Online Information Review

Individual processing of phishing emails: How attention and elaboration protect against phishing

Brynne Harrison Elena Svetieva Arun Vishwanath

Individual processing of phishing emails

How attention and elaboration protect against phishing

Brynne Harrison
Department of Communication, University at Buffalo, Buffalo, New York, USA
Elena Svetieva
Catolica-Lisbon School of Business and Economics, Universidade Catolica Portuguesa, Lisbon, Portugal, and
Arun Vishwanath
Department of Communication, University at Buffalo – SUNY, Buffalo, New York, USA

Received 8 April 2015
Revised 7 October 2015
Accepted 18 December 2015

Abstract

Purpose – The purpose of this paper is to explore user susceptibility to phishing by unpacking the mechanisms that may influence individual victimization. The focus is on the characteristics of the e-mail message, users' knowledge and experience with phishing, and the manner in which these interact and influence how users cognitively process phishing e-mails.

Design/methodology/approach – A field experiment was conducted where 194 subjects were exposed to a real phishing attack. The experimenters manipulated the contents of the message and measures of user traits and user processing were obtained after the phishing attack.

Findings – Of the original list of targets, 47 percent divulged their private information to a bogus form page. Phishing susceptibility was predicted by a particular combination of both low attention to the e-mail elements and high elaboration of the phishing message. The presence of a threat or reward-based phishing message did not affect these processes, nor did it affect subsequent phishing susceptibility. Finally, individual factors such as knowledge and experience with e-mail increased resilience to the phishing attack.

Research limitations/implications – The findings are generalizable to students who are a particularly vulnerable target of phishing attacks.

Practical implications – The results presented in this study provide pragmatic recommendations for developing user-centered interventions to thwart phishing attacks. Lastly the authors suggest more effective educational efforts to protect individuals from such online fraud.

Originality/value – This study provides novel insight into why phishing is successful, the human factor in susceptibility to online deception as well the role of information processing in effective decision making in this context. Based on the findings, the authors dispel common misconceptions about phishing and discuss more effective educational efforts to protect individuals from such online fraud.

Keywords Phishing, Experimental study, Online cognitive processing, Online deception

Paper type Research paper

1. Introduction

Phishing is an attempt to gain personal and sensitive information from individuals through online deception. Rather than using technical expertise to compromise system security, phishing – defined as a "semantic attack" (Downs *et al.*, 2006) – employs social engineering techniques in an attempt to persuade users to divulge private information like usernames and passwords, account details (including bank account details) and social security numbers. Phishers typically utilize an e-mail with a hyperlink embedded

Online Information Review
Vol. 40 No. 2, 2016
pp. 265-281

1468-4527
DOI 10.1108/OIR-04-2015-0106

in it and a message with a warning of account closure or suggesting some unclaimed reward to entice the potential victim to click on the link. When clicked, such links open web-forms that mimic legitimate websites asking people to enter login and other credentials, which are then used to compromise individual computers and networks. In this manner, phishers obtain sensitive information from their victims and subsequently attempt to sell the information, open bank accounts, and even steal money.

Such phishing attacks are the vector of choice among cybercriminals. The Anti-Phishing Workgroup consistently discovers upwards of 40,000 unique phishing sites per month, targeting around 500 unique brands (Anti Phishing Work Group, 2014), while the Department of Defense and the Pentagon report receiving as many as 10 million phishing attacks per day. However, not every phishing attack is successful: estimates are that 30-60 percent of all phishing attacks result in victimization (Team, Verizon RISK, 2013). Thus, while many attacks are successful, some are not, perhaps due to certain features in those attacks or within the targeted individuals themselves. As such, it is plausible that variables exist within users or the content of the phishing message that cause some attacks to result in higher levels of victimization than others. To disentangle this the current research asks the following question:

RQ1. What makes certain phishing attacks more successful and certain users more susceptible than others?

Understanding what makes some attacks successful and why some users might be better at detecting than others holds the key to developing more targeted anti-phishing interventions (Harrison *et al.*, 2015; Vishwanath *et al.*, 2015).

Extant research on phishing has implicated users' cognitive processing as a key reason for individual victimization (Vishwanath *et al.*, 2011). Theoretically, many scholars use Petty and Cacioppo's (1986) Elaboration Likelihood Model (ELM) to explain how cognitive processing influences deception (e.g. Vishwanath *et al.*, 2011; Workman, 2008). None have, however, examined how persuasive factors in phishing e-mail messages, such as warnings or rewards, affect how users cognitively process the e-mail and their subsequent likelihood of victimization. Moreover, prior research has linked e-mail knowledge and experience to individual phishing victimization (Downs *et al.*, 2006; Jakobsson, 2007; Jakobsson *et al.*, 2007). However, the extent to which these factors interact with the structural features in an e-mail and influence users' cognitive processing of the e-mail also remains unexplored.

The current research therefore examines how specific persuasive aspects of phishing e-mails influence individual processing and susceptibility to phishing. To this end, the study uses a naturalistic experiment where subjects are exposed to a real phishing attack that either offers a reward or poses a threat. The ensuing sections provide a review of relevant theoretical underpinnings driving the study's research questions followed by an overview of the experiments and a discussion of findings and implications.

2. Theoretical premise

The ELM is a dual-process model that distinguishes between two ways in which individuals process information; the central processing route involves careful consideration of the information presented using comparisons and prior experience, while the peripheral processing route does not consider all elements of the message and instead relies on simple cues to make a decision regarding message veracity. This tendency to process information in different ways could affect users' attitudes, judgments, and behaviors toward a particular message (Petty and Cacioppo, 1986), resulting in varying levels of susceptibility to the persuasive material. When individuals

engage in central information processing of a message, such as a phishing e-mail, they engage in two sub-processes known and attention and elaboration (Petty and Cacioppo, 1986). The amount of attention paid by an individual is determined by the amount of mental focus they give to specific elements of the message. The resulting elaboration process occurs when individuals make connections between these elements and prior knowledge and experience.

ELM provides a useful theoretical framework for understanding the process of victimization through phishing because it allows a concurrent examination of how attention to message cues and elaboration of phishing messages can result in either resisting or succumbing to a phishing attack. It also provides a theoretical premise for examining how attention to certain cues in a phishing e-mail can affect both the nature and extent of elaboration. Upon receiving an e-mail, a user might read the sender's name, notice their e-mail address, or read the subject line (what ELM deems attention) before opening the message. In the case of illegitimate phishing e-mails, this process becomes particularly important. This initial attention may cause a particular user to feel compelled to search for further cues in the e-mail (ELM's elaboration process), connecting them to existing knowledge and perhaps ultimately coming to the conclusion that the e-mail is a scam. Conversely, other users who do not attend to the e-mail upon receipt would neglect to elaborate on the information and judge the e-mail as relevant (Jakobsson, 2007). In essence, the differences in processing in terms of users' attention and elaboration of the message ultimately lead to differences in phishing susceptibility. Of course processing is heavily contingent on the information presented in the persuasive context (Vishwanath *et al.*, 2011). Hence, we begin our exploration by examining the factors within phishing e-mail messages and how they might influence information processing.

3. Message-level factors influencing attention and elaboration

In the context of phishing, the perpetrator attempts to persuade the victim into divulging private information by constructing a message that encourages attention to certain message cues and limits the kind of elaboration that would result in deception detection. In fact, Workman (2008) argues that phishers specifically craft messages that decrease the amount of cognitive processing (i.e. elaboration) of a message. The message component of phishing e-mails tends to be brief and typically relies on urgency cues by using words like "warning" or "deadline" in conjunction with phrases such as "imminent account closure" or "unclaimed tax refund." Phishers intend for these cues to accentuate affective reactions and lead users to act quickly, bypassing more rational decision-making processes and ignoring other cues that could indicate the message source is not legitimate (Vishwanath *et al.*, 2011). For example, the presence of a threat element in the message (or fear arousal) can lead to increased acceptance of a persuasive message through its particular effect on information processing (Das *et al.*, 2003). Fear-arousing content in phishing messages may likewise affect the way in which users' process the e-mail, increasing their likelihood of ignoring the elements of the message that signal its fraudulent nature.

While many phishing attacks attempt to incite fear (e.g. by threatening that an account is about to be closed or suggesting it is compromised), others attempt to persuade users by creating a reward-based message in which the phisher offers something of value to users, such as goods or money. The infamous Nigerian scam offers a great example of a widely successful phishing attack that is based on the promise of an enticing reward. This popular scam provokes users to provide personal

and bank account details by promising a significant percentage of funds from a multimillion-dollar bank account in return for assistance in moving this large sum of money out of Nigeria.

Over three decades of research on fear appeals and media framing demonstrates how negative, fear-based information, ranging from threats, warning, and deadlines, is more salient during information processing than positive, reward-based information (Rogers, 1983; Schenck-Hamlin *et al.*, 2000). The authors therefore pose the following hypotheses regarding fear and reward-based phishing messages:

H1a. A fear-based phishing attack is more likely to result in decreased attention and decreased elaboration of the message than a reward-based attack.

H1b. A fear-based phishing attack is more likely to result in victimization than a reward-based attack.

In contrast to deliberate deception cues placed within phishing e-mail messages, deceptive messages may also contain "leakage" cues that inadvertently expose their deceptive origin and are not controlled or intended by the source of the message. In their deception research, Ekman and Friesen (1969) originally examined leakage cues in the context of nonverbal communication, defining leakage cues as "specific types of body movements and facial expressions which escape efforts to deceive" (p. 88), Such leakage cues have been found to be present in the in the computer-mediated context as well. From the reliance on "language correctness" by people assessing the veracity of dating profiles (Toma and Hancock, 2012) to the increased use of typographical errors by deceptive senders in e-mail communication (Zhou *et al.*, 2004), leakage cues prove to play in important role in the computer-mediated context. Typical leakage cues in phishing e-mails can be found in the typographical and spelling errors that betray the e-mail as one not composed by a professional organization or legitimate individual. The presence of such leakage cues could potentially result in greater attention to the message (Toma and Hancock, 2012) and reduce the victimization rate, as compared to a message that contains no such errors at all. In other words, leakage cues (i.e. typographical errors) could result in increased elaboration of the message, and a lower likelihood of getting phished. The authors therefore pose the following hypotheses:

H2a. The presence of leakage cues will result in increased attention and increased elaboration of the phishing message.

H2b. The presence of leakage cues will result in a lower likelihood of phishing victimization.

4. Individual-level variables influencing attention and elaboration

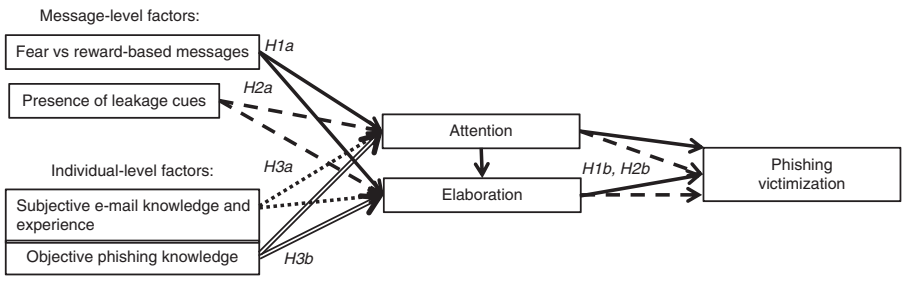
A user's processing of a message as well as their response to a phishing attack will also be influenced, in part, by their experience with and knowledge of both e-mail in general and phishing e-mails. The interpersonal deception literature places experience central to the deception-detection process, where exposure (i.e. a kind of baseline for experience) to truthful communication increases accuracy when it comes to spotting deceptive messages (Feeley *et al.*, 1995). Such experience gives users not only a cognitive schema for the kinds of messages they expect to receive, but also a set of tools with which they can judge the veracity of potentially deceptive e-mails. Further, in the phishing context, Wright and Marett (2010) found that security knowledge and web experience rendered users less prone to being deceived. While such work has made

clear the critical influence of knowledge and experience in making successful veracity judgments, the mechanism regarding how they protect users form phishing victimization remains unexplored.

It is plausible that knowledge and experience with both e-mail in general as well as with phishing-specific messages is protective because it helps users more readily spot and identify the deceptive cues within a phishing e-mail. This could therefore lead to increased likelihood of attention and elaboration of the message, leading to a decreased likelihood of phishing victimization. There is, however, a distinction between subjective knowledge and objective knowledge. The former is perception of knowledge while the latter is based on facts as an impartial assessment of one's knowledge. Consequently, subjective knowledge could be problematic if it is premised on faulty information. When it comes to information, many individuals may believe they have a wealth of knowledge but in reality have limited objective knowledge. For instance, Downs *et al.* (2006) interviewed non-expert users to determine their awareness of phishing-associated risks, their ability to recognize commonly used phishing cues, and the decision strategies they employed when faced with a phishing e-mail. The authors concluded that users simply do not have adequate objective knowledge about the risks of phishing. Likewise, Jakobsson (2007) explored users' information processing when presented with a phishing e-mail and found that individuals tend to make judgments regarding the relevance of an e-mail before assessing its authenticity. Having such faulty objective knowledge combined with high subjective knowledge could lead users to be cavalier in their treatment of e-mails and rather than protect against victimization, such knowledge could lead to increased phishing susceptibly. Dually, having faulty knowledge could cause a false sense of confidence and lead to decreased attention to and elaboration of the specific nuances in the phishing e-mail that might reveal the deception. The present study therefore seeks to examine how users' self-reported, subjective knowledge and experience with e-mail as well as their objective, phishing-specific knowledge influences information processing and phishing susceptibility by posing the following hypotheses:

H3a. Increased subjective knowledge of and experience with e-mail will lead to increased attention and increased elaboration of the phishing message.

H3b. Increased objective knowledge of and experience with phishing-specific e-mails will lead to increased attention and elaboration of the phishing message (Figure 1).



Note: Differences in trait-level technological innovativeness was controlled

Figure 1.
Proposed model

5. Methods

The study experimentally tested the process by which cognitive processing interacted with both message-level and individual-level factors to potentially influence phishing victimization. In developing the experiment, the authors considered that many studies on phishing involve participants being exposed to a series of websites or messages, after which they are required to state whether the sites are legitimate or bogus (e.g. Dhamija *et al.*, 2006; Jakobsson *et al.*, 2007). While these studies are informative, their paradigm makes the deception detection task salient, and so artificially increases the amount of cognitive processing of the message. This situation does not mirror real life where users are unlikely to scrutinize every e-mail they receive nor are they likely to expect deception by the entire contents of their e-mail inbox. The present study, thus, used a naturalistic experiment, where participants were subjected to a real-world phishing attack.

6. Participants and design

The study utilized college students at a large university in the Northeastern USA. University students were used for three reasons. First, they are a particularly vulnerable population who are often the target of phishing attacks. Colleges and universities expend significant resources in trying to protect students and educate them about phishing. Second, research evidence points to students being particularly susceptible to phishing attacks (Sheng *et al.*, 2010), perhaps because of low levels of phishing knowledge, experience, and awareness. Third, the study used an experimental methodology where the focus was on internal validity, which was made possible by the use of homogenous sample of student subjects.

Students were recruited from introductory communication courses (mean age of 20 years, 52.8 percent male). A 2×2 between-subjects experimental design was created with e-mail message type (fear vs reward based) and leakage cues (present vs not present). Participant e-mails were randomly assigned to one of these four e-mail conditions.

6.1 Stimulus material

The "phishing" e-mail constructed by the researchers mimicked the kinds of phishing attacks that had already been attempted on student populations. The fear and reward messages are shown below, respectively:

> Dear Student,
>
> A review of our records shows permanent error with your XX account. To prevent closure of your account please log in here to your account to resolve the problem.

> Dear Student,
>
> A review of our record show you have been overcharged by our system by $1210. To receive your refund, please log in here to your account and resolve the problem.

The study was conducted with the knowledge and approval of the university-based systems security department, as well as the ethics review board. A fake e-mail account using a widely available e-mail provider (gmail.com) was utilized in sending the phish e-mail. The name assigned to the e-mail account (which is what appears in the "From" field) was XXITinfo@XX.edu. Apart from this, no other attempt was made to conceal the fact that the e-mail was from a non-university e-mail provider.

7. Measures

7.1 Information processing: elaboration

At the outset of the questionnaire (prior to answering any other question) one open-ended item measured elaboration by asking participants why they did or did not respond to the phish e-mail. Consistent with prior research, response length (word count) was used as a measure capturing elaboration. Although word count is already used as a primary indicator of cognitive complexity (Abe, 2012; Dreschler, 2012), validity was further assessed by using Pennebaker *et al.*'s (2007) Linguistic Inquiry and Word Count (LIWC) program on the open-ended responses. LIWC analyzes text and compares words to a predefined set of dictionaries consisting of terms validated to be representative of different psychological dimensions (Pennebaker and Stone, 2003; Gonzales *et al.*, 2010). The analyses confirmed that the measure of elaboration was strongly related to the LIWC category of cognitive mechanisms (which measures depth of thinking; Tausczik and Pennebaker, 2010) $r = 0.304$, $p = 0.002$[1].

7.2 Information processing: attention

Accurate recall of the message elements was used as a measure of the extent of attention to e-mail elements. Participants were asked to indicate elements of the e-mail they remembered seeing. Response options included both actual features of the e-mail as well as elements that were not present. Additionally, this measure of attention made clear elements of the e-mail that were most and least attended to.

Elaboration and attention were significantly correlated with each other such that individuals who showed more elaboration of the message also showed more attention to the message elements ($r = 0.35$ $p < 0.001$, $n = 113$).

7.3 Subjective e-mail knowledge and experience

Participants' subjective knowledge and experience with e-mail were measured using seven items (e.g. I am knowledgeable about e-mail; I have experience receiving official e-mails from __IT; I am confident in my knowledge about e-mail-based scams). Participants responded on a five-point Likert-type (strongly disagree – strongly agree). Higher values indicated greater e-mail knowledge and experience. $M = 2.63$, SD = 0.61, $p = 0.83$, single factor explained 51 percent of the variance.

7.4 Objective phishing knowledge

To measure existing phishing knowledge, participants were asked to indicate the extent to which they were familiar with the term "phishing" (unfamiliar with this term/have heard the term but do not know what it means/have heard it and know a little about it/very familiar and know what it means). A minority (33.6 percent) of the sample indicated they were very familiar with phishing and knew what it meant. Because of the absence of an a priori scale specifically designed to estimate phishing knowledge among college students, a 12-question measure was developed. Each item stated a characteristic of an e-mail (e.g. asks for personal information) and asked participants to indicate the extent to which it was characteristic of a phishing e-mail, using a five-point scale. Seven items tapped into the actual phishing knowledge construct (e.g. asks me to verify my password; has links embedded in the e-mail) while the other five were distractor items. The seven correct items formed one principal factor ($a = 0.87$). For the purposes of analysis, a weighted phishing-specific knowledge score was calculated. This was composed of the seven items related to phishing, minus a $0.5 \times$ non-phishing specific items; $M = 8.73$, SD = 3.80.

7.5 Control measure: individual personality-based technological innovativeness

While college students tend to be relatively homogenous on socio-economic levels, they tend to differ in technological innovativeness (Vishwanath, 2004). Innovativeness is defined as the degree to which individuals are relatively earlier in adopting a technological innovation than others within their social system (Rogers, 1995). Users with high technological innovativeness often have increased knowledge, efficacy, and experience with technology (Vishwanath, 2004), which likely influences how aware they are about phishing attacks. Because the focus of the current study is cognitive processing of phishing e-mails in reaction to specific message elements, contextual trait-level factors are outside the scope of the study. Consequently, it is imperative that any undue variance or noise caused by this trait is reduced. The authors therefore statistically controlled for innovativeness by measuring the construct using an abbreviated three-item scale was that measured the extent to which users were early adopters of technology (Vishwanath, 2004: If I heard of a new software, I would be interested enough to buy it; I know about most technology products before other people do and I will buy a new computer software even if I don't know much about it; $M = 1.71$, SD = 0.71, $a = 0.72$)

8. Procedure

Participants provided their e-mail address in an online sign-up sheet. Each address was randomly assigned to one of the four e-mail conditions such that roughly equal numbers of participant addresses would be in each e-mail group. The phish e-mail was sent two weeks after participants gave their e-mail addresses so that the two events were not associated with one another. Participants received one of four possible e-mail messages simultaneously.

Once clicked on, the hyperlink within the phishing e-mail directed subjects to the phish form page. The page was designed to be an unsophisticated form page, which made a minimal visual attempt to look like a university site but made no attempt to conceal the host domain (not a university site). The page prompted visitors to enter their university e-mail login and password. The data were collected through a web survey operating via an encrypted link, preventing third parties and illegitimate intercepts of the participants' responses. The authors deleted password data entered by participants, retaining only records of the e-mail addresses of those who entered form data. This allowed for an experimental count of the success of the experimental phish. Once subjects clicked on the "login" button on the form page, they were redirected to a debriefing page that explained the nature of the experiment and invited them to participate in the post-experimental survey.

Subjects who did not respond to the phishing e-mail within 24 hours were sent a second e-mail that debriefed them as to the nature of the e-mail and provided a direct link to the post-experimental survey. The data from the phished and non-phished participants therefore composed one continuous data set. E-mail use among undergraduate students has always been high, but with the proliferation of laptops and hand-held devices, the overwhelming majority of college students use e-mail at least once a day (Smith and Borreson Caruso, 2010). Therefore, the assumption was made that a nonresponse by any participant within 24 hours indicated our phishing attempt was unsuccessful.

9. Results

The victimization rate obtained from the experiment was consistent with other studies using simulated phishing attacks (Team, Verizon RISK, 2013): 91 subjects (47 percent of the initial list) clicked on the experimental phishing link and provided their login information within five hours of sending the experimental phish e-mail.

9.1 Manipulation checks and general recall

Several manipulations were performed to confirm that the different experimental groups were indeed exposed to and remembered different message elements. For the experimental groups who were sent the fear-based message (an account error warning), 51 percent recall seeing the threat. By contrast, only 10 percent of the non fear-based groups indicated seeing an account error warning. Of the non fear-based group, 53 percent recall seeing the account overcharge element that characterized their e-mail, while 0 percent of the fear-based group recalled seeing this element. The authors therefore conclude that the manipulation was successful.

Table I shows the rates at which each element we included was noticed by our sample. Only 5 percent of the sample actually noticed the source of the e-mail was a Gmail address, in contrast to 37 percent who stated that it came from the university-based e-mail system. Furthermore, as Table I indicates, no individual in the error conditions noticed the typographical errors inserted in the messages.

9.2 Message and individual influences on processing

A multiple linear regression was utilized to examine the effect of both message and individual influences on elaboration and attention (*H1a*, *H2a*, *H3a*, and *H3b*). Next, a stepwise multiple regression was used where the two message factors (fear vs reward and leakage cues vs no leakage cues) were entered in the first block, and the individual factors (subjective e-mail knowledge, objective phishing knowledge, and innovativeness) were entered in the second block as predictors of elaboration and attention. Residuals for both the attention and elaboration measures were normally distributed, plots of predicted values with standardized residuals showed homoscedasticity, and there was no indication of collinearity[2].

9.2.1 Elaboration. Results indicated that neither the fear vs reward message variable nor the presence of leakage cues influenced the extent of elaboration, therefore support was not found for *H1a* and *H2a* [3]. However, elaboration was predicted by the knowledge variables, specifically subjective e-mail knowledge and experience, and objective phishing-specific knowledge. The research therefore found significant support for *H3a* and *H3b*. Table II presents the regression results and standardized coefficients.

Thus elaboration was unaffected by the manipulated message factors but was predicted by both subjective and objective domain-specific knowledge when it comes to incoming e-mails. Note, however, that while the addition of the knowledge variables resulted in a significant omnibus model, neither the subjective measure of e-mail knowledge and experience nor our objective measure of phishing knowledge were individually significant predictors of elaboration.

E-mail element	% of sample that recall the element
University logo	41.6
IT department phone number	54.0
IT department signature	37.2
Hyperlink	46.0
University e-mail source address	38.9
Gmail source address	6.2

Notes: $n = 113$. While we had data on the phish success for 194 participants, the following results are based on a sample of students who both completed the survey and were retained after data cleaning and checking for completeness. Each of the above e-mail elements appeared in every experimental condition

Table I.
Recall rates for elements included in the e-mail

			Correlations	
Predictors	β	p	Partial	Semi-partial
Threat vs gain in message (threat = 1, gain = 0)	0.133		0.133	0.132
Typogr. errors in message vs no errors (errors = 1, no errors = 0)	−0.063		−0.162	−0.150
E-mail knowledge and experience	0.233	0.060	0.224	0.211
Phishing-specific knowledge	0.228	0.064	0.221	0.208
Innovativeness	0.254		0.010	0.010
Model test	R	p		
Block 1	0.151			
Block 2	0.402	0.030		
	R^2 Δ = 0.139	0.014		

Table II.
Results of a regression analysis predicting elaboration from message and individual factors

Notes: $n = 75$. The β column represents standardized regression weights in the final (Block 2) model. Collinearity analysis showed for all the predictors tolerance to be ≥ 0.816 and variance inflation factor ≤ 1.225. Significance is indicated exact p-value for all values of $p < 0.05$

9.2.2 Attention. Concurrent with the above analysis on elaboration, message factors did not affect the extent of attention to the phishing e-mail (*H1a* and *H2a*). However, the addition of the individual-level variables resulted in a significant improvement to the model. The only significant individual predictor was objective phishing knowledge (*H3b*), which was associated with more attention to the e-mail. See Table III for attention regression results.

What is clear from the preceding analyses is that the message factors that were manipulated did not influence the amount of attention to the phishing message, or how much users elaborated. However, individual factors were predictive in that users higher in knowledge and experience were more likely to show increased attention and elaboration of the incoming phishing e-mail. Specifically, user's objective phishing-specific knowledge was most likely to predict increased attention to the e-mail.

The fact that the message factors that were manipulated did not affect processing does not mean message cues play no role. It is important not to assume that merely because a cue was present in the message, it also influenced processing. A more

			Correlations	
Predictors	β	p	Partial	Semi-partial
Threat vs gain in message (TH)	−0.008		−0.008	−0.008
Typogr. errors in message vs no errors (ER)	−0.009		−0.009	−0.008
E-mail knowledge and experience (EK)	0.065		0.062	0.058
Phishing-specific knowledge (PK)	0.283*	0.025	0.266	0.258
Innovativeness (IN)	−0.215	0.069	−0.217	−0.208
Model Test	R	p		
Block 1	0.088			
Block 2	0.353	0.094		
	R^2 Δ = 0.177	0.033		

Table III.
Results of a regression analysis predicting attention from message and individual factors

Notes: $n = 75$. The β column represents standardized regression weights in the final (Block 2) model. Collinearity analysis showed for all the predictors tolerance to be ≥ 0.816 and variance inflation factor ≤ 1.225. Significance is indicated by $^*p < 0.05$, as well as exact p-value for all values of $p < 0.1$

complete analysis requires examining the way in which attending to different elements of the phishing message affects the extent of subsequent elaboration. This analysis enabled the authors to better link attention to subsequent elaboration by understanding how attention to initial cues can influence the extent to which subjects used elaboration in their e-mail response decision process.

For the subsequent OLS regression, we used participants' indications as to whether they saw certain elements of the message as binary predictor variables for the extent of elaboration. The regression results reveal that attending to certain cues in the phishing message predict the extent of subsequent elaboration. Specifically, individuals who noticed the bogus source address, the hyperlink and the IT signature line were significantly more likely to exhibit increased elaboration. In contrast, elaboration was inhibited in individuals who reported seeing "a chance to earn money" in the message. This result is particularly interesting because the reward message manipulation stated that the individual's account was overcharged and would be refunded, whereas the "chance to earn money" was a distractor item. Those who (correctly) noticed seeing an account overcharge did not exhibit less elaboration, yet those who incorrectly remembered it as "a chance to earn money" did. These results are preliminary evidence that the same message cue can be processed and interpreted differently by users, which in turn influences the extent to which users elaborate the message. See Table IV for regression results.

9.3 Message and processing determinants of phishing susceptibility

The last stage in our analysis was to examine how message factors, elaboration, and attention predict succumbing to a phishing attack (*H1b* and *H2b*). A binary logistic regression was performed where being phished or not phished was the outcome to be predicted. The independent variables in the first block were: the categorical fear vs reward message variable[4], (the message containing leakage cues was excluded given that no individual reported noticing the error), the measure of elaboration (response length, mean centered), and the measure of attention (the number of items recalled, corrected for erroneous recall and mean centered). The omnibus model was statistically

			Correlations	
Predictors	β	p	Partial	Semi-partial
Hyperlink	0.276*	0.008	0.267	0.234
University IT dept signature	0.216*	0.023	0.230	0.200
University IT dept phone number	−0.058		−0.056	−0.047
Bogus (Gmail) source address	0.363*	0.000	0.365	0.331
University (.edu) source address	−0.018		−0.019	−0.016
Account overcharge	0.165	0.081	0.178	0.153
Account error warning	−0.215		−0.095	−0.080
Chance to earn money	−0.266*	0.007	−0.272	−0.239
Model test	R	p		
	0.535	0.000		
	$R^2 = 0.287$			

Notes: $n = 103$. The β column represents standardized regression weights. All the predictor variables are binary (where 1 = cue is recalled); collinearity analysis showed for all the predictors tolerance to be $\geqslant 0.665$ and variance inflation factor $\leqslant 1.504$. Significance is indicated by $*p < 0.05$, as well as exact p-value for all values of $p < 0.1$

Table IV. Results of a regression analysis predicting elaboration from attention to specific message cues

significant χ^2 (df = 3) = 7.85, $p = 0.05$, with both attention and elaboration as significant individual predictors. See Table V for standardized coefficients and Table VI for estimates of sensitivity and specificity.

Moreover, both elaboration and attention was associated with a lower overall likelihood of being phished. The interaction between elaboration and attention was added in the second block, significantly improving the predictive ability of the model, χ^2 (df = 4) = 13.08; $p = 0.01$, and emerging as significant predictor of whether an individual was phished or not (elaboration and attention were individually no longer significant predictors). See Table VII for correlations among the variables.

The interaction between attention and elaboration was examined using the PROCESS macro (Hayes and Matthes, 2009), which estimates the effect of the focal variable (in this case elaboration) at different levels of the moderating variable

Table V.
Results of a logistic regression analysis predicting being phished

	β	Exp(B)	Wald's χ^2	df	p	−2 log likelihood
Predictors						
Threat vs gain in message (TH)						
(1 = threat, 0 = gain)	−0.157	0.855	0.127	1		
Elaboration (EL)	−0.030	0.970	1.935	1		
Attention (AT)	0.234	1.264	2.380	1		
		1.170	0.127	1		
EL × AT	−0.030*	0.971	4.747	1	0.029	
Model test						
Block 1			7.750	3	0.049	127.851
Block 2			13.081	4	0.011	122.620
Goodness of fit test (Hosmer-Lemeshow)			6.401	8	0.602	

Notes: $n = 113$. The β column represents standardized regression weights in the final (Block 2) model. Significance is indicated by $*p < 0.05$, as well as exact p for all values of $p < 0.1$

Table VI.
Observed and predicted frequencies for phishing susceptibility

	Predicted		
Observed	Phished	Not phished	% correct
Phished	56	7	88.9
Not phished	25	14	35.9
Overall % correct			68.6

Notes: Sensitivity = 56/(56 + 7) = 88.89 percent. Specificity = 14/(14 + 25) = 35.90 percent. False positive = 25/(25 + 56) = 30.86 percent. False negative = 7/(7 + 14) = 33.33 percent

Table VII.
Correlation matrix of predictor variables used in analyses

	2	3	4	5
1. Elaboration	0.243**	0.302**	0.213	0.010
2. Attention		0.110	0.312*	−0.203
3. E-mail knowledge and experience			0.366**	0.203
4. Phishing-specific knowledge				0.062
5. Innovativeness				

Notes: Correlations calculated using Spearman's ρ. Significance is indicated by $*p < 0.05$; $**p < 0.01$

(in this case attention). The output revealed that the negative effect of elaboration on likelihood of being phished was stronger at higher levels of attention. In other words, elaboration is protective of phishing susceptibility when users process and pay attention to the e-mail elements themselves.

The naturalistic experiment reported in this study obtained a 47 percent phishing success rate, enabling an adequate comparison between individuals who are more susceptible to phishing and those who are relatively unaffected by it. This analysis attempted to clarify what determines susceptibility to phishing and by doing so determine how and if it is possible to build resilience to phishing. With respect to the study's hypotheses, the research found that susceptibility to phishing, and the mechanism by which phishing succeeds is explained by the extent of attention to, and elaboration of, the phishing message by the recipient, and that these in turn are affected by both an individual's personal and knowledge-based attributes.

Specifically, susceptibility to phishing is predicted by high levels of attention to a message but with less subsequent elaboration, therefore finding partial support for *H1b* and *H2b*. Those who are most likely to get phished exhibit both increased initial attention to the phishing message and insufficient subsequent elaboration as to whether to respond or not. Phishing susceptibility is thus a function of being immersed in the e-mail, yet without sufficient consideration of its meaning and viability in a larger context. Resilience to getting phished, on the other hand, is predicted by low initial levels of attention to a phishing message, followed by elaboration as to whether to respond. This finding also aligns with other research that examines dual processes in effective decision making (Dijksterhuis *et al.*, 2006; Evans, 2008; Reyna, 2004). Individuals who did not get phished managed to both conserve cognitive resources when initially attending to the message, but then mobilize their knowledge of both phishing and e-mail to elaborate on whether a response is required. Put differently, greater knowledge also means that less attention resources are required in order to trigger expertise.

Further, evidence was obtained that implicates a few key cues in the message that influence elaboration. Individuals who noticed the Gmail source address (the main clue to the message's illegitimate nature) signature and hyperlink exhibited significantly higher levels of subsequent elaboration. Although the fear vs reward message manipulation did not affect elaboration, the manner in which individuals interpreted the "gain" message did. Those who saw it as a chance to earn money showed lower subsequent elaboration. Thus, not only can different cues affect elaboration, but the same message cue can also have different effects on elaboration depending on how it is initially interpreted by the user.

10. Implications

These findings not only inform how information processing affects decision making in a general sense, but they also hold implications for how we approach the development of more effective educational efforts to protect individuals from these types of online fraud. For example, it is clear from the data that increased attention to the e-mail is not associated with phishing resilience, and that instructing individuals to more closely examine incoming e-mail messages may not be an effective strategy. In fact, research to-date has found that attempts to specifically educate consumers about phishing is only making them generally and temporarily more suspicious. Jackson *et al.* (2007) found that the "help" file on phishing simply made participants more likely to categorize both real and fake sites as phishing, while Anandpara *et al.* (2007) found that phishing education simply increased people's suspicion, without fine-tuning their ability.

The current study complements these findings by showing that those who more closely attend to a phishing e-mail do not necessarily end up making the right choice.

Consequently, anti-phishing efforts should focus more on refining the quality of initial attention to the e-mail. This can be enhanced by teaching users to pay attention to just a few key elements in the message, such as knowing where to find the actual address that the e-mail was sent from and noticing red flag elements such as a hyperlink. There are some cues, on the other hand, which would be less effective as target cues. Our message manipulation including typographical/spelling errors (leakage cues) went completely unnoticed and subsequently did not affect either processing or susceptibility to getting phished. Online security professionals and educators may wonder why phishing attacks are at all successful given the relative lack of written sophistication and the seemingly obvious cues to their illegitimate origin. The present study provides evidence for why phishers may not take great care incorrectly constructing their message – because these factors remain largely unnoticed. Thus, although spelling and grammar are legitimate phishing detection cues, instructing users to look for them may impede the kind of attention processes that are most effective in determining the legitimacy of a particular e-mail.

The study's findings also show that elaboration of the message was greater in individuals who had increased experience and a more global understanding of e-mail, including the kinds of e-mail that can be expected from institutions, as well as knowledge about e-mail scams. This means that more frequent exposure and familiarity with an organization's e-mails and e-mail system can help individuals spot when an e-mail is not legitimate. For example, one non-phished student wrote: The English in the actual e-mail threw me off as it did not sound like something _____IT would send out. Also the webpage it took me to looked extremely sketch [sic] and I did not want to provide my user information at that point. These results thus align with current deception research, which finds that deception detection in an interpersonal setting is not a matter of attending to specific behaviors or words, but to the person's behavior in the context of the situation and in relation to how they normally behave (Buller and Burgoon, 1996; Ekman, 1985; Feeley *et al.*, 1995).

Although the present work provides initial evidence as to how attending to certain message elements is related to the extent of subsequent elaboration, future theoretically driven research in phishing could experimentally examine different facets of attention and elaboration, including time spent reading the e-mail, and the sequence in which message elements are noticed and recalled. This can be achieved through free recall by the individual, a thinking aloud procedure as they are presented with the message, or even eye tracking software that can record which areas of the screen are attended to first. Further, while the study population of students provides a homogeneous sample of e-mail users, future work would benefit from the use of other relevant subject groups such as employees within an organization or an older population who may have less e-mail and phishing knowledge.

11. Conclusions

Overall, the present study first finds evidence that susceptibility to phishing is supported by an information processing style wherein individuals pay more attention to its elements, yet show decreased levels of subsequent elaboration as to whether to respond or not. Second, attention to and elaboration of phishing messages are predicted by broader, individual factors related to e-mail knowledge and experience. These dual

findings dispel some of the common conceptions of why and how phishing is successful and provide greater understanding of the human factor in susceptibility to online deception. Finally, they provide a theoretically and empirically informed account of where educational efforts and interventions need to be targeted, so as to provide protection to individuals and online economies.

Notes

1. The possibility that longer responses may simple contain more filler words and excess verbiage was also tested. The LIWC analysis found that only 4/113 participants (3.5 percent) used any filler words at all.
2. $\text{Durbin-Watson}_{\text{elaboration}} = 1.80$ $\text{Durbin-Watson}_{\text{attention}} = 1.41$. Collinearity statistics for predictor variables are included in Tables II and III.
3. All the analyses, including the interaction between error and threat, were initially run. The interaction term was always nonsignificant and thus excluded from the final models.
4. This was tested to determine what direct effect it may have on phishing susceptibility.

References

Abe, J.A.A. (2012), "Cognitive-affective styles associated with position on war", *Journal of Language and Social Psychology*, Vol. 31 No. 2, pp. 212-222.

Anandpara, V., Dingman, A., Jakobsson, M., Liu., D. and Roinestead, D. (2007), "Phishing IQ tests measure fear, not ability", *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security, Heidelberg and Berlin*, pp. 362-366.

Anti Phishing Work Group (2014), "Phishing activity trends report", 2nd Quarter, APWG, San Francisco, CA, available at: www.apwg.org (accessed January 2015).

Buller, D.B. and Burgoon, J.K. (1996), "Interpersonal deception theory", *Communication Theory*, Vol. 6 No. 3, pp. 203-242.

Das, E.H.H.J., de Wit, J.B.F. and Stroebe, W. (2003), "Fear appeal motivate acceptance of action recommendation: evidence for a positive bias in the processing of persuasive messages", *Personality and Social Psychology Bulletin*, Vol. 29 No. 5, pp. 650-664.

Dhamija, R., Tygar, J.D. and Hearst, M. (2006), "Why phishing works", *Proceedings of Conference on Human Factors in Computing Systems, Montreal*, pp. 581-590.

Dijksterhuis, A., Bos, M.W., Nordgren, L.F. and van Baaren, R.B. (2006), "On making the right choice: the deliberation-without-attention effect", *Science*, Vol. 311 No. 5763, pp. 1005-1007.

Downs, J., Holbrook, M. and Cranor, L. (2006), "Decision strategies and susceptibility to phishing", *Symposium on Usable Privacy and Security, Pittsburgh, PA*.

Dreschler, G. (2012), "One language, two grammars? Differences between British and American English", *English Studies*, Vol. 93 No. 2, pp. 244-246.

Ekman, P. (1985), *Telling Lies: Clues to Deceit in the Marketplace, Marriage, and Politics*, W.W. Norton, New York, NY.

Ekman, P. and Friesen, W.V. (1969), "Nonverbal leakage and cues to deception", *Psychiatry*, Vol. 32 No. 1, pp. 88-105.

Evans, J.S.B. (2008), "Dual-processing accounts of reasoning, judgement and social cognition", *Annual Review of Psychology*, Vol. 59, pp. 255-278.

Feeley, T.H., deTurck, M.A. and Young, M.J. (1995), "Baseline familiarity in lie detection", *Communication Research Reports*, Vol. 12 No. 2, pp. 160-169.

Gonzales, A.L., Hancock, J.T. and Pennebaker, J.W. (2010), "Language style matching as a predictor of social dynamics in small groups", *Communication Research*, Vol. 37 No. 1, pp. 3-19.

Harrison, B., Vishwanath, A., Yu, J. Ng and Rao, R. (2015), "Examining the impact of presence on individual phishing victimization", *48th Hawaii International Conference on System Sciences (HICSS), January 5-8*, pp. 3483-3489. doi: 0.1109/HICSS.2015.419.

Hayes, A.F. and Matthes, J. (2009), "Computational procedures for probing interactions in OLS and logistic regression: SPSS and SAS implementations", *Behavior Research Methods*, Vol. 41 No. 3, pp. 924-936.

Jackson, C., Simon, D.R., Tan, D.S. and Barth, A. (2007), "An evaluation of extended validation and picture-in-picture phishing attacks", in Ditrich, S. and Dhamija, R.R. (Eds), *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, New York, NY, pp. 281-293.

Jakobsson, M. (2007), "The human factor in phishing", *Privacy & Security of Consumer Information*, Vol. 7 No. 1, pp. 1-19.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E. and Lim, Y. (2007), "What instills trust? A qualitative study of phishing", in Ditrich, S. and Dhamija, R.R. (Eds), *Financial Cryptography and Data Security: Lecture Notes in Computer Science, Volume 4886*, Springer Berlin Heidelberg, New York, NY, pp. 356-361.

Pennebaker, J.W. and Stone, L.D. (2003), "Words of wisdom: language use over the lifespan", *Journal of Personality and Social Psychology*, Vol. 85 No. 2, pp. 291-301.

Pennebaker, J.W., Booth, R.J. and Francis, M.E. (2007), *Linguistic Inquiry and Word Count (LIWC2001)*, LIWC.net, Austin, TX.

Petty, R.E. and Cacioppo, J.T. (1986), "The elaboration likelihood model of persuasion", in Berkowitz, L. (Ed.), *Advances in Experimental Social Psychology*, Vol 19, Academic Press, New York, NY, pp. 123-205.

Reyna, V.F. (2004), "How people make decisions that involve risk: a dual-processes approach", *Current Directions in Psychological Science*, Vol. 13 No. 2, pp. 60-66.

Rogers, E.M. (1995), *Diffusion of Innovations*, Simon and Schuster, New York, NY, p. 12.

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation", in Cacioppo, J. and Petty, R. (Eds), *Social Psychophysiology*, Guilford, New York, NY, pp. 153-176.

Schenck-Hamlin, W.J., Procter, D.E. and Rumsey, D.J. (2000), "The influence of negative advertising frames on political cynicism and politician accountability", *Human Communication Research*, Vol. 26 No. 1, pp. 53-74.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010), "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM*, pp. 373-382.

Smith, S.D. and Caruso, J.B. (2010), *The ECAR Study of Undergraduate Students and Information Technology*, Educause, CO.

Tausczik, Y.R. and Pennebaker, J.W. (2010), "The psychological meaning of words: LIWC and computerized text analysis methods", *Journal of Language and Social Psychology*, Vol. 29 No. 1, pp. 24-54.

Team, Verizon RISK (2013), "Verizon 2013 data breach investigations report", available at: www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (accessed June 25, 2014).

Toma, C.L. and Hancock, J.T. (2012), "What lies beneath: the linguistic traces of deception in online dating profiles", *Journal of Communication*, Vol. 62 No. 1, pp. 78-97.

Vishwanath, A. (2004), "Impact of personality on technology adoption: an empirical model", *Journal of the American Society for Information Science and Technology*, Vol. 56 No. 8, pp. 803-811.

Vishwanath, A., Harrison, B. and Ng, Y.J. (2015), "Suspicion, cognition, automaticity model (SCAM) of phishing susceptibility", presented at the Annual Meeting of 65th International Communication Association Conference, San Juan.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011), "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model", *Decision Support Systems*, Vol. 51 No. 3, pp. 576-586.

Workman, M. (2008), "A test of intervention for security threats from social engineering", *Information Management & Computer Security*, Vol. 16 No. 5, pp. 463-483.

Wright, R. and Marett, K. (2010), "The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived", *Journal of Management Information Systems*, Vol. 27 No. 1, pp. 273-303.

Zhou, L., Burgoon, J.K., Nunamaker, J.F. and Twitchell, D. (2004), "Automating linguistics-based cues for detecting deception in asynchronous computer-mediated communications", *Group Decision and Negotiation*, Vol. 13 No. 1, pp. 81-106.

Further reading

Hale, J.L., Lemieux, R. and Mongeau, P.A. (1995), "Cognitive processing of fear-arousing message content", *Communication Research*, Vol. 22 No. 4, pp. 459-474.

Petty, R.E. and Jarvis, W.B.G. (1996), "An individual differences perspective on assessing cognitive processes", in Schwarz, N. and Sudman, S. (Eds), *Answering Questions: Methodology for Determining Cognitive and Communicative Processes in Survey Research*, Jossey-Bass, San Francisco, CA, pp. 221-257.

Corresponding author

Arun Vishwanath can be contacted at: avishy@buffalo.edu