Predicting Phishing Victimization: Roles of Protective and Vulnerable Strategies and Decision-Making Styles

Eric Chan-Tin
Loyola University Chicago
Chicago, Illinois, USA

Loretta Stalans
Loyola University Chicago
Chicago, Illinois, USA

Spencer Johnston
Loyola University Chicago
Chicago, Illinois, USA

Daisy Reyes
Loyola University Chicago
Chicago, Illinois, USA

Shelia Kennison
Oklahoma State University
Stillwater, Oklahoma, USA

ABSTRACT

Phishing is a common vector for cybercrime and hacking. This research examines participants' personality styles (e.g. decision-making styles, self-control) and the likelihood of falling victim to phishing attacks. Over 300 participants completed an online survey assessing protective and vulnerable strategies, personality styles, trust in people, prior victimization from catphishing or identity theft, and demographics information. Unbeknownst to the participants, 2 to 4 weeks after completing the survey they received a phishing e-mail asking them to click on a link. Individuals with a stronger systematic decision-making style were more likely to have a greater number of protective strategies, and those with greater protective strategies were less likely to be a victim of catphishing and identity theft. Individuals with low avoidant decision-making styles and prior vulnerable strategies were more likely to be phished. These findings suggest that learning protective strategies and not using vulnerable strategies are insufficient to lower substantially the risk of being phished. Training might be improved through considering the match between decision-making styles and the content of the training.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Social and professional topics** → *User characteristics.*

KEYWORDS

Phishing, Victimization, strategies, Decision-making Styles

ACM Reference Format:
Eric Chan-Tin, Loretta Stalans, Spencer Johnston, Daisy Reyes, and Shelia Kennison. 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, New York, NY, USA, 8 pages. https://doi.org/10.1145/3526064.3534107

SNTA '22, June 30, 2022, Minneapolis, MN, USA
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9315-7/22/06…$15.00
https://doi.org/10.1145/3526064.3534107

1 INTRODUCTION

Phishing is an attempt to obtain private information from people by masquerading a message as legitimate. An example of a phishing attack is an e-mail appearing to be from a victim's bank asking victims to click on a link to confirm their identity. The linked website would ask victims to enter their bank login credentials, which the phisher would then be able to steal. In 2021, The FBI Internet Crime Complaint Center [12] reported that there were over 300,000 victims related to phishing with over $44 million in losses. This is likely an underestimate as many do not know they fell victim to a phishing attack. Moreover, phishing could be used for other crimes, such as identity theft and business e-mail compromise. Another variant of phishing is catphishing where individuals fake their identity on dating websites to obtain personal information and money. Phishing clearly is a prevalent and costly societal problem.

How can people lower their vulnerability to phishing victimization? In general, people are advised to guard against phishing attacks by using protective strategies such as checking for grammar, checking the "from" address, checking the URL of a link before clicking, refraining from opening or clicking on attachments or links, and deleting e-mails from unknown senders. People also are told to reduce falling victims through refraining from using vulnerable strategies such as regularly clicking on links in emails or replying to an email to determine whether it is legitimate.

In addition to these strategies, habitual ways of perceiving and problem solving, called decision-making styles, also might lower or increase vulnerability to becoming a victim of phishing. Decision-making styles include systematic, avoidant, and intuitive [29]. A systematic style involves careful examination of all information whereas intuitive style is faster decision-making based on limited cues and a feeling that the email is trustworthy. Those using avoidant styles delay making a decision for as long as possible, and often have higher anxiety about making decisions. Individuals with avoidant styles, thus, might feel more pressure when phishing emails threaten a negative consequence or might lower victimization through procrastination and forgetting about the email.

Prior studies have surveyed individuals after they clicked on the link in a phishing email and have found that those who click report more vulnerable than protective strategies and report less careful decision-making [36]. In this retrospective design, these findings might simply be justifications for participants' prior phishing victimization rather than contributors to increase vulnerability to phishing attacks. Empirical studies, moreover, have not examined decision-making styles or trust in people as predictors of phishing victimization. Our research addressed these shortcomings in prior research. We used a prospective design, one where strategies and personality were assessed in an online survey 2 to 4 weeks before phishing emails were sent to those who completed the survey. Respondents were unaware that they would receive a phishing email, and the survey did not mention phishing. Each participant was also asked to provide an e-mail address to obtain credit for completing the survey. The e-mail included a tracking pixel which could be used to determine whether or not a participant opened the e-mail. Many e-mail clients disable remote loading of images, thus the number of participants who opened the e-mail is an undercount. The phishing e-mail asked participants to click on a link for a fake company "JT Morgan" to donate to a fictitious cancer charity. We tracked the number of participants who clicked on the link as well as who submitted their private information on the website. IRB approval from our university was obtained.

The contributions of this research are as follows.

- Determine which protective or vulnerable strategies predict actually being phished in the future.
- Determine the decision-making styles, and personality styles, such as low or high self-control, of people who are more (or less) likely to fall victims to phishing attacks.
- Provide suggestions on how to improve training to prevent phishing attacks.

2 BACKGROUND

2.1 Phishing

Phishing is a malicious attempt to obtain victim's confidential information such as passwords, social security numbers, and credit card numbers. Phishing attacks have occurred for over two decades. They have historically been sent over e-mail, although phishing attacks now have been conducted over SMS (smishing), voice (vishing), and social media (e.g. Twitter). Usually, phishing attacks are sent en masse to a high number of targets. Even if only 0.01% of all recipients respond, if one billion e-mails were sent, that still translates to about 100,000 victims. Phishing e-mails can also include tracking code to indicate if a recipient has opened the e-mail.

Although stealing login credentials or financial information are the most common reasons for phishing, identity thefts and catphishing are also popular. Identity theft involves using private information such as credit cards, SSN, name, address, date of birth, medical records, for unlawful financial gain. Catphishing involves impersonating someone else (usually in a romantic setting) to ask victims to send money. Phishing, in general, is broad. The success of phishing attacks relies on sending masses of phishing e-mails.

To prevent phishing attacks, both technical approaches and user training methods have been used. Technical methods involve automatic phishing detection using machine learning and keyword detection to analyze the e-mail header, body, and links/attachments. These approaches also take user input as each user can tell the system that certain e-mails are "spam". Different types of warnings are used in e-mail clients to protect users from unsafe e-mails, such as a red "potential phishing e-mail" warning or moving phishing e-mails to a "spam" folder. Phishing attacks are now using real e-mail addresses that pass the DMARC verification. They are also more targeted and better written. Moreover, the automatic phishing detection usually requires some time to detect new phishing campaigns. However, technical approaches will not prevent all phishing emails from being received, and thus we need to understand what type of user is more likely to be phished.

Users are trained and educated on ways to detect phishing e-mails as well as on how not to become victims of a phishing attack. Some common advice is to check for spelling errors, not to click on links or attachments, type the URL manually, and to check the sender. Yet, phishing is becoming more sly with improvements such as fewer spelling errors, using URL link shorteners, and sending e-mails from real accounts (sometimes after an account takeover). Moreover, phishing attacks are now varied: e-mail, SMS, social media, and phone calls. Plus, human errors will always occur, and phishing as a result remains successful.

Decision-making styles are ways that people habitually make decisions across context and time and are part of each person's personality. In this study, we examine whether decision-making styles are associated with opening a phishing e-mail, deciding whether to read the e-mail, and to click on the phishing link.

2.2 Related Work

2.2.1 *Phishing.*

There have been many studies on anti-phishing training and their effectiveness. In general and as expected, phishing training is not effective, especially in the long run. Younger age groups and women tend to be more likely to fall victims to phishing [30]. Although training focused on phishing links tend to reduce the number of clicks on phishing links, it also reduced the number of clicks on legitimate links. Since the web is the main avenue of phishing attacks due to phishing links, many browsers implement phishing warning and/or detection. However, those warnings and detection do not work – 79% of participants ignore the warnings [7]. Due to the ineffectiveness of training, new phishing training is proposed [1, 14–16, 31]. The results are that 1) the retention length could be higher than a month, 2) more training messages might help reinforce anti-phishing, 3) rate of clicking on legitimate links is not reduced, and 4) some anti-phishing tips are more effective than others. Phishing attacks are sent to the masses. Spear phishing is more targeted. A study on a spear phishing campaign [3] found that although overall phishing awareness is increased after training, targeted spear phishing attacks are still a problem. A survey of phishing literature was performed [28] – the survey found that there is still much work to be done in phishing research, anti-phishing training, and automated phishing detection.

Victimization on the internet has been previously explored [17], suggesting that there is no clearly defined group indicating whether an individual becomes a victim. However, [11] showed that an information-rich social presence condition leads to victimization. Moreover, digital literacy and social position impacts the effect of becoming a phishing victim. As expected, individual with higher digital literacy and social position tend to receive more phishing e-mails, but are less likely to respond to them [8]. Phishing on social media sites has also been studied [2]. It found that users on social media can also be victims. Some factors such as the # of friends, # of strangers, and # of close friends, affect how likely an individual is to fall victim. A "routine activity" approach and protective strategies have been studied in [13]. The results were similar to ours as they found that even individuals with high protective strategies can fall victim to phishing attacks. However, we further quantify our results with decision-making styles and vulnerable strategies as well as differentiate the different types of victimization. The routine activities theory is further explored [23], showing that fear of victimization, social demographics, fear of identity theft victimization, education level, routine online activities are all related to phishing and identity theft victimization. A theoretical model of victimization due to phishing, using the Heuristic-Systematic model, was proposed in [20], but has not been adequately explored further.

2.2.2 *Protective and Vulnerable Strategies.*

Strategies about engaging with communication in emails and social media also inform people's decisions about which emails to read and respond to through replying or clicking on links. Strategies have been defined as "learned sequences of acts that have become automatic responses to specific cues and are functional in obtaining certain goals or end-states." [33]. Some studies have found that habitual email use, frequent and automatic checking and responding to email, is related to clicking on a phishing email [34–36]. Mobile phones increase the strength of habitual checking and responding to emails, which in turn leads to a higher rate of being phished [35]. These studies, however, measured strategies as well as explanations of heuristic and systematic processing after students clicked on the phishing email or one week later if they did not click. Thus, it is unclear whether strategies and beliefs about how they processed the information were merely justifications for being phished or not phished rather than increased the chance of being phished.

Moreover, the aforementioned research has focused on habitual strength of opening and responding to email rather than the nature of mental habitual rules. Some strategies might be protective and result in a decrease chance of being phished whereas other strategies might increase vulnerability to victimization. One study assessed whether after being phished or not, respondents reported attention to potential cues of phishing emails: urgency to respond, the subject line, the URL (source), and grammar mistakes. Respondents reporting attention to the subject line or urgency cue were more likely to be phished whereas respondents who focused on the URL source or grammar mistakes were less likely to be phished [37]. Respondents can develop strategies about procedures for handling unknown emails or emails of urgency that can increase or decrease vulnerability to phishing. One other study found that respondents having stronger protective strategies also had more confidence as well as greater accuracy in differentiating phishing from legitimate emails [6]. Both of these studies, however, have not assessed protective and vulnerable strategies in a survey weeks before respondents are sent a phishing email. Strategies are difficult to change as research has shown that training effects often wear off, and individuals can be phished within four hours of training as they revert back to vulnerable strategies in reading emails and low involvement in decision-making. The current research focuses on two strategies that will increase vulnerability to phishing: regularly clicking on links in emails and replying to authenticate the legitimacy of the email. We also examine three protective habitual mental rules: deleting emails from unknown sources, checking URLs, and only visiting reputable websites.

2.2.3 *Decision-making Styles.*

Whereas strategies allow automatic responding from mental rules, decision-making styles focus on the habitual and dispositional ways people make decisions across contexts (e.g., [10, 29]). A two-component factor structure suggests that individuals vary on how well they consider available information in the context compared to their internal feelings and the extent to which they make decisions easily or have anxiety about making choices [4]. Much research has focused on whether people generally rely more on a systematic, rational decision-making style that focuses on careful consideration of the available information or an intuitive decision-making style that focuses more on feelings and instinct as well as faster decision-making rather than careful reflection about the information (see [24]). A recent meta-analysis of 89 samples and a pooled sample of 17,704 participants found that systematic thinking style had small but significant effects on increased decision accuracy and confidence whereas intuitive thinking had small significant effects on lowering accuracy but increasing confidence. A match between decision-making style and decision task produced the strongest effects for thinking styles on decision performance [24]. Both students and employees with higher scores on preferences for rational thinking were less likely to be victims of computer-based cybercrimes such as malware and phishing [19].

Avoidant styles and its associated anxiety have received little attention in cybercrime victimization, including phishing and identity theft. Anxiety, like fear, will increase resistance to making a decision in order to delay increasing anxiety and lack of control. Thus, anxious individuals often avoid and delay decision-making [5]. How people make decisions about threats to human health was examined using the context of consumption of raw eggs and contracting Salmonellosis. [32] analyzed data from 2,960 respondents who completed an online survey on food safety. They found that those who preferred to delay decisions were more likely to seek information, but anxiety lowered the likelihood of information seeking.

3 HYPOTHESES

Our research provides one of the few studies that have examined how well different decision-making styles, protective and vulnerable strategies, and beliefs about trusting others predict being phished 2-4 weeks after these traits were assessed. Based on prior research with retrospective designs, we hypothesized that systematic decision-making style and protective strategies would reduce the likelihood of being phished. We also hypothesized that individuals with vulnerable strategies such as clicking on links, and those with greater general trust would have a higher likelihood of being phished. We also hypothesized that those with avoidant decision styles, which were often associated with anxiety, would be more likely to have vulnerable strategies, as they sought additional information to make decisions (e.g., [32]). We examine whether vulnerable strategies predict being phished differently for those with low and high avoidant decision-making styles.

4 METHODS

4.1 Sample and Sampling

Undergraduate students in introductory psychology classes received one research credit hour to participate in this study. Respondents signed up through the psychology research pool. Of the

354 respondents who started the Qualtrics online survey, 329 provided completed data and took at least five minutes to complete the survey. The qualified sample consisted primarily of self-identified women (84%), and cisgender/heterosexual persons (84%). Most respondents were freshmen (62.5%) or sophomores (24.5%), with a mean age of 18.87 (sd = 1.17). Racial identification was more diverse with 60.8% identifying as only White, and 38.9% identifying with at least one racial or ethnic minority group (3.9% Black; 0.6% Native American; 0.9% Pacific Islander; 14.5% Latinx; and 19.9% Asian).

4.2 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 decision-making styles, self-control, and demographics. Respondents were unaware of the second phase, which occurred after a completed survey was submitted. The online survey examined the participants' protective strategies, vulnerable strategies, victimization, and decision-making styles.

In the second phase, respondents were randomly assigned to receive an email consisting of one of three phishing appeals: a) normative – social justice focus; b) normative – group appeal; and c) pragmatic, cost-effectiveness appeal. The first line of the email contained the manipulation, and all other information in the email was constant across conditions, including the subject heading of "Click to Support Reducing Deaths from Cancer" and the greeting, "Hello There!", and the signature of "International Cancer Foundation". For example, the social justice appeal condition email read: "As a <University> student, are you concerned about social justice enough to take a second to help? If you click HERE, JT Morgan Inc. will donate $10 to the International Cancer Foundation (or another charity of your choice). Death from cancer has declined 26% since 1991, but the economically disadvantaged have much higher death rates. Thank you for your support of reducing cancer death rates for the disadvantaged or your preferred charity. Every click matters." The first line of the normative group appeal email was "As a <University> student, will you take a second to help reduce cancer – and be in the 90% who care enough to click for JT Morgan Inc. to donate to the International Cancer Foundation?" The first line of the pragmatic cost-effective appeal was: "As a <University> student, will you take a second to help lower the taxpayers' burden to reduce deaths from cancer?" The actual e-mail included the name of the university.

To prevent the phishing email being blocked by our university's spam filters, the information technology department placed the email on a white list. We assessed whether participants opened the email, clicked on the link, and added their name to receive recognition for their effort. For this email, the URL was unique for each participant's e-mail. For example, $hash(example@company.com) = MTNhMWY2NDlkMWI1MDMxMmNkMDQzMzNkZTBlOGI3NjU=$ in base64 encoding. The hash algorithm is a one-way function. Moreover, this e-mail included a tracking 1x1 remote image to assess if participants opened the e-mail and their e-mail client/browser allowed remote image loading.

Data were collected over the Fall 2019 and Spring 2020 semester. In the Fall 2019 semester, respondents were randomly assigned to receive the email either two or four weeks after submitting the completed survey. As the time gap did not have an appreciable difference and to increase sample size within each appeal, during Spring 2020, we sent the email out after an average of three weeks after submitting the completed survey. Respondents were fully debriefed about the study three weeks after all data were collected.

We obtained IRB approval to recruit participants, distribute the survey, and collect the e-mail addresses. Since our survey required some deception, we had to undergo a full IRB board approval. All participants were debriefed whether they clicked on the link or not. We received no response from the debriefing e-mail. 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 increase the anxiety level of the participants.

5 MEASUREMENT

5.1 Use of Email and Dating Apps

Individuals were asked how many minutes they spent on various tasks using a seven point scale: "No Time; 5 minutes; 6 to 15 minutes; 16 to 30 minutes; 31 to 60 minutes; One to two hours and over two hours. Based on the skewness of the data and sufficient time to create more demand, a dichotomous measure was created for time spent reading email with 0 = to 15 minutes or less, 64.5%; and 1 = 16 minutes to 2 hours, 35.5%. Based on the skewness of the data, use of dating apps was coded as 0 for did not use (79.2%) and 1 = some time (20.8%).

5.2 Behavioral Strategies

Respondents were asked: "How well each of these statements characterizes your behavior in operating your computer or web-based technology." Respondents indicated their agreement on a 1 to 5 scale where 1 = 'strongly disagree' and 5 'strongly agree'. These strategies were generated based off best practices.

Protective Strategies Scale. Protective strategy scale comprised a count of the number of agreement or strong agreement with these three strategies that might lower the risk of phishing victimization: a) "I immediately delete emails from senders I do not know," b) "I check the URL of a link in an email before clicking on it," c) "I only conduct online transactions with reputable sites," mean = 1.87, Median = 2.00, sd = .92. Each item also was treated as a dependent variable to assess whether significant predictors were consistent across all items.

Vulnerable Strategies Scale. This scale was comprised of a count of whether individuals agreed or strongly agreed to two items: a) regularly click on links in emails; and b) regularly reply to determine whether an email is legitimate, mean = .31, median = 0, sd = .53. Most individuals did not hold these strategies (72.9%, n = 239) while 23.5% had one strategy, and 3.7% had two of these strategies.

5.3 Decision-making Thinking Styles

The decision-making thinking scale developed by Scott & Bruce [29] was used to assess stable thinking styles. 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 or disagree; 5 = strongly agree.

Systematic Style. Systematic style was measured using eight items such as "I make decisions in a logical and systematic way," "my decisionmaking 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 = 3.83; Median = 3.87; sd = .61) and had good inter-item reliability (Cronbach alpha = .85). 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.

Intuitive Style. Intuitive style was an average of four questions where individuals assessed how they made decisions: "I tend to rely on my intuition," "it is more important for me to feel the decision is right than to have a rational reason for it," "I trust my inner feelings and reactions," and "I do what feels natural" (Mean = 3.36; Median = 3.5; sd = .72, Cronbach alpha = .74).

Avoidant Decision-making. Two items from the Decision-making 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 = .74), and a mean of 2.97, Median = 3.0, sd = .99).

5.4 Self-Control Scale

A standardized 11 item scale [9] 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 (see [25]). 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 .80. Respondents indicated their agreement to each of the eleven items using a five-point scale from 1 = strongly disagree and 5 = strongly agree. The eleven items were averaged (Mean = 2.52; Median = 2.45; sd = .62).

5.5 Trust in People Scale

Three questions focusing on an individuals' trust in people generally were averaged to form a reliable scale (Cronbach alpha = .83) and had a mean of 3.68, median=4.0, sd=.89. Respondents indicated on a five-point scale their agreement with each item. One example is "I usually trust people until they give me a reason not to trust them."

5.6 Victimization of Catphishing/Identity Theft

Respondents were asked several questions about their victimization from cybercrimes in the past year and responded using the categories, 'never', 'once', 'sometimes', 'often', and 'very often'. Respondents answered three questions about 'catphishing' victimization where the perpetrator pretends to be someone they know to obtain information or imitates them online to obtain information, and three questions about unauthorized used of computers or credit cards, which is often part of identity theft cybercrimes. As the responses were skewed, dichotomous measures were created with 0 = never and 1 = one or more times for (catphishing 34.4% = 1) and identity theft (52.6% = 1). To assess whether individuals with both types of victimization had different predictors, we created a nominal variable where 0 = neither catphishing or identity theft victimization (36.7%), 1 = having either catphishing or identity theft (42.1%), and 2 = having both types of victimization (21.2%).

6 RESULTS

We first conduct ordinary least squares (OLS) regressions to test the hypotheses about decision-making styles, and cognitive load on the vulnerable and protective strategy scales. We then examine how protective and vulnerable strategies, decision-making styles, and personal orientations are related to reported victimization from catphishing or identity theft and to confidence of detecting phishing emails. Finally, we examine how protective, vulnerable strategies, personal orientations and decision-making styles predict actual decisions about clicking on the phishing email that was sent and how these relationships differ for those who have decision anxiety and have an avoidant decision-making style.

6.1 Predicting Number of Protective and Vulnerable strategy Scales

We conducted ordinary least squares (OLS) regression to assess the hypotheses about decision-making styles and cognitive load. The second column of Table 1 presents the findings for predicting total number of protective strategies, and the third column shows the findings for predicting total number of vulnerable strategies. As expected, individuals with stronger systematic decision-making style were more likely to have a greater number of protective strategies, but this style was unrelated to vulnerable strategies. Consistent with prior research suggesting that avoidant decision styles seek information (e.g., [32]), individuals with avoidant decision style were more likely to have vulnerable strategies. Individuals who used dating apps had a greater number of vulnerable strategies than those who did not use dating apps, suggesting that such use might lower suspicion of requests or increase confidence to detect scammers. Finally, consistent with prior research on habitual email use [34–36], individuals who spent over sixteen minutes a day reading emails had a greater number of vulnerable strategies than those who spent less time.

6.2 Predicting Victimization from Catphishing and Identity Theft

Individuals who fall victim to phishing scams often might have others imitate them on social media accounts to gain additional information or can be victims of unauthorized use of credit cards or accounts). Table 2 presents the results of a multinominal logistic regression to assess the predictors of those who were victims of either catphishing or identity theft as well as those who were victims of both catphishing and identity theft compared to those who were victims of neither cybercrime. The group of neither a victim of catphishing or identity theft served as the reference group. Time spent on emails or dating apps were not entered into the models as they were not significantly related to victimization.

As shown in Table 2, those with greater protective strategies were less likely to be a victim or repeat victim. However, vulnerable strategy scale was unrelated to victimization. Those high in avoidant decision-making style were 1.41 times more likely to be a victim of either catphishing or identity theft than those low in avoidant decision-making style. It is unclear why those with more

Predictors	Total # of Protective Strategies			Total # of Vulnerable Strategies		
	b	Beta	(SE)	b	Beta	(SE)
Systematic Decision-making Style	$.29^{D}$	.19	.086	.02	.02	.05
Avoidant Decision-making Style	−.06	−.07	.050	$.08^{D}$	.15	.03
Used dating app	−.20	−.09	.124	$.17^{C}$	.13	.07
Greater amount of time reading emails	−.01	−.00	.105	$.11^{A}$	.10	.06
Low Trust in People	.02	.10	.01	$-.12^{A}$	−.09	.07
Constant	.43		.32	−.038		.208
F-value (1, 286)	3.37^{C}			3.76^{C}		
R^2	.05			.055		
Standard Error of the Estimate	.90			.52		
N	325			326		

Note. One-Tailed p-values are: $^{A}p < .05;^{B} p < .025;^{C} p < .01;^{D} p < .001;^{E} p < .0001$

Table 1: OLS Regression Predicting Total Number of Protective and Vulnerable Strategies.

Predictors	Either Catphishing OR Identity Theft Victim		Both Catphishing and Identity Theft Victim	
	Odds Ratio	SE	Odds Ratio	SE
Protective strategy Scale	$.70^{C}$	.15	$.70^{B}$	.18
Vulnerable strategy Scale	1.12	.25	.99	.32
Avoidant Style	1.41^{D}	.14	.96	.18
Systematic Style	1.30	.24	1.37	.29
Low Self Control	1.43	.25	1.98^{C}	.30
Higher Trust in People	$.52^{B}$	.34	1.45	.30
Constant	b = -1.52	1.23	b = -3.07	1.56
-2 Likelihood	33.22^{D}			
Nagelkerke R^2	.11			

Note. Superscripts indicate the one-tailed p-values: $^{A}p < .05;^{B} p < .025;^{C} p < .01;^{D} p < .005$.

Table 2: Multinominal Logistic Regression Predicting Whether Victim of Catphishing or Identity Theft or Both.

trust in people were less likely to be victims of catphishing or identity theft. Consistent with research on cybercrime victimization (see [26]), individuals with lower levels of self-control were more likely to be victims of both identity theft and catphishing than those with higher levels of self-control.

6.3 Examining Actual Behavior: Did Strategies and Decision-Making Styles Predict Being Phished

Of our sample of 327 respondents, only 128 viewed the phishing email that we sent two to four weeks later. None of the demographics, victimization experiences, strategies, beliefs, or decision-making styles predicted who viewed the email and who did not. Some individuals may rarely check their school emails or open emails that do not seem directly relevant to school. To examine who clicked on the link in the phishing email, we conducted analyses on only the 128 individuals who viewed the email. As individuals with avoidant styles might have less consistent strategies or processing styles, we separated the sample from those who had a high avoidant style (agreed to both statements) and those who had a less avoidant style. Table 3 presents the Point-biserial correlations for those with Low Avoidant Style, High Avoidant Style, and the entire sample. The superscripts on the correlations indicate whether the correlations are statistically significant, and the size of the correlation can be converted to percentage of variance explained (R-square) by multiplying the correlation with itself. First, there are only two relationships that are in the same direction for the samples of low avoidant and high avoidant styles: Individuals with the strategy of deleting unknown emails were significantly less likely to click on the link, r = -.23, p <.01. Thus, deleting unknown email explains 5.29% of the variance in clicking or not clicking on the link, which is moderate, especially when there is a gap of 2-4 weeks between completing the survey and receiving the phishing email, viewing it, and deciding whether to click on the link. Research that measured both being phished and protective strategies such as checking for grammar mistakes have generally found similar size correlations [37].

For those with low avoidant styles who do not delay decision-making, we shows that individuals who reported more agreement with vulnerable strategies of regularly clicking on links, replying to suspicious emails to assess authenticity, and using the same password for multiple sites were significantly more likely to click on the links. Conversely, these associations were not significant and in the opposite direction for those with high avoidant decision-making style; the anxiety associated with real world decisions for

	Decision-making Style		
Correlates	Low Avoidant N = 104	High Avoidant (Delays Decision N = 26	Entire Sample that Viewed Email N = 130
Strategies:	15.4% clicked	26.9% clicked	17.7% clicked
Deletes Unknown emails	$-.23^{**}$	$-.22$	$-.24^{**}$
Clicks on links	$.20^{*}$	$-.23$	.09
Replies to determine authenticity of message	$.27^{**}$	$-.17$	$.15^{*}$
Uses same password for multiple sites	$.17^{*}$	$-.14$	.15
Protective Strategy Scale	$-.14$	$-.13$	$-.15^{*}$
Vulnerable Strategy Scale	$.21^{*}$	$-.23$	.10
Systematic Decision-making Style	.05	$-.35^{*}$	.04
Higher Trust in People Scale	$-.05$	.31	$-.02$
Low Self-Control	$-.05$	$-.34^{*}$	$-.10$

Note: Point-Biserial Correlations are appropriate for the continuous measures and the dichotomous outcome of clicked or did not click on phishing link. Coefficients with superscripts indicate significant beyond chance at one-tailed p-values: $^{T}p < .06;^{*} p < .05;^{**} p < .01$.

Table 3: Point-Biserial Correlations between strategies and Whether Clicked on Link in Phishing Email After Viewing Within High and Low Avoidant Decision-making Style.

this group might reduce information seeking and lower the relationship between self-reported strategies and real behavior. Those with high avoidant style, however, were less likely to click on the link if they had a systematic decision-making style or if they had lower general trust in people, with these relationships explaining over 9% of the variance. A prior meta-analysis of thinking styles on decisions found significant, but small effects (r = .11), but these effects were stronger when the style matched the decision task [24].

In the last analysis, we conducted a logistic regression predicting clicking on the phishing link for only those who viewed the email. We created an interaction term to assess whether individuals with a low avoidant style were more likely to click on the link when they previously reported using vulnerable strategies in the survey. Those with high avoidant decision-making style might be very inconsistent in their use of strategies, as their primary objective is to delay decision-making.

Individuals with high avoidant strategies overall were 4.57 times more likely to click on the link (Wald = 5.11, p < .05). Moreover, those with low avoidant style and vulnerable strategies were 11.6 times more likely to click on the link than those without this combination (Wald = 4.88, p < .05). Vulnerable strategies did not predict clicking on the link for those with high avoidant styles (Odds ratio = .33, Wald = 1.41, p > .05.). In the previous analysis, individuals with high avoidant styles were more likely to be victims of either catphishing or identity theft, and some might have learned to refrain from vulnerable strategies of clicking on links or replying to unknown persons. These findings suggest that training to reduce vulnerability to phishing attacks need to consider the decision-making style of individuals. Future research needs to explore the conditions under which victimization reduces or exacerbates the chances of further victimization. Future research, moreover, with a larger sample will need to examine the potential moderating role of anxiety and orientations of general trust or suspicion of people.

7 DISCUSSION

Our research has some limitations. First, the participants were all college students aged 18-21. This could mean they are technologically more savvy than the average user. This could mean that phishing might be more prevalent for older people. We plan to perform a larger scale study with a more diverse group on a crowdsourcing platform in the future. Not many participants clicked on the link, although many viewed the e-mail (remotely loaded the tracking image). This could be because they knew it was a phishing e-mail or were not interested in either cancer or donating to charity. At debriefing, we did not ask the participants to explain whether they read the e-mail, why they clicked or did not click on the link, or whether the phishing e-mail was realistic or persuasive.

The reliability of self-reported strategies and self-reported behaviors have been previously studied. For example, [22] found that self-reported practice behaviors and actual practice behaviors among music players were similar, [27] found that self-reported and device-measured sedentary behaviors were similar, and [18] found that habits have a role in predicting learning technologies. Moreover, [21] found that information security habits were good predictors of security behaviors.

Based on our findings, it is not clear whether exhibiting protective strategies or vulnerable strategies can accurately predict whether an individual will fall victim to phishing. Since phishing (and its variants) are still a popular avenue of attacks, better anti-phishing training is needed. Phishing training could include more personalization based on the individual's decision-making style.

8 CONCLUSION

Our prospective design where individuals completed the survey before the phishing email was sent improved the design of prior phishing research. This design increases the confidence that avoidant decision-making styles and vulnerable behaviors contributed to being phished and were not ad-hoc justifications for being a victim of phishing. Furthermore, the survey results provide further correlational support, showing that those with high avoidant styles were more likely to report using vulnerable strategies, and these vulnerable strategies were related to prior catphishing or identity theft victimization. The survey results also show that those with systematic decision-making styles reported more protective strategies, and those with a greater number of protective strategies were less likely to report catphishing or identity theft victimization.

Looking ahead, the research showed that teaching rules, such as check the URL, is not enough to prevent victimization due to avoidant decision-making styles. This research suggests that current anti-phishing training can be improved by paying more attention to decision-making styles of the individuals in addition to teaching protective and vulnerable strategies. Our future research examines how decision-making styles, protective and vulnerable strategies and prior victimization intersect with generalized trait anxiety as phishers often attempt to manipulate people through increasing their anxiety.

9 ACKNOWLEDGMENTS

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

REFERENCES

[1] A. Alnajim and M. Munro. 2008. An evaluation of users' tips effectiveness for Phishing websites detection. In *2008 Third International Conference on Digital Information Management*. 63–68. https://doi.org/10.1109/ICDIM.2008.4746717

[2] Z. Alqarni, A. Algarni, and Y. Xu. 2016. Toward Predicting Susceptibility to Phishing Victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC)*. 419–426. https://doi.org/10.1109/SCC.2016.61

[3] A. J. Burns, M. Johnson, and D. Caputo. 2019. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce* 29, 1 (2019), 24–39.

[4] C. Dewberry, M. Juanchich, and S. Narendran. 2013. Decision-making competence in everyday life: The roles of general cognitive styles, decision-making styles and personality. *Personality and Individual Differences* 55, 7 (2013), 783–788.

[5] C. Dewberry, M. Juanchich, and S. Narendran. 2013. The latent structure of decision styles. *Personality and Individual Differences* 54, 5 (2013), 566–571.

[6] J. S. Downs, B. Donato, and A. Alessandro. 2015. Predictors of risky decisions: Improving judgment and decision making based on evidence from phishing attacks. *Neuroeconomics, judgment, and decision making* (2015), 239–253.

[7] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. ACM, New York, NY, USA, 1065–1074. https://doi.org/10.1145/1357054.1357219

[8] Roderick Graham and Ruth Triplett. 2017. Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior* 38, 12 (2017), 1371–1382.

[9] Harold G Grasmick, Charles R Tittle, Robert J Bursik Jr, and Bruce J Arneklev. 1993. Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of research in crime and delinquency* 30, 1 (1993), 5–29.

[10] Katherine Hamilton, Shin-I Shih, and Susan Mohammed. 2016. The development and validation of the rational and intuitive decision styles scale. *Journal of personality assessment* 98, 5 (2016), 523–535.

[11] B. Harrison, A. Vishwanath, Y. J. Ng, and R. Rao. 2015. Examining the Impact of Presence on Individual Phishing Victimization. In *2015 48th Hawaii International Conference on System Sciences*. 3483–3489.

[12] FBI IC3. 2021. https://pdf.ic3.gov/2021_IC3Report.pdf.

[13] J. Jansen and R. Leukfeldt. 2016. Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology* 10, 1 (2016), 79.

[14] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 3, 12 pages. https://doi.org/10.1145/1572532.1572536

[15] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, New York, NY, USA, 905–914. https://doi.org/10.1145/1240624.1240760

[16] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. 2008. Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit*. 1–12. https://doi.org/10.1109/ECRIME.2008.4696970

[17] E. R. Leukfeldt. 2014. Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking* 17, 8 (2014), 551–555. https://doi.org/10.1089/cyber.2014.0008

[18] Moez Limayem and Christy MK Cheung. 2011. Predicting the continued use of Internet-based learning technologies: the role of habit. *Behaviour & Information Technology* 30, 1 (2011), 91–99.

[19] Eric R Louderback and Olena Antonaccio. 2017. Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. *Journal of research in crime and delinquency* 54, 5 (2017), 639–679.

[20] Xin (Robert) Luo, Wei Zhang, Stephen Burd, and Alessandro Seazzu. 2013. Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security* 38 (2013), 28 – 38. https://doi.org/10.1016/j.cose.2012.12.003 Cybercrime in the Digital Economy.

[21] Kalana Malimage. 2013. *The role of habit in information security behaviors*. Mississippi State University.

[22] P. Miksza. 2007. Effective practice: An investigation of observed practice behaviors, self-reported practice habits, and the performance achievement of high school wind players. *Journal of Research in Music Education* 55, 4 (2007), 359–375.

[23] Seung Yeop Paek and Mahesh K. Nalla. 2015. The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice* 43, 4 (2015), 626 – 642. https://doi.org/10.1016/j.ijlcj.2015.02.003

[24] Wendy J Phillips, Jennifer M Fletcher, Anthony DG Marks, and Donald W Hine. 2016. Thinking styles and decision making: A meta-analysis. *Psychological Bulletin* 142, 3 (2016), 260.

[25] A. Piquero and A. Rosay. 1998. The reliability and validity of Grasmick et al.'s self-control scale: A comment on Longshore et al. *Criminology* 36 (1998), 157.

[26] Travis C Pratt, Jillian J Turanovic, Kathleen A Fox, and Kevin A Wright. 2014. Self-control and victimization: A meta-analysis. *Criminology* 52, 1 (2014), 87–116.

[27] Stephanie A Prince, Luca Cardilli, Jennifer L Reed, Travis J Saunders, Chris Kite, Kevin Douillette, Karine Fournier, and John P Buckley. 2020. A comparison of self-reported and device measured sedentary behaviour in adults: a systematic review and meta-analysis. *International Journal of Behavioral Nutrition and Physical Activity* 17, 1 (2020), 1–17.

[28] Swapan Purkait. 2012. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security* (2012).

[29] Susanne G Scott and Reginald A Bruce. 1995. Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement* 55, 5 (1995), 818–831.

[30] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 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 Systems (CHI '10)*. ACM, New York, NY, USA, 373–382. https://doi.org/10.1145/1753326.1753383

[31] Hossein Siadati, S. Palka, A. Siegel, and D. McCoy. 2017. Measuring the Effectiveness of Embedded Phishing Exercises. In *10th Workshop on Cyber Security Experimentation and Test (CSET 17)*. USENIX Association, Vancouver, BC.

[32] Emma Soane, Iljana Schubert, Rebecca Lunn, and Simon Pollard. 2015. The relationship between information processing style and information seeking, and its moderation by affect and perceived usefulness: Analysis vs. procrastination. *Personality and Individual Differences* 72 (2015), 72–78.

[33] Bas Verplanken and Henk Aarts. 1999. Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-directed Automaticity? *European Review of Social Psychology* 10, 1 (1999), 101–134. https://doi.org/10.1080/14792779943000035

[34] A. Vishwanath. 2015. Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication* 20, 1 (2015), 83–98.

[35] Arun Vishwanath. 2016. Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Computers in Human Behavior* 63 (2016), 198–207.

[36] Arun Vishwanath, Brynne Harrison, and Yu Jie Ng. 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research* 45, 8 (2018), 1146–1166.

[37] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H Raghav Rao. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* 51, 3 (2011), 576–586.