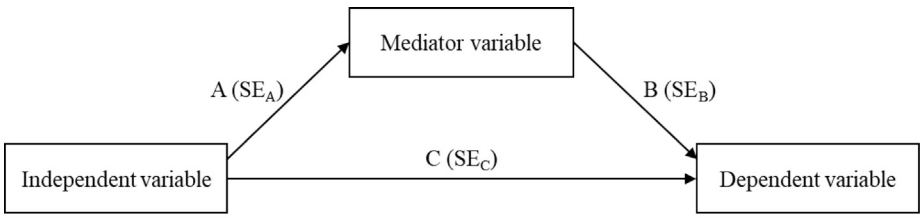
Fig. 2. Final structural model. Note. All the coefficients are standardized coefficients. $^{\#}p < .10$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

4.4. Supplemental analyses

We did not explicitly suggest mediating roles of perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring on the relationship between CRBs and likelihood of reporting spear phishing emails. However, it appears worthwhile to test whether perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring are able to mediate the influence of CRBs on the likelihood of reporting spear phishing emails in an attempt to better understand the relationships among those variables. Moreover, it likewise seems meaningful to examine whether the influence of perceived self-efficacy toward antiphishing behaviors on the likelihood of reporting spear phishing emails would be mediated by the expected negative outcomes from reporting spear phishing emails and cyber security self-monitoring.

To determine the possibility of mediation, we conducted Sobel tests (1982) using the parameter estimates and standard errors of the independent variable to the mediator variable (A and SE_A) and the mediator variable to the dependent variable (B and SE_B) to calculate the significance of the mediating effect of the independent variable on the dependent variable through the mediator variable (see Fig. 3). A significant Sobel test statistic (z-value) indicates support for mediation.

The findings indicated that the influence of CRBs on the likelihood of reporting spear phishing emails was mediated through perceived self-efficacy toward antiphishing behaviors ($z = 2.07$, $p < .05$), expected negative outcomes from reporting spear phishing emails ($z = 4.32$, $p < .001$), and cyber security self-monitoring ($z = 3.60$, $p < .001$). In addition, the results showed that expected negative outcomes from reporting spear phishing emails ($z = 3.37$, $p < .001$) and cyber security self-monitoring ($z = 4.04$,



$$z\text{-value} = A*B / SQRT(B^2*SE_A^2 + A^2*SE_B^2)$$

Fig. 3. Sobel test formula.

$p < .001$) mediated the influence of perceived self-efficacy toward antiphishing behaviors on likelihood of reporting spear phishing emails.

5. Discussion

Using SCT's motivational mechanisms as its foundation, the study empirically tested a research model explaining why people do not report spear phishing emails to IT help desks. Drawing from current research, the model also incorporated CRBs, a construct shown to influence cognitive processing, in the SCT framework.

The overall results confirmed the triadic reciprocal determinism of SCT in explaining why users do not report phishing emails. The likelihood of reporting spear phishing emails was determined by perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring. CRBs also played an important role. The CRBs of users directly influenced perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring. Moreover, CRBs indirectly affected the likelihood of reporting spear phishing emails through the three internal motivators of SCT (i.e., perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring). Prior research has correlated SCT-derived factors such as self-efficacy (Vishwanath et al., 2011; Wang et al., 2012) and self-monitoring (Rhee et al., 2009) to the cyber security-related actions of users, and another stream of research has connected CRBs to spear phishing deception likelihood (Vishwanath et al., 2016). The current research is the first to incorporate CRBs into the explanatory framework of SCT. In doing so, the findings both expand SCT and directly contribute to the science of security.

These findings also have important implications for practice. The research found that the self-efficacy of users toward performing antiphishing behaviors directly and indirectly influenced reporting. The latter was through influencing the negative outcome expectations and increasing self-regulation. This suggests that users with high self-efficacy are more concerned about the negative outcomes from reporting spear phishing emails. This could stem from the fact that many spear phishing emails are difficult to discern from legitimate emails, which someone with higher self-efficacy and high self-regulation likely realizes. This is an important finding because most antiphishing training focuses on improving self-efficacy rather than on improving communication between the user who is reporting and the portal collecting such reports. Our results suggest the need for better communication aimed at reducing the dissonance in the minds of individuals who might consider reporting a suspected spear phishing email. Such communication could over time enhance reporting rates.

Second, the research found that individuals with high cyber security self-monitoring consistently showed a higher likelihood of reporting spear phishing emails. Self-regulation involves effortful and continuous vigilance, which is difficult to maintain in the long run. However, self-regulation can be improved using technological aids. In fact, fitness monitors built into watches and apps in smartphones do just that in terms of improving how people pay attention to their daily activity levels and overall health. The same can be applied for cyber security and spear phishing reporting. By developing portals and apps that allow for frequent and quick reporting, coupled with an enjoyable game-based reward system, the self-monitoring of users can be improved. Increased self-monitoring could enhance cognitive involvement, which could, over time, improve not just reporting but also the accuracy of spear phishing email detection. Besides, increased self-monitoring could reduce the impact of habituation, where users mindlessly click on spear phishing hyperlinks and attachments, which prior research has shown to increase spear phishing victimization (Vishwanath, 2015). By enhancing self-monitoring through the implementation of the aforementioned approaches, the action loops of users and their thoughtless reactions could be short-circuited, and the impact of email habits could likely be attenuated.

Finally, the research found that CRBs plays an important role in reporting. The CRBs of users directly influenced the three socio-cognitive constructs of SCT: perceived self-efficacy toward antiphishing behaviors, expected negative outcomes from reporting spear phishing emails, and cyber security self-monitoring. Hence, CRBs had a direct impact on users' behavioral motivations. Furthermore, prior research has also found higher CRBs motivating higher systematic processing and thereby enhancing phishing deception-detection (Vishwanath et al., 2016). By combining these two streams it can be concluded that CRBs not only influence the amount of cognitive effort users are willing to exert, but by influencing self-regulation, outcome expectations, and perceptions of ability or self-efficacy, they also influence the degree of mindfulness with which they engage in reporting behavior.

Mindfulness is a close analog to metacognition (Hussain, 2015), and is defined as a person's awareness of cognitive processes, such as understanding one's capabilities to perform a task, or of cognitive regulatory processes like planning, monitoring, and evaluating one's performance (Flavell, 1992). Better metacognition leads to better strategies while dealing with problematic situations; this results in successful accomplishment of tasks required to solve the problem. The findings of the current study suggest CRBs activate different types of metacognitive activities, including self-efficacy and self-regulation, that ultimately lead to the optimal enactment of appropriate behaviors. The present results thus call for policy makers and training programs to focus not just on improving users' knowledge about spear phishing but also on their beliefs about online risk and work on interventions that improve risk perceptions and assessments. The results suggest that such interventions would have a positive impact on the extent of effort or involvement in examining spear phishing emails as well as an individual's decision to report it.

The current study shares similar limitations with other empirical model testing studies. This included a student sample, used for both convenience and internal validity necessary for model testing. The use of students also restricted the research from examining the effect of intra-organizational processes such as the existing security culture, impact of leadership initiatives, and social norms that might influence reporting. Furthermore, the results, although extensible to only student populations, are still pertinent; students are increasingly the targets of spear phishing attacks. The research is also limited by the measures available for individual constructs. While measures for CRBs and cyber security self-efficacy were readily available, measures for self-efficacy toward reporting spear

phishing emails, expected negative outcomes from reporting spear phishing emails, cyber security self-monitoring, and the likelihood of reporting spear phishing emails were created for the study. Although their reliability and construct validity were statistically established, future research on the matter is needed to establish adequacy. Moreover, future research is necessary for establishing the robustness of the explanatory model and for testing its validity in reporting different types of attacks (e.g., phone based scams, social media scams, and non-cybercrimes). This can be achieved using a range of different populations, from employees in organizations to students and senior citizens in different parts of the world, all of whom are routinely targeted by spear phishing attacks and could benefit from reporting and its concomitant benefits. Finally, the focus herein was solely on reporting; whether the user had fallen victim to spear phishing tests or attacks was, unfortunately, ignored. How such an outcome could impact the user, perhaps by causing fear, shame or other maladaptive reactions, or maybe causing even more heightened awareness and increased reporting, was not examined and needs to be studied further.

All said, the overall findings of the research are noteworthy. The research model explains the motivational factors that inhibit the reporting of spear phishing and in doing so contributes to the science of security. It appears that the reporting is inhibited by internal factors such as self-efficacy and the users' fear of reporting emails that might not be spear phishing emails; these are driven by users' self-regulation, which serves to calibrate expectations and influence behavior. Finally, the research also points to the role of users' CRBs, which serves as a scope condition, motivating the internal expectations, assessments, and regulatory process that ultimately lead an individual to report spear phishing emails.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Amo, L., 2016. Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. IEEE Secur. Priv. 14 (1), 72–75. https://doi.org/10.1109/MSP.2016.12.

Ardichvili, A., Page, V., Wentling, T., 2003. Motivation and barriers to participation in virtual knowledge-sharing communities of practice. J. Knowledge Manage. 7 (1), 64–77. https://doi.org/10.1108/13673270310463626.

Bandura, A., 1986. Social foundations of thought and action: A social cognitive theory. Prentice-Hall, Englewood Cliffs, NJ.

Bandura, A., 1989. Human agency in social cognitive theory. Am. Psychol. 44 (9), 1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175.

Bandura, A., 1997. Self-efficacy: The exercise of control. W H Freeman/Times Books/Henry Holt & Co, New York, NY.

Bandura, A., 1998. Health promotion from the perspective of social cognitive theory. Psychology and Health. 13 (4), 623–649. https://doi.org/10.1080/08870449808407422.

Bandura, A., 2006. Guide for constructing self-efficacy scales. In: F. Pajares & T. Urdan (Eds.), Self-efficacy beliefs of adolescents (Vol. 5, pp. 307-337). Information Age Publishing, Greenwich, CT.

Bandura, A., Cervone, D., 1983. Self-evaluative and self-efficacy mechanisms governing the motivational effects of goal systems. J. Prsonality Soc. Psychol. 45 (5), 1017–1028. https://doi.org/10.1037/0022-3514.45.5.1017.

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., 2016. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. arXiv preprint arXiv:1606.00887.

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

CSO, May 3, 2019. Why business don't report cybercrimes to law enforcement. Retrieved from https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

Dijkstra, A., Buunk, A.P., 2008. Self-evaluative emotions and expectations about self-evaluative emotions in health-behaviour change. Br. J. Soc. Psychol. 47 (1), 119–137. https://doi.org/10.1348/014466607X216133.

Dijkstra, A., Vries, H.D., Kok, G., Rouackers, J., 1999. Self-evaluation and motivation to change: Social cognitive constructs in smoking cessation. Psychology and Health. 14 (4), 747–759. https://doi.org/10.1080/08870449908410762.

Flavell, J.H., 1992. Cognitive development: Past, present, and future. Dev. Psychol. 28 (6), 998–1005. https://doi.org/10.1037/0012-1649.28.6.998.

Furnell, S., 2008. 2008, End-user security culture: A lesson that will never be learnt? Comput. Fraud Secur. 4, 6–9. https://doi.org/10.1016/S1361-3723(08)70064-2.

Furnell, S., Tsaganidi, V., Phippen, A., 2008. Security beliefs and barriers for novice Internet users. Comput. Secur. 27 (7), 235–240. https://doi.org/10.1016/j.cose.2008.01.001.

Halevi, T., Memon, N., Nov, O., 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. (January 2, 2015). https://doi.org/10.2139/ssrn.2544742.

Hu, L.T., Bentler, P.M., 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Struct. Equation Model.: A Multidiscip. J. 6 (1), 1–55. https://doi.org/10.1080/10705519909540118.

Hussain, D., 2015. Meta-cognition in mindfulness: a conceptual analysis. Psychol. Thought. 8 (2), 132–141. https://doi.org/10.5964/psyct.v8i2.139.

Intel Security, May 12, 2015. 97% of people globally unable to correctly identify phishing emails. Retrieved from https://www.mcafee.com/us/about/news/2015/q2/20150512-01.aspx.

Kline, P., 2013. Handbook of psychological testing. Routledge, London.

Kline, R.B., 2011. Principles and practice of structural equation modeling. The Guilford Press, New York, NY.

KnowBe4, n.d.. Retrieved from https://www.knowbe4.com/spear-phising/.

Krol, K., Moroz, M., Sasse, M.A., 2012. Don't work. Can't work? Why it's time to rethink security warnings. In 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS). IEEE. https://doi.org/10.1109/CRSIS.2012.6378951.

LaRose, R., Lin, C.A., Eastin, M.S., 2003. Unregulated Internet usage: addiction, habit, or deficient self-regulation? Media Psychol. 5 (3), 225–253. https://doi.org/10.1207/S1532785XMEP0503_01.

Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19 (5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9.

Pishing.org, n.d.. How to report phishing. Retrieve from http://www.phishing.org/how-to-report-phishing.

Ponemon Institute, 2015. The cost of phishing & value of employee Training. Retrieved from https://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf.

Preece, J., Nonnecke, B., Andrews, D., 2004. The top five reasons for lurking: Improving community experiences for everyone. Comput. Hum. Behav. 20 (2), 201–223. https://doi.org/10.1016/j.chb.2003.10.015.

Rhee, H.S., Kim, C., Ryu, Y.U., 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comput. Secur.. 28 (8),

816–826. https://doi.org/10.1016/j.cose.2009.05.008.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In proceedings of the SIGCHI conference on human factors in computing sytems (pp. 373-382). ACM.
Siponen, M., Mahmood, M.A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manage. 51 (2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.
Sobel, M.E., 1982. Asymptotic confidence intervals for indirect effect in structurcal equation models. Sociol. Methodol. 13, 290–312. https://doi.org/10.2307/270723.
Talib, S., Clarke, N.L., Furnell, S.M., 2010. An analysis of information security awareness within home and work environments. In 2010 International Conference on Availability, Reliability, and Security (pp. 196-203). IEEE. https://doi.org/10.1109/ARES.2010.27.
Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a protection motivation theory perspective. Comput. Secur. 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009.
United States Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services (NCATS), 2018. Phishing Campaign Assessment Summary. Retrieved from https://www.us-cert.gov/sites/default/files/resources/ncats/PCA%20Sample%20Report_508-Compliant.pdf.
Vishwanath, A., 2015. Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. J. Comput.-Mediated Commun. 20 (5), 570–584. https://doi.org/10.1111/jcc4.12126.
Vishwanath, A., November 8, 2016b. “Spear-phishing” roiled the presidential campaign—here’s how to protect yourself. The Conversation. Retrieved from http://theconversation.com/spearphishing-roiled-the-presidential-campaign-heres-how-to-protect-yourself-68274.
Vishwanath, A., 2016a. Spear phishing: The tip of the spear used by cyber terrorists. In: Combating Violent Extremism and Radicalisation in the Digital Era. IGI Global, pp. 469–484.
Vishwanath, A., Harrison, B., Ng, Y.J., 2016. Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. 45 (8), 1146–1166. https://doi.org/10.1177/0093650215627483.
Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H.R., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis. Support Syst. 51 (3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002.
Vishwanath, A., Kwak, Y.S., Harrison, B., 2017. The critical role of cyber risk beliefs (CRB) in determining why people fall victim to spear phishing. The International Communication Association's Annual Conference. San Diego, California.
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 Trans. Prof. Commun. 55 (4), 345–362. https://doi.org/10.1109/TPC.2012.2208392.
Wang, J., Li, Y., Rao, H.R., 2017. Coping responses in phishing detection: an investigation of antecedents and consequences. Inf. Syst. Res. 28 (2), 378–396. https://doi.org/10.1287/isre.2016.0680.
Wendelken, A., Danzinger, F., Rau, C., Moeslein, K.M., 2014. Innovation without me: why employees do (not) participate in organizational innovation communities. R & D. Management. 44 (2), 217–236. https://doi.org/10.1111/radm.12042.
Williams, E.J., Beardmore, A., Joinson, A.N., 2017. Individual differences in susceptibility to online influence: a theoretical review. Comput. Hum. Behav. 72, 412–421. https://doi.org/10.1016/j.chb.2017.03.002.
Williams, E.J., Hinds, J., Joinson, A.N., 2018. Exploring susceptibility to phishing in the workplace. Int. J. Hum Comput Stud. 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004.
Vade Secure, 2018. What’s the difference between phishing and spear phishing?. Retrieved from https://www.vadesecure.com/en/whats-the-difference-between-phishing-and-spear-phishing.
Verizon, 2019. 2019 data breach investigations report.