6-2-2023

Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies

Loretta Stalans
Loyola University Chicago

Eric Chan-Tin
Loyola University Chicago, dchantin@luc.edu

Anna Hart
Loyola University Chicago, ahart2@luc.edu

Madeline Moran
Loyola University Chicago, mmoran11@luc.edu

Shelia Kennison
Oklahoma State University

Recommended Citation

Loretta Stalans, Eric Chan-Tin, Anna Hart, Madeline Moran & Shelia Kennison (2023) Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies, Victims & Offenders, 18:7, 1216-1235, DOI: 10.1080/15564886.2023.2218369

Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uvao20

Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies

Loretta Stalans, Eric Chan-Tin, Anna Hart, Madeline Moran & Shelia Kennison

To cite this article: Loretta Stalans, Eric Chan-Tin, Anna Hart, Madeline Moran & Shelia Kennison (2023) Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies, Victims & Offenders, 18:7, 1216-1235, DOI: 10.1080/15564886.2023.2218369

To link to this article: https://doi.org/10.1080/15564886.2023.2218369

Published online: 02 Jun 2023.

VICTIMS & OFFENDERS
2023, VOL. 18, NO. 7, 1216–1235
https://doi.org/10.1080/15564886.2023.2218369

OPEN ACCESS

Predicting Phishing Victimization: Comparing Prior Victimization, Cognitive, and Emotional Styles, and Vulnerable or Protective E-mail Strategies

Loretta Stalans[a,b], Eric Chan-Tin[c], Anna Hart[a], Madeline Moran[c], and Shelia Kennison[d]

[a]Department of Psychology, Criminal Justice and Criminology, Loyola University Chicago, Chicago, Illinois, USA; [b]Department of Criminal Justice and Criminology, Loyola University Chicago, Chicago, Illinois, USA; [c]Department of Computer Science, Loyola University Chicago, Chicago, Illinois, USA; [d]Department of Psychology, Oklahoma State University, Stillwater, Oklahoma, USA

ABSTRACT
Phishing victimization is prevalent and results in theft of personal identifiable information (PII) or installing malware to steal PII. Drawing upon social psychological and criminological theories, we conducted a prospective study to assess three groups of predictors to being phished or not: a) prior victimization; b) protective or vulnerable habitual strategies, and c) emotional and cognitive decision-making styles. Students ($N = 236$) completed a survey assessing these predictors and then about 4 weeks later received a phishing e-mail using the university's phishing testing system. The e-mail requested that they click on a link and enter their student ID to avoid having their account blocked. About half (50.8%) clicked on the link, and 81.6% of those phished entered their PII. Individuals who had low avoidant style and high generalized anxiety were four times more likely to be phished, after controlling for the significant effects of vulnerable habitual strategies and using dating apps. Machine learning analyses also found cognitive styles and generalized anxiety are the better predictors of getting phished compared to vulnerable and protective strategies and prior victimization. These findings suggest that cybersecurity training needs to be expanded to address the emotional and cognitive processing of deceptive appeals in e-mails.

KEYWORDS
Phishing; Lifestyle-Routine Activities Theory; Victimization

Phishing and its variants were the most frequently reported cybervictimization in the United States (FBI, 2023). Phishers steal personal identifiable information (PII) through sending deceptive e-mails that urge recipients to immediately address a fake issue, such as being permanently locked out of their account, through clicking on a link to enter PII. Victims unknowingly enter PII on a counterfeit website or click links or attachments that install malware. This victimization leads to substantial loss of productivity hours to the organization and additional victimization such as identity theft, hacking, or ransomware (Ponemon, 2021). To decrease costs from victimization, organizations often mandate employees to participate in cybersecurity training.

CONTACT Loretta Stalans lstalan@luc.edu Department of Psychology, Criminal Justice and Criminology, Loyola University Chicago, 1032 W. Sheridan Road, Chicago, IL 60660, USA

Training aims to enhance cybersecurity awareness and teach rules such as "delete unknown e-mails" to reduce risk of phishing victimization. The current study provides a more expansive test of lifestyle antecedents that contribute to the risk of being phished using a prospective design and actual behavioral responses to phishing e-mails. Using Lifestyle Theory (Hindelang et al., 1978) with an embedded dual-processing theory from social psychology, we examine three categories of individual antecedents: a) stable personal traits of generalized anxiety and cognitive decision-making styles; b) protective and vulnerable rule-based habitual strategies to interact with e-mail messages; and c) prior victimizations from identity theft or related cybercrimes.

Integrative theoretical framework

Lifestyle Theory (Hindelang et al., 1978) is often connected to Routine Activity Theory (RAT) (i.e., Cohen & Felson, 1979) as both theories posit three key situational features to determine the risk of victimization: motivated offenders, suitable targets, and lack of capable guardians. There are some key differences. RAT proposed that all three of these features must converge in time and space for opportunities for victimization to arise and was originally a macro-level theory to describe how crime rates vary across geographical areas (Pratt & Taranovic, 2016). Conversely, Lifestyle Theory explains victimization at the individual level, does not require all three elements to be present for an increased risk of victimization and focuses on how routine activities such as lifestyle choices may account for higher risk of victimization. Moreover, Lifestyle Theory recognizes that victimization risk is probabilistic and changes across situations and within persons across time, whereas RAT describes whether a victimization occurred or not (Pratt & Taranovic, 2016).

Suitable targets

Phishers are motivated offenders who conduct targeted spear-phishing where they pretend to be a higher-level supervisor in phishing e-mails sent to employees or do bulk emailing hoping to find suitable targets. Spear-phishing is a targeted attack and has grown in recent years (Ghazi-Tehrani & Pontell, 2021). Phishers may target organizations where e-mail lists of employees are readily accessible, and only target-specific individuals in spear phishing (Miro-Llinares et al., 2020). The integrated Lifestyle-RAT (L-RAT) theory argues that suitable targets have value, inertia, visibility, and accessibility. Organizations with weakened cybersecurity controls such as inadequate spam filters or visible e-mail directories are more suitable targets as increased accessibility allows phishing e-mails to reach more employees.

Target visibility has been measured through online activities such as the amount of time spent in cyberspace and on specific activities such as shopping, banking, and social media. Measures of the amount of time on specific activities are inconsistent predictor of cybercrime victimization and vary across samples as well as measures (see Miro-Llinares et al., 2020; Ngo et al., 2020). Some research finds that specific activities such as downloading and shopping are related to several different victimizations including malware attacks, fraud, and identity theft (Leukfeldt & Yar, 2016; Pratt et al., 2010; Reyns, 2013, 2015; Van Wilsem, 2013), whereas other researchers find no relationship (Leukfeldt, 2014; Ngo & Paternoster, 2011; Reyns, 2013; Reyns & Henson, 2016). Suggestions to reduce online shopping and other activities are likely to be met with resistance and would have collateral economic consequences. It is imperative to understand what makes these activities riskier for some individuals than for others (e.g., Pratt & Taranovic, 2016).

Which individuals are more capable guardians?

Social psychology research and theory provide a bridge to understanding how variations in cognitive and emotional styles, cybersecurity knowledge, and dispositional traits contribute to variation in the riskiness of routine activities in cyberspace. These variations in knowledge and styles of decision-making will make some individuals less capable guardians of organizations' networks and PII. People often have time pressure and cognitive overload and reserve their cognitive effort for difficult tasks. Reading and responding to e-mails typically is not considered a challenging task. According to dual-processing theories, people generally have two ways to select and interpret information: Type 1 (heuristic) approach and Type 2 (systematic) approach (Stanovich & Toplak, 2012). In the Type 1 approach, specific cognitive or emotional heuristics, which are short-cuts stored in memory, are used to make quick and automatic decisions based on information in the decision context. The Type 2 approach uses more cognitive effort and is slower with more careful consideration of the information and options. Individuals must make a deliberate choice to slow down the decision-making process. Type 2 processing overrides the more automatic Type 1 processing through interrupting and suppressing the response and through imagining alternative scenarios of outcomes for the possible response options (Stanovich & Toplak, 2012). Type 1 processing draws upon prior knowledge as well as habitual ways of cognitively and emotionally responding to situations such as reading and responding to e-mails.

Variation in risk: cognitive styles

Routine ways of making decisions across time and contexts are called cognitive styles and focus on how people perceive and interpret information to make decisions (Scott & Bruce, 1995; Volkova & Rusalov, 2016). Individuals may have different cognitive styles for different decision tasks. The systematic style involves carefully considering all information and checking for deceptive cues, whereas intuitive style relies more on instinct about the veracity of the message. Individuals also can prefer to make decisions quickly and have a quick style or prefer to delay decisions if possible and have an avoidant style.

A meta-analysis of a pooled sample of 17,704 participants found that a systematic style had small but significant effects on increased decision accuracy and cognitive styles had the strongest effects on decision performance when they matched the decision task (Phillips et al., 2016). Individuals who scored higher on systematic style were less likely to report prior victimization from phishing and malware in a cross-sectional survey (Djulbegovic et al., 2015). In another study, respondents first completed a survey and then were sent three weeks later a phishing e-mail that asked for assistance to increase J. T. Morgan's contribution to a fake international cancer fund through clicking on a link. This study found that a higher systematic style was unrelated to clicking on the link, but those with low avoidant styles compared to high avoidant styles were over four times more likely to click on the link (Chan-Tin et al., 2022). Thus, high avoidant styles served a protective link through delaying the opening and responding to an e-mail; supporting this argument, Lerner et al. (2015) noted that time delay was one way to minimize the contribution of emotions on decisions.

Emotional responding: generalized anxiety

Few studies have examined how emotions are related to victimization risk from phishing e-mails or other online frauds (see for a review Norris & Brookes, 2021; Williams et al., 2017). Persons with less emotionally stable dispositions were more susceptible to phishing or online fraud in two cross-sectional survey studies (Van Weijer & Leukfeldt, 2017; Vishwanath, 2015). Another study found that respondents who scored higher on anxiety about COVID reported a higher likelihood to click the links in the 15 phishing e-mails where they role-played their responses (Abroshan et al., 2021). These prior cross-sectional survey studies have not examined persons' actual responses to phishing e-mails or examined generalized anxiety.

Generalized anxiety is experiencing worry and dread across daily events. Numerous psychological studies have found that people with higher generalized anxiety are more likely to interpret ambiguous messages as threatening and conclude that negative events are more probable (Blanchette & Richards, 2010). Moreover, empirical research has consistently found that anticipatory emotions such as generalized anxiety can create "action tendencies" that are stored in memory and save cognitive energy (Lerner et al., 2015). Additionally, people with higher social anxiety were less successful at detecting deception in a task where they watched videotapes of people who sometimes were lying and sometimes telling the truth (DePaulo & Tang, 1994). Anxiety can create either an approach response to quickly make a decision with the goal of reducing anxiety or an avoidance response through delaying the decision to avoid a potential negative outcome (Beckers & Craske, 2017). Thus, if a phishing e-mail is opened, individuals with higher generalized anxiety will be more likely to interpret the threat appeal as authentic and comply with the request to reduce their anxiety and avoid the negative consequences.

Protective or vulnerable rule-based strategies

Cybersecurity training provides rule-based strategies designed to increase protection against phishing and decrease vulnerability to phishing (Hamilton et al., 2016). Training curriculum such as Anti-Phishing Phil (CMU Usable Privacy and Security Lab (CUPS) and PhishGuru (Kumaraguru et al., 2009) teach trainees to look for cues in the e-mail and URLs to differentiate authentic e-mails from phishing e-mails. Trainees are encouraged to create habits that follow rule-based protective strategies that focus on these cues and omit the use of rule-based vulnerable strategies. For example, rule-based protective strategies include "never click on links from suspicious e-mails", and "check the URL of websites before clicking the link in the e-mail". Research that first sent out phishing e-mails and then asked individuals why they clicked or did not click on the link found that automatic responding to e-mail or trusting the content were the explanations for clicking on the link in the phishing e-mail (Tschakert & Ngamsuriyaroj, 2019; Vishwanath, 2015; Vishwanath et al., 2016). Leukfeldt and Yar (2016) assessed nine vulnerable or protective strategies and found that those who more often used protective strategies also were less likely to report being a victim of internet fraud scams or hacking in the last 12 months, though these strategies were unrelated to victimization from identity theft or malware. In the current study, we controlled whether individuals regularly used dating apps as habitual clicking on profiles may build up a habit of clicking and implicitly trusting the content (Vishwanath, 2015).

Prior victimization

Dual-processing theories suggest that victims might be unaware or misattribute the reason why they were victimized, resulting in limited utility of learning from their victimization. Victims may experience anger and/or anxiety after fraud victimization and these emotions may become associated with specific action tendencies such as avoiding the threat through not responding to unknown e-mails or through having undue confidence in their ability to detect future phishing. These varying responses will cancel out any overall effect.

Self-control theory

Self-control theory asserts that individuals differ in their ability to regulate behavior to delay gratification if the long-term costs exceed the immediate rewards (Gottfredson & Hirschi, 1990). Persons with low self-control prefer immediate short-term gratification rather than working through difficult tasks for greater rewards in the long term, take risks, and express anger when frustrated. Low self-control has been consistently related to committing a wide range of cybercrimes (Stalans & Donner, 2018). Pratt and Taranovic (2016) called for the integration of self-control into L-RAT theory as an individual difference variable and Pratt (2016) provides a thorough theoretical analysis of how self-control increases the likelihood of choosing risky situations, over-reacting to setbacks or confrontations, and is related to neuropsychological deficits (Pratt, 2016). Individuals with low self-control also may make quicker and less rational decisions. In this study, we controlled self-control in our analyses to separate it from the more changeable cognitive styles and generalized anxiety.

Current research

Pratt and Taranovic (2016) noted future research and conceptual development are needed to understand victimization risk. This paper begins to address this gap through examining the emotional and cognitive styles that increase vulnerability to being phished. Phishing is a prevalent and costly form of victimization for individuals and organizations but has received limited attention in criminology (Ghazi-Tehrani & Pontell, 2021). While prior research relies on cross-sectional self-reports of victimization, we assess behavioral responses to phishing e-mails in a prospective design where the lifestyle antecedents are measured in a survey four weeks before respondents received the phishing e-mail. Being phished was defined as clicking on the embedded link and/or entering the requested personal information. Thus, individuals may have "routine" strategies of engaging with e-mails. From the psychology research and lifestyle theory, individuals with more vulnerable than protective strategies, and less systematic cognitive styles would be at a higher risk of being phished if they opened the e-mail. Individuals with higher generalized anxiety will be more likely to treat this anxiety as an action tendency when they have an approach response (i.e., low avoidant cognitive style) and will be more likely to interpret the phishing e-mail as authentic and click on the link. Phishing e-mails might not be opened for a variety of reasons including being buried in an inbox; thus, it is critical to assess whether the e-mail was opened, which is assessed through an embedded image in the e-mail. Those with higher avoidant styles might be less likely to open e-mails.

Methods

Sample

Undergraduate students ($N = 240$) in introductory psychology courses completed a Qualtrics online survey and received one research credit hour in the Spring of 2021; we removed four students from the analyses, as three students did not provide an e-mail address and one student only answered half the survey. The majority were women (75%) and cis-gendered individuals (99.6%). Most participants were first-year students in college (56.7%) with a median age of 19 (standard deviation 2.6). Of the respondents, most identified as Caucasian (47.7%) or Asian/South Asian/Eastern Asian (17.8%), with smaller percentage identifying as Latinx (15.4%), Black (6.6%) or multi-racial (10.8%). The population of undergraduate students at this university consists of 42% from a racial minority group and 68% women. Thus, the sample slightly overrepresents women (75%) and students from a racial minority (52.3%). Most individuals (81.2%) reported receiving phishing e-mails with 39.6% receiving these e-mails often or very often. In addition, 51.7% were victims at least once of hacking or identity theft, and 30.5% were victims of someone faking an identity to obtain information, money, or a relationship. Finally, the average time spent on technology a week was 19 hours with a standard deviation of 20.69. Most students (90.8%) reported checking their e-mail daily with only 7.5% checking it every other day and 1.7% checking it once or twice a week.

Research design and procedures

The research design had two phases. In phase one, respondents completed an online Qualtrics survey, which assessed strategies that either increased or reduced vulnerability to phishing (protective strategies), their cognitive styles, generalized anxiety, self-control, and demographics. Respondents were unaware of the second phase, which occurred after a completed survey was submitted. In the second phase, respondents received a phishing e-mail three weeks after completing the survey. We used the university's Information Technology Department's system that sends out training phishing e-mails to students and employees. The phishing e-mail had the header: "Account Recovery." The e-mail stated: "Your account will be blocked unless you act right away for immediate service. Click here to provide ITS with your student ID and contact information to facilitate fast recovery."

To prevent the phishing e-mail being blocked by our university's spam filters, the information technology department placed the e-mail on an allowed list and allowed it to go to the students' inbox. We assessed whether the students opened the e-mail, clicked on the link, and entered their student ID on the fake website. For this e-mail, the URL was unique for each participant's e-mail. e.g.,*hash*(*example@company.com*) = *MTNhMWY2NDlkMWI1MDMxMmNkMDQzMzkZTBlOGI3NjU=* in base64 encoding. The hash algorithm is a one-way function. Moreover, the phishing e-mail includes a tracking 1 × 1 remote image so we could see if participants opened the e-mail, and their e-mail client/browser allows remote image loading. The computer programming allows the collection of the following data: a) whether the participant opened the e-mail; b) whether the participant clicked on the hyperlink; and c) whether the participant entered their information after they clicked on the link and are directed to the website. Any data that participants entered were removed. We only recorded whether they entered data or not (not the actual data). The phishing e-mail is similar to other phishing e-mails the participants might receive; thus, it does not create undue stress beyond that typically experienced.

The study received IRB approval before data collection began; phishing attempts are a widespread practice at most organizations, including universities, and are used to assess who needs additional training. Any anxiety associated with the phishing e-mail is likely not beyond that experienced in everyday life and was reduced through debriefing. To reduce confidentiality breach, we did not collect the PII that was entered into our project's website.

After the study was completed, all participants were debriefed and could request to have their data from the phishing e-mail removed from the study and/or their survey data removed by writing to the PI or Co-PI. None of the participants made this request. As part of the debriefing, participants were asked to complete another short survey on whether they saw the phishing e-mail and why/why-not they clicked on the link. To encourage participation in the debriefing survey, participants could enter a raffle to win one of three $25 amazon gift cards.

Dependent measure

Being phished

From respondents' behavior toward the phishing e-mail, we had a four-category nominal variable: a) not open coded as 0 (21.5%); b) open but not phish coded as 1 (27.8%); c) phished but data not entered coded as 2 (9.3%); and d) phished and entered data coded as 3 (41.4%). From this measurement, a trichotomous measure was used: 0 = not opened (21.5%); 1 = opened but not phished (27.8%); 2 = phished with or without entering PII (50.6%). Whether opened or not was determined through the image contained in the e-mail, which automatically recorded their responses of opening or clicking on the link.

Only 55 of the respondents completed the debriefing survey. Its purpose was to see their explanations for why they were phished. Respondents were asked if they remembered the phishing e-mail after being told about the purpose of the study, and 89.1% ($n = 49$) responded that they did remember the e-mail and 10.9% ($n = 6$) did not remember. Of those who did not remember, four provided their e-mail and we were able to link their debriefing response to their phishing behavior; two did not open the e-mail, one opened it, and one was phished. Recall, of course, has measurement error, and this is why the behavioral response is better than a self-report. The image in the e-mail recorded their behavior so we did not have to rely on self-report. Respondents were asked: "why did they click or not click on the link provided in the e-mail?" We coded the responses into categories. Students had a variety of responses, including seeking advice from friends (14.3%), conducting an extra search to check URL (6.1%), noting that the website looked suspicious (4.1%), looking at the content of the e-mail (18.4%) or e-mail address (18.4%) to judge credibility. The most prevalent one was that the e-mail came from the university's information technology department and appeared genuine (40.8%), suggesting spear phishing e-mails that utilized an authority were often persuasive.

Independent measures

Vulnerable and protective strategies

Respondents indicated how well each of several strategies characterized their behavior in operating a computer using a 1 to 5 scale where 1 = strongly disagree, 3 = unsure, and 5 = strongly agree. Five of these behaviors were vulnerable strategies increasing the risk of phishing victimization and included: frequently clicking on links in unknown e-mails, frequently purchasing items from e-mails, regularly clicking links in e-mails, and replying to e-mail messages to assess their authenticity. Four of these behaviors were protective strategies decreasing the risk of phishing victimization. These protective strategies were checking the URL of the e-mail, deleting unknown e-mails, never sharing confidential documents, and calling the company they do business with if e-mail is suspicious. The total number of protective strategies was subtracted from the vulnerable strategies such that higher numbers indicated a greater number of vulnerable strategies. A trichotomous measure was created with greater number of protective strategies = 0 (19.7%), slightly more protective than vulnerable = 1 (48.1%), and a greater number of vulnerable strategies = 2 (32.2%).

Generalized anxiety scale

A five-item standardized scale for generalized anxiety was used, with respondents asked to read each statement and indicate how they generally feel using "not at all", "somewhat", "moderately so" and "very much so"; in previous research, this scale had high inter-item consistency and strong correlations with the full scales of trait anxiety (Zsido et al., 2020). The scale had a Cronbach Alpha of .82, mean = 2.42, sd = .76. Cronbach alpha provides the consistency of items measuring a concept, and a coefficient of .70 or higher indicates that the items are measuring the same concept. Individuals with a score less than 2.2 were considered low on generalized anxiety (36.7%) and coded as 0 and those with a score greater than 2.2 had higher generalized anxiety (63.3%) and were coded as 1. A score of 2.2 meant that individuals reported on average having moderate or very much anxiety on at least one of the items as 2 was equal to somewhat. Individuals with moderate or very much anxiety are conceptually distinct from those with somewhat or little anxiety.

Decision-making strategies

Scott and Bruce (1995) developed the general decision-making style scale, which assessed systematic, intuitive, and avoidant stable thinking styles. They found both concurrent and construct validity across four large samples; for example, individuals who scored higher on innovativeness also were more likely to have an intuitive thinking style, whereas individuals who had higher internal control were more likely to have a rational thinking style. The scale has been used in a variety of different decision-making settings. Participants rated their agreement on a five-point scale with 1 = strongly disagree; 3 = neither agree nor disagree; 5 = strongly agree.

Systematic style

Systematic style was measured using six items such as "I make decisions in a logical and systematic way," "my decision-making requires careful thought," and "I double check my information sources to be sure I have the right facts before making a decision." The eight items were averaged (Mean = 3.77; Median = 3.83; sd = .66) and had good inter-item reliability (Cronbach alpha = .84). Cronbach alpha provides the consistency of items measuring a concept, and a coefficient of .70 or higher indicates that the items are measuring the same concept. A dichotomous measure was created using a median split with low systematic thinking classified as a score of below 4 (51.2%) and coded as "0", and a score of 4 or 5 classified as high and coded as "1" (48.8%).

Avoidant decision-making

Two items from the Cognitive styles Scale assessed avoidant decision-making: a) "I put off decision-making because thinking about them makes me uneasy", and b) "I postpone decision-making whenever possible." The scale had good reliability (Cronbach Alpha = .81), and a mean of 3.01, Median = 3.0, sd = 1.01). A dichotomous measure was created using a median split with 0 representing low avoidant style and a score less than 3 (58.3%), and 1 equal to high avoidant style and a score of 3 or higher (41.7%).

Self-control scale

A standardized 11-item scale comprised the self-control scale; it has been widely used in the criminology field and has been shown to conform to a one-factor solution for both men and women (Grasmick et al., 1993). Items on the scale assess risk-taking, focusing on short-term compared to long-term consequences, self-interest, preference for simple tasks, and low tolerance for frustration, and had a Cronbach Alpha of .78. Respondents indicated their agreement to each of the 11 items using a five-point scale from 1 = strongly disagree and 5 = strongly agree. Two students were missing one item and their scores were created through averaging the remaining items. The 11 items were averaged (Mean = 2.55; Median = 2.54; sd = .59).

Dating app usage

A dichotomous measure assessed whether individuals regularly used a dating app with 0 equal to not used (76.3%) and 1 equal to used regularly (23.8%). This measure was added as a control for developing an automatic tendency to click on links and assume their veracity (Vishwanath, 2015; Vishwanath et al., 2016).

Analysis strategy

Chi-square analyses examined the bivariate relationships between our independent variables and whether phished or not and whether entered data or not. We then conducted Somer's D symmetrical correlations to assess for multicollinearity among our independent variables as well as provide an empirical test of the relationship between avoidance cognitive style and generalized anxiety found in psychological research. To assess whether these bivariate relationships held after the effects of other independent variables were removed, we conduct two types of multivariate analyses. First, we conducted a multinomial logistic regression using the trichotomous phishing outcome, and having whether opened the e-mail serve as the reference category. This analysis tested for systematic biases between those who opened and did not open the e-mail, including the hypothesis that those with avoidance cognitive style would be less likely to open the e-mail. Second, for those who opened the e-mail, it tested whether the capable guardianship variables explained being phished after controlling for self-control and habitual use of a dating app.

We then conducted a Random Forest Machine Learning analysis to assess which category of capable guardianship variables are the best predictors of being phished for those who opened the e-mail. If there is consistency between the multinomial logistic regression and the Random Forest model, we can have more confidence in the findings, and can assess the relative predictive accuracy of each category of potential independent variables. Moreover, Random Forest Models and logistic regression models were compared in 245 datasets and Random Forest models outperformed logistic regressions in 69% of the datasets (Couronne et al., 2018). Thus, by including both analyses, we examine consistency across the two models and the Random Forest allows for assessments of the strength of relationships for three sets of variables: a) prior victimization; b) cognitive styles and generalized anxiety; and c) protective compared to vulnerable strategies.

Results

Chi-square analyses are presented in Table 1. The second and third columns examine the effect of the independent variables on being phished or not (clicking on the link). A significant interaction between avoidant cognitive style and generalized anxiety is supported. For individuals with a low avoidant cognitive style, a greater percentage were phished if they had high (63%) than low (46.3%) generalized trait anxiety, X^2 (1) = 3.97,

Table 1. Bivariate analyses of anxiety, decision styles, and victimization on being phished and entering personal data on phishing website.

Variables	Not Phished	Phished with or without data entry	Did not enter data	Entered data
Generalized Anxiety				
Low	53.4% (47)	46.6% (41)	60.2% (53)	39.8% (35)
High	47.0% (70)	53.0% (79)	57.7% (86)	42.3% (63)
Avoidant Style				
Low	45.0% (63)^{T}	55.0% (77)	55.0% (77)	45.0% (63)
High	55.7% (54)	44.3% (43)	63.9% (62)	36.1% (35)
Within Low Avoidant Style				
Low Generalized Anxiety	53.7% (36)^{A}	46.3% (31)	59.7% (40)	40.3% (27)
High Generalized Anxiety	37.0% (27)	63.0% (46)	50.7% (37)	49.3% (36)
Within High Avoidant Style				
Low Generalized Anxiety	52.4% (11)	47.6% (10)	61.9% (13)	38.1% (8)
High Generalized Anxiety	56.6% (43)	43.4% (33)	64.5% (49)	35.5% (27)
Overall Vulnerable Strategies				
Mostly protective strategies	69.6% (32)^{B}	30.4% (14)	73.9% (34)^{A}	26.1% (12)
Slightly more vulnerable strategies	42.5% (64)	57.5% (49)	56.6% (64)	43.4% (49)
Mostly vulnerable strategies	46.8% (36)	53.2% (41)	51.9% (40)	48.1% (37)
Hacking or identity theft victimization				
No	43.5% (50)	56.5% (65)	49.6% (57)^{B}	50.4% (58)
Yes	54.9% (67)	45.1% (55)	67.2% (82)	32.8% (40)
Uses a dating app				
No	52.5% (95)	47.5% (86)	62.4% (113)^{A}	37.6% (68)
Yes	39.3% (22)	60.7% (34)	46.4% (26)	54.6% (30)

Note two-tailed *p*-values: $^{B}p < .01$; $^{A}p < .05$ $^{T}p < .10$.

$p < .046$. Generalized anxiety, however, did not predict being phished for those with a high avoidant style. Table 1 also shows a trend where those with a low avoidant cognitive style were more likely to be phished (55%) than those with a high avoidant style (44.3%), X^2 (1) = 2.61, one-tailed $p < .053$. Habitual use of vulnerable strategies compared to protective strategies also significantly increased the likelihood of being phished with only about one-third of mostly protective strategies (30.4%) phished compared to over 50% with slightly more or mostly vulnerable strategies being phished.

The fourth and fifth columns of Table 1 presents the relationships between the independent variables and whether individuals entered or did not enter data on the website. The group of those who did not enter data included those who were not phished. Those with slightly or mostly vulnerable strategies were significantly more likely to enter data than those with only protective strategies. Only one-third of prior victims of identity theft or hacking compared to one half of non-victims entered their personal data, X^2 (1) = 6.02, $p < .049$. Finally, individuals who regularly used dating apps were more likely to enter their personal data (54.6%) than those who never used dating apps (37.6%).

The strongest relationship between the independent variables supported the psychology research and showed that those with higher generalized anxiety were more likely to have an avoidant cognitive style, Somer's D = .33, $p < .001$.Prior victims of identity theft or hacking were more likely to have a high avoidant style (Somer's D = .12, $p < .05$) and to have higher generalized anxiety (Somer's D = .15, $p < .05$). Individuals with lower self-control were more likely to use more vulnerable strategies than protective strategies ($R = .19$, $p < .01$), have higher generalized anxiety ($R = .20$, $p < .01$), to be a victim of identity theft or hacking ($R = .20$, $p < .01$), to have an high avoidant cognitive style ($R = .27$, $p < .01$) and to be less likely to have a systematic style ($R = -.18$, $p < .01$). All other relationships were not significant and close to zero. The significant relationships are small and do not pose multicollinearity issues in the multivariate statistical analyses.

Multinominal logistic regression explaining being phished

Table 2 presents a multinominal regression for a trichotomous measure of being phished with opening the e-mail serving as the reference category. As shown in the second column of Table 2, there were no significant relationships between the independent variables and whether the e-mail was opened or not. There were no selection biases for the measured attributes, including avoidant style was not related to opening the e-mail or not. The model did a very poor job of classifying those who opened (21.5%) or did not open (0%) their e-mail.

The third column of Table 2 compares those who opened the e-mail and were not phished (59%) to those who were phished with or without entering personal data (41%). Compared to those with primarily protective strategies, those with mostly or slightly more vulnerable strategies were three times more likely to be phished. Individuals who had a low avoidant strategy also were four times more likely to be phished if they had high generalized anxiety. Finally, individuals who never used dating apps were less likely to be phished than those who regularly used dating apps. Self-control and systematic cognitive style were not statistically significant.

Table 2. Multinominal regression predicting being phished: avoidance decision style, generalized anxiety, and vulnerable strategies.

Predictors	Did not Open Email compared to Those who Opened WALD SE ODDS Ratio	Phished compared to Those who Opened Email WALD SE ODDS Ratio
High Generalized Anxiety	.38 .40 1.47	.43 .62 1.51
Cognitive styles		
High Systematic Thinking	3.73 .40 2.17	.15 .34 1.14
Low Avoidant Style	.36 .48 .75	.01 .40 .39
Strategies (Reference Category: Protective Strategies)		
Mostly Vulnerable Strategies	.37 .54 1.39	6.05 .49 3.42^{B}
Slightly more Vulnerable Strategies	.18 .50 .81	7.69 .42 3.37^{C}
Did not use dating app	2.05 .52 .48	4.41 .45 $.39^{A}$
Low self-control	2.45 .37 1.78	.20.31 1.15
Identity Theft/Hacking Victim	.16 .41 1.17	2.99 .34 1.80
Interaction between Low Avoidant Style and Anxiety		
High Generalized Anxiety	1.78 .55 2.17	5.14 .44 2.73^{A}
Intercept	1.74 1.20	.338 .707
−2 Log Likelihood Final	427.24^{C}	
Nagelkerke R-square	.179	
Accurately Classified Not Opened	11.8% (6/51)	
Accurately Classified Opened and Not Phished	32.3% (21/65)	
Accurately Classified Opened and Phished	89.2% (107/120)	
% of those Phished Accurately Predicted: Precision	78.1% (107/186)	

Note one-tailed p-values: $^{C}p < .005$; $^{B}p < .01$; $^{A}p < .05$.

Machine learning to predict phishing using different models

Which set of capable guardianship variables are more strongly related to being phished or not? Based on bridging social psychology with the L-RAT theory, we compared three models: 1) vulnerable and protective strategies; 2) decision-making strategies and generalized anxiety; and 3) prior victimization. The classification algorithm used was Random Forest. We compared it with other popular classification algorithms and found that Random Forest provided the best accuracy. We did a 10-fold cross-validation where a random 90% of the dataset was used for training and the remaining 10% of the dataset was used for testing – this was repeated 10 times.[1] The outcome variable was being phished (clicking on the link with or without entering PII on the website) or not being phished for the total sample and for the sample where we knew they opened the e-mail.

To assess the strength of these sets of variables, sensitivity/recall, specificity, precision, and F1-score are more reliable information about the accuracy of machine learning prediction than is classification accuracy (Lu et al., 2022); these metrics are explained below and in Table 3. None of these measures, however, provide the improvement in classification accuracy beyond chance. Classification accuracy, which is the primary strength indicator in multinomial logistic regression, is an incomplete and unreliable measure of model performance, as it does not indicate improvement beyond chance performance and hides the possible imbalance in accuracy of classified those who are phished and not phished (Yarnold & Soltysik, 2016). For this, we used the Effect Strength of Sensitivity (ESS) as this measure indicates the percentage of improvement in classification accuracy achieved with a predictor

Table 3. Machine learning models predicting who was phished or not for total sample and only those who opened the phishing e-mail.

	Sensitivity/Recall	Specificity	Precision	ESS	F1-Score
Total Sample					
Vulnerable and Protective (V&P) Strategies	56.90%	51.85%	55.93%	8.18%	56.41%
Cognitive styles (DS) and Anxiety	**61.21%**	**54.63%**	**59.17%**	**15.60%**	**60.17%**
Prior Victimization	45.55%	39.81%	45.38%	−14.6%	45.46%
All Features	**61.21%**	51.85%	57.72%	13.50%	59.41%
Only Those Who Opened the Phishing Email					
V&P Strategies	84.61%	17.46%	65.56%	2.07%	73.88%
DS and Anxiety	82.10%	**36.51%**	**70.59%**	**18.61%**	**75.92%**
Prior Victimization	77.78%	19.05%	64.08%	−3.17%	70.27%
V&P Strategies and DS and Anxiety	85.3%	20.63%	66.67%	6.10%	74.9%
All Features	**88.89%**	20.63%	67.53%	9.52%	**76.75%**

Sensitivity or Recall = Number of true positive (TP)/(Number of TP + Number of False Negatives (FN)); Specificity = Number of TN/(Number of TN + Number of FP); Precision = Number of TP/(Number of TP + Number of FP); The Effect Strength of Sensitivity (ESS) as this measure indicates the percentage of improvement in classification accuracy achieved with a predictor or model beyond the classification accuracy achieved through chance alone.

F1-Score = 2 * ((Precision * Recall)/(Precision + Recall)).

Bolded are the highest numbers in each column.

or model beyond the classification accuracy achieved through chance alone. ESS can range between −100 and 100; below zero indicates that the model performed worse than chance, 0 indicates no improvement in classification accuracy versus chance, and 100 indicates errorless classification or perfect accuracy beyond chance levels. Thus, ESS is normed relative to chance classification (Yarnold & Soltysik, 2016).[2]

Table 3 shows the result of the three separate models, including the formulas for strength metrics in the note of the table and an explanation in the endnote.[3] The top half of the table is for the entire sample ($N = 236$) while the bottom half of the table is for only those who opened the e-mail ($N = 180$). The results are similar for both samples, where the prior victimization model does worse in all metrics, followed by the vulnerable and protective strategies. Indeed, the model containing only prior victimization performs worse than chance level as shown by the negative ESS values. The cognitive styles and anxiety model did the best with a sensitivity/recall, identifying those who were actually phished, of 61.21% for the entire sample and 82.10% for the sample including only those who opened the e-mail, specificity, classification accuracy of those who were not phished, of 54.63% and 36.51%, precision, when the model predicts that a person is phished it is correct 59.17% for the entire sample and 70.59% for the sample that opened the e-mail, and F1-score, the harmonic mean of precision and recall, of 60.17% and 75.92% respectively.

For the sample including only participants who opened the e-mail, the vulnerable and protective strategies model had slightly higher sensitivity/recall, identifying those who were phished, than the cognitive styles and anxiety model (84.61% vs 82.10%). However, the precision and specificity are much lower. Specificity is important because it means that victims of phishing attacks were classified as successfully ignoring the phishers' requests; these misclassified cases will not be flagged for additional cybersecurity training, which means they are likely to fall victim again. The current study assessed the predictors via a survey four weeks prior to sending out the phishing e-mail.

When all features were used as predictors, the model with cognitive styles and generalized anxiety had slightly higher ESS for the total sample (15.60% vs. 13.50%), and two times higher ESS for the sample where there was confirmation that the phishing e-mail was opened (18.61% vs 9.52%). Thus, including the predictors of prior victimization and vulnerable or protective strategies, produced a slightly lower ESS and a substantially lower ESS for those who were known to have interacted with the e-mail. Examining the ESS for each predictor using Optimal Data Analysis (Yarnold & Soltysik, 2016), the ESS for the measure comparing those with generalized anxiety and low avoidance styles to all others is 19.91% for those who opened the e-mail, two-tailed Monte Carlo $p < .007$. This finding underscores the importance in addressing generalized anxiety and low avoidance styles to reduce phishing in this subgroup.

Discussion

Our study extends conceptually the antecedents that underlie victimization risk of phishing through integrating a dual processing model of social psychology with the Lifestyle-Routine Activities theory (L-RAT). Psychological studies in other domains have found that emotions and cognitive styles contribute to people's decisions and behaviors (Blanchette & Richards, 2010; Lerner et al., 2015; Phillips et al., 2016), but these concepts have received negligible attention as explanatory concepts for cybercrime victimization such as phishing. Criminology studies have focused primarily on assessing target visibility through measuring the time spent on routine activities in cyberspace and on assessing capable guardianship through focusing on measures of habitual vulnerable and protective strategies (e.g., Leukfeldt & Yar, 2016; Reyns, 2015; Van Wilsem, 2013). Other scholars have called for more theoretically driven scholarship to understand victimization risk from a L-RAT perspective (Pratt & Taranovic, 2016). This study finds that psychological measures of cognitive styles and generalized anxiety show promise for providing a fuller understanding about the conditions under which routine activities increase risk of victimization. How people routinely feel and think as well as their behavioral habits are fruitful avenues through which to lower vulnerability to phishing victimization.

Low avoidant style and higher generalized anxiety were the strongest contributor to being phished, across all statistical models. Moreover, when the models were compared, the cognitive styles and generalized anxiety measures had the highest predictive accuracy for being phished, for not being phished, and showed the strongest classification accuracy above chance performance. Moreover, these findings cannot be attributed to social desirability or experimental demand as the survey was completed four weeks prior to sending the phishing e-mail and respondents were unaware that the e-mail was sent or connected to the survey study. Further buttressing the findings, prior research has found that individuals with generalized anxiety and anxiety about COVID had lower rates of accuracy in identifying which e-mails were phishing (Abroshan et al., 2021). Our findings underscore that trait anxiety can increase the likelihood of being phished using a prospective design and realistic phishing e-mail. These findings suggest that a fuller understanding of capable guardianship will expand upon the explanatory potential of emotions and cognition.

Although cognitive styles and generalized anxiety are important psychological concepts for understanding which persons will be less capable guardians of PII and be more vulnerable to phishing appeals, social psychology dual-processing theory needs to be combined with L-RAT. Students who had more vulnerable than protective strategies for interacting with e-mails also were more likely to be phished. Cyber-awareness training typically attempts to eliminate vulnerable strategies and reinforce protective strategies (e.g., Kumaraguru et al., 2009). This finding further supports the need to enhance knowledge about phishing and phishing strategies and supports prior survey research (e.g., Cheng et al., 2020; Graham & Triplett, 2017; Vishwanath, Harrison & Ng, 2016). Our measure of vulnerable and protective strategies asked about very specific behaviors in regard to responding to e-mails and making purchases or financial exchanges in virtual space. Other correlational survey studies have examined a broader range of cybersecurity awareness behaviors (Leukfeldt & Yar, 2016; Reyns, 2015; Van Wilsem, 2013), and the empirical support has been inconsistent.

Findings about the effectiveness of training centering around rule-based strategies also are inconsistent, with training increasing phishing victimization (Back & Guerette, 2021), decreasing phishing vulnerability within one week (Mayhorn & Nyeste, 2012) or for 28 days (Kumaraguru et al., 2009) or having no effect on victimization (Caputo et al., 2014). A review of 28 studies generally found that training improved detection of phishing, but that the findings for the effectiveness of training across time were inconsistent (Baki & Verma, 2022). Finally, a study using data from students in a military academy found that a longer time since last training and military GPA were the best predictors of being phished compared to demographics or standardized tests such as SAT or ACT (Rutherford et al., 2022).

The social psychology research on dual-processing models, cognitive styles, and emotional contributors to decisions begins to address how individuals interact with situations. L-RAT theory combined with a dual-processing theory provides potential to understand more fully how people think and feel and how our cognitive and emotional responses may make us vulnerable to manipulation and persuasion from phishers and other cybercriminals.

Phishing e-mails such as the one used in our study have an implied threat to affecting the receiver's relationship with their educational institution. Students with higher generalized anxiety may think more about the negative consequences of this disruption with their educational institution and react quickly without checking whether the message is authentic. The stable cognitive styles, strategies, and generalized anxiety were assessed four weeks prior to receiving the phishing e-mail, demonstrating that these traits came before being phished. The prospective design and the prior research showing the reliability and validity of our measures of cognitive styles and generalized anxiety (Hamilton et al., 2016; Louderback & Antonaccio, 2017; Scott & Bruce, 1995; Zsido et al., 2020) allow for more confidence that these measures contributed to being phished.

The machine learning models show a high F1-score, Recall and ESS and were consistent with the findings of the multinominal regression. However, predictive accuracy might be improved further by doing a grid search for the hyperparameters, doing feature selection or using different classification algorithms such as deep learning. For the sample having verification that respondents opened the phishing e-mail, the high recall of 82.00%, precision of 70.59%, and the ESS of 18.61% suggests that expanding training to address generalized anxiety for those with low avoidance has potential to reduce phishing rates in educational settings. While the experts in Ghazi-Tehrani and Pontell (2021) suggested machine learning algorithms to improve technological detection of phishing e-mails and websites, our research also highlights that machine learning algorithms can improve predictive modeling of cybervictimization. Moreover, our research underscores that theoretically guided research may enhance our understanding and prediction of phishing victimization.

There are several lines of future research from this study. Future work could look at varying the time to determine if the time between survey and phishing e-mail makes a difference. Moreover, the demographics of the participants were 18–21 years old college students, and our sample slightly overrepresented women and minorities for this university. Future research needs to address whether these findings generalize to older adults, to different emotional responses, and to different threat appeals. The phishing e-mail was specific to students noting that their account was locked and requesting that they click on the link as soon as possible to restore access – the phishing attack used authority and urgency. Future research also might examine whether these traits are related to distinct types of phishing e-mails such as reward framing, authority framing, or loss framing. Additional research is needed to examine how other emotions might contribute to interpretation and responses to phishing e-mails. Finally, more applied research is needed to assess the effectiveness of interventions that address generalized anxiety.

Cybersecurity training can be improved in two critical ways to address the emotional instability of those with higher generalized anxiety and to address the incidental fear and anxiety that phishing e-mails attempt to evoke. Consistent with the research supporting the appraisal-tendency hypothesis, individuals can be trained to reappraise their implicit tendency to reduce uncertainty through perceiving the attempt to exploit an emotional state (Lerner et al., 2015) and change their action tendency to thwart the phisher's attempt through reporting it to the organization. Organizations can promote reappraisal through encouraging employees to report suspicious e-mails and providing supportive feedback, even when the report is inaccurate. Another critical training option is to reduce state and generalized anxiety by providing mindfulness training; a meta-analysis of psychological research has shown the effectiveness of mindfulness training in reducing generalized and state anxiety (see for a review Hofmann et al., 2010). A recent study found cognitive-based mindfulness training compared to rule-based training significantly reduced vulnerability to a phishing e-mail 10 days after training (Jensen et al., 2017). Our findings, however, suggest that mindfulness training needs to focus on providing more emotional regulation through addressing generalized anxiety.

Notes

1. Each of our three models used features directly from the survey or derived from the survey. Features obtained directly from the survey include the answers from the participants such as a number between 1 and 5 for the question "I routinely delete e-mails from unknown sources." Features derived from the survey include calculations from the answers, such as the sum of all protective strategies where the participant answered the number 3, 4, or 5. The prior victimization model had five features; the decision-making strategies and generalized anxiety model had 17 features; and the vulnerable and protective strategies model had 35 features.
2. The formula for ESS = 100% X (MEAN PAC − 50)/50, and Mean PAC = (100 × (sensitivity + specificity)/2).
3. True Positive (TP) is the number of phished participants who were correctly predicted as having been phished. True Negative (TN) is the number of non-phished participants who were correctly predicted as having been not phished. False Positive (FP) is the number of non-phished participants who were incorrectly predicted as having been phished. This is similar to having a false alarm (e.g., an alarm goes off when there is no burglary). False Negative (FN) is the number of phished participants who were incorrectly predicted as having not been phished. This is usually worse than false positives as participants are getting phished without their awareness or their organizations' awareness.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This material is based upon work supported by the National Science Foundation under Grant No. DGE 1918591 and 1919004.

ORCID

Loretta Stalans http://orcid.org/0000-0003-1568-1577
Eric Chan-Tin http://orcid.org/0000-0001-8367-5836

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, *9*, 121916–121929. https://doi.org/10.1109/access.2021.3109091

Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, *104398622110016*(3), 427–451. https://doi.org/10.1177/10439862211001628

Baki, S., & Verma, R. (2022). Sixteen years of phishing user studies: What have we learned? *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/tdsc.2022.3151103

Beckers, T., & Craske, M. G. (2017). Avoidance and decision making in anxiety: An introduction to the special issue. *Behaviour Research and Therapy*, *96*, 1–2. https://doi.org/10.1016/j.brat.2017.05.009

Blanchette, I., & Richards, A. (2010). The influence of affect on higher level cognition: A review of research on interpretation, judgement, decision making and reasoning. *Cognition & Emotion*, *24*(4), 561–595. https://doi.org/10.1080/02699930903132496

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

Chan-Tin, E., Stalans, L. J., Johnston, S., Reyes, D., & Kennison, S. (2022). Predicting Phishing Victimization: Roles of Protective and Vulnerable Strategies and Decision-Making Styles. In Proceedings of the Fifth International Workshop on Systems and Network Telemetry and Analytics (SNTA '22), June 30, 2022, Minneapolis, MN, USA. ACM, Minneapolis, MN, USA. https://doi.org/10.1145/3526064.3534107 .

Cheng, C., Chan, L., & Chau, C.-L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, *108*, 106311. https://doi.org/10.1016/j.chb.2020.106311

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Couronne, R., Probst, P., & Boulesteix, A. (2018). Random forest versus logistic regression: A large-scale benchmark experiment. *BMC Bioinformatics*, *19*(1), 270–284. https://doi.org/10.1186/s12859-018-2264-5

DePaulo, B. M., & Tang, J. (1994). Social anxiety and social judgment: The example of detecting deception. *Journal of Research in Personality*, *28*(2), 143–152. https://doi.org/10.1006/jrpe.1994.1012

Djulbegovic, M., Beckstead, J., Elqayam, S., Reljic, T., Kumar, A., Paidas, C., Djulbegovic, B., & Antonietti, A. (2015). Thinking styles and regret in physicians. *PLos One*, *10*(8), e0134038. https://doi.org/10.1371/journal.pone.0134038

FBI. (2023). *2022 internet crime report*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders*, *16*(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press. https://doi.org/10.1515/9781503621794

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, *38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Grasmick, H. G., Tittle, C., Bursik, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *The Journal of Research in Crime and Delinquency*, *30*(1), 5–29. https://doi.org/10.1177/0022427893030001002

Hamilton, K., Shih, S.-I., & Mohammed, S. (2016). The development and validation of the rational and intuitive decision styles scale. *Journal of Personality Assessment*, *98*(5), 523–535. https://doi.org/10.1080/00223891.2015.1132426

Hindelang, M., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Hofmann, S. G., Sawyer, A. T., Witt, A. A., & Oh, D. (2010). The effect of mindfulness-based therapy on anxiety and depression: A meta-analytic review. *Journal of Consulting & Clinical Psychology*, *78*(2), 169–183. https://doi.org/10.1037/a0018555

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

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. https://doi.org/10.1145/1572532.1572536

Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. *Annual Review of Psychology*, *66*(1), 799–823. https://doi.org/10.1146/annurev-psych-010213-115043

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activities theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization. *The Journal of Research in Crime and Delinquency*, *54*(5), 639–679. https://doi.org/10.1177/0022427817693036

Lu, Y., Li, S., Freitas, A., & Ioannou, A. (2022). How data-sharing nudges influence people's privacy preferences: A machine learning-based analysis. *EAI Endorsed Transactions on Security and Safety*, *8*(30), e3. https://doi.org/10.4108/eai.21-12-2021.172440

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work*, *41*, 3549–3552. https://doi.org/10.3233/wor-2012-1054-3549

Miro-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology*, *14*(1), 139–155.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*, 773–793.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online or what we post online? *Criminal Justice Review*, *45*(4), 430–451. https://doi.org/10.1177/0734016820934175

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality & Individual Differences*, *169*, 1098–2016. https://doi.org/10.1016/j.paid.2020.109847

Phillips, W. J., Fletcher, J. M., Marks, A. D., & Hine, D. W. (2016). Thinking styles and decision making: A meta-analysis. *Psychological Bulletin*, *142*(3), 260–290. https://doi.org/10.1037/bul0000027

Ponemon. (2021, September 14). *The 2021 ponemon cost of phishing study: Proofpoint us*. Proofpoint. Retrieved October 26, 2022, from https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study

Pratt, T. C. (2016). A self-control/life course theory of criminal behavior. *European Journal of Criminology*, *13*(1), 129–146. https://doi.org/10.1177/1477370815587771

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *The Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903

Pratt, T. C., & Taranovic, J. J. (2016). Lifestyle and J routine activity theories revisited: The importance of 'risk' to the study of victimization. *Victims & Offenders*, *11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Reyns, B. W. (2013). Online routine and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *The Journal of Research in Crime and Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian general social survey. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119–1139. https://doi.org/10.1177/0306624X15572861

Rutherford, S., Lin, K., & Blaine, R. W. (2022). Predicting phishing vulnerabilities using machine learning. *SoutheastCon 2022*. https://doi.org/10.1109/southeastcon48659.2022.9764045

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement*, *55*(5), 818–831. https://doi.org/10.1177/0013164495055005017

Stalans, L. J., & , and Donner, C. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In H. Janankhani (Ed.). *Cyber criminology. Part of the advanced sciences and technologies for security applications book series (ASTSA)* (pp. 25–45). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_2

Stanovich, K. E., & Toplak, M. E. (2012). Defining features versus incidental correlates of type 1 and type 2 processing. *Mind & Society*, *11*(1), 3–13. https://doi.org/10.1007/s11299-011-0093-6

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

Van Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Van Wilsem, J. (2013). Hacking and harassment – Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453. https://doi.org/10.1177/1043986213507402

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, *20*(5), 570–584. https://doi.org/10.1111/jcc4.12126

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Volkova, E. V., & Rusalov, V. M. (2016). Cognitive styles and personality. *Personality & Individual Differences*, *99*, 266–271. https://doi.org/10.1016/j.paid.2016.04.097

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Yarnold, P. R., & Soltysik, R. C. (2016). *Maximizing predictive accuracy*. Optimal Data Analysis, LLC.

Zsido, A. N., Teleki, S. A., Csokasi, K., Rozsa, S., & Bandi, S. A. (2020). Development of the short version of the spielberger state-trait anxiety inventory. *Psychiatry Research*, *291*, 165–178. https://doi.org/10.1016/j.psychres.2020.113223