Decision Support Systems 51 (2011) 576–586

Contents lists available at ScienceDirect

Decision Support Systems

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

Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model

Arun Vishwanath [a,*], Tejaswini Herath [b], Rui Chen [c], Jingguo Wang [d], H. Raghav Rao [e]

[a] Department of Communication, Management Science and Systems, 333 Lord Christopher Baldy Hall, State University of New York at Buffalo, Buffalo, NY 14260, United States
[b] Department of Finance, Operations and Information Systems, Brock University, Canada
[c] Department of Information Systems and Operations Management, Ball State University, United States
[d] Department of Information Systems and Operations Management, University of Texas at Arlington, United States
[e] Management Science and Systems, State University of New York at Buffalo, United States

ARTICLE INFO

Article history:
Received 23 July 2010
Received in revised form 28 December 2010
Accepted 6 March 2011
Available online 11 March 2011

Keywords:
Social engineering
Phishing
Phishing vulnerability
Information processing
Message cues
Attention
Elaboration

ABSTRACT

This research presents an integrated information processing model of phishing susceptibility grounded in the prior research in information process and interpersonal deception. We refine and validate the model using a sample of intended victims of an actual phishing attack. The data provides strong support for the model's theoretical structure and causative sequence. Overall, the model explains close to 50% of the variance in individual phishing susceptibility. The results indicate that most phishing emails are peripherally processed and individuals make decisions based on simple cues embedded in the email. Interestingly, urgency cues in the email stimulated increased information processing thereby short circuiting the resources available for attending to other cues that could potentially help detect the deception. Additionally, the findings suggest that habitual patterns of media use combined with high levels of email load have a strong and significant influence on individuals' likelihood to be phished. Consistent with social cognitive theory, computer self-efficacy was found to significantly influence elaboration, but its influence was diminished by domain specific-knowledge.

1. Introduction

Phishing is an email based deception where a perpetrator (phisher) camouflages emails to appear as a legitimate request for personal and sensitive information (Bose et al. 2007; Bose et al. 2008a; Bose et al. 2008b) [8–10]. Phishers use social engineering techniques such as using the names of credible businesses (American Express, eBay), government institutions (Internal Revenue Service, Department of Motor Vehicles), or current events (political donations, Beijing Olympic tickets, aiding Katrina victims) in conjunction with statements invoking fear, threat, excitement, or urgency, to persuade people to respond (Wang et al. 2009) [45]. In the last few years such attacks have increased in frequency and sophistication. The antiphishing workgroup (2008) reports that for the year 2008, there were over 85,630 unique phishing reports with 81,215 new unique phishing sites. A recent Gartner report notes that nearly 11 million online adults – representing about 19% of those attacked – may have clicked on the link in a phishing attack email (Litan 2004) [34]. Because phishing scams are sent to thousands of customers, even a 2–3% success rate can be financially costly. A study by Gartner group estimated the losses in 2003 to be $1.2B (Litan 2004) [34]. In addition to the monetary impact, phishing is likely to erode consumer trust in online security and payment systems. This distrust increases consumer resistance towards online communication, and increases the cost of doing business online (Belanger et al. 2006; Belanger et al. 2002; Gupta et al. 2004; McNall et al. 2007) [6,7,23,37]. With the growing popularity of electronic commerce, researchers have estimated the losses to exceed US$1 trillion globally (Bose et al. 2008a) [8].

A growing body of research has begun to explore ways to shield individuals from getting phished. The overall body of work takes one of two approaches. One approach, emanating from the computer sciences, focuses on engineering technological fixes that automatically detect phishing emails and either inhibit such emails from entering an individual's in-box (e.g., (Kamaraguru et al. 2006) [30] or alert individuals about the deception (Kamaraguru et al. 2006) [30]. While such research is noteworthy, past experience suggests that technology alone does not provide adequate protections especially because phishers tend to evolve with the technology and improve their baiting techniques. Some examples of this evolution are recent scams called spear phishing that target specific victims such as CEOs and high net worth individuals, and puddle phishing that target smaller regional bank and credit union customers. In such cases, the phisher creates sophisticated and personalized emails that overcome technology based screeners.

The other approach, taken by social scientists, is to study the individual or the potential victim and understand why they respond

* Corresponding author. Tel.: +1 716 6451163; fax: +1 716 6452086.
E-mail addresses: avishy@buffalo.edu (A. Vishwanath), teju.herath@brocku.ca (T. Herath), rchen3@bsu.edu (R. Chen), jwang@uta.edu (J. Wang), mgmtrao@buffalo.edu (H.R. Rao).

0167-9236/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2011.03.002

to phishing emails. Here, some researchers focus on the elements of the email that communicate trust, credibility, and authenticity (e.g., (Jakobsson 2007) [27]. Others focus on the individual victims and how they process deceptive online information (e.g., (Grazioli 2004) [22]. Some others extend theories from consumer behavior, persuasion, and market research to understand why some individuals get victimized by social engineering threats (e.g., (Workman 2007) [46]. Each stream of research, however, focuses on a single set of causative factors while controlling for others. Missing from the literature is a single comprehensive model that simultaneously tests how individuals evaluate and process phishing emails, elements of the email that are attended to, individual level factors that manifest the cognitive evaluation process, and how this evaluation, in-turn, affects the individuals phishing susceptibility.

In the present study, by proposing an integrated information processing model of phishing susceptibility, we argue that contextual factors influence phishing susceptibility indirectly by influencing information processing activities. In other words, the influence of cognitive and information processing activities on phishing susceptibility are tempered by the individuals levels of motivation, their personality based beliefs, their prior knowledge, and their day-to-day experiences. Thus, the research model provides an overarching theoretically driven structure to compare and contrast the influence of the key factors thought to influence phishing susceptibility. The integrated model is tested using structural equation modeling on a sample of intended victims of an actual phishing email that occurred at a major university in northeast USA. This study was conducted to take advantage of a natural event where the phishing attacks were real, with the attacking e-mails crafted by attackers and targeted towards a general university population with a purpose to harvest university user account and password. The model is then validated using another sample of intended victims, thereby providing confirmatory evidence of its conceptual usefulness.

The manuscript is organized as follows: The following section presents the theoretical approaches taken by prior research on phishing. Next we develop the research model. The third section details the methodology, measures and procedures used to test the model followed by the section that presents the results. The last section presents the discussion, conclusions and implications of this research to both practice and theory.

2. Background and prior literature

This research evaluates the decision making involved in processing deceptive phishing emails. As Downs et al. (2006a) [17] argue, if we want to develop tools that will be effective in combating phishing schemes, we first must know how and why people fall for them. In this section we summarize the recent publications that explore how individual online users process and detect phishing attacks (Table 1).

Prior literature that explores how individual online users detect phishing attacks has predominantly adopted descriptive analyses (Downs et al. 2006b; Jagatic et al. 2007a; Jakobsson et al. 2007; Karakasiliotis et al. 2006; Tsow et al. 2007) [18,25,31,44] with a few exceptions (Downs et al. 2007; Workman 2008) [19,47]. The majority of studies explore the general decision strategies that online users adopt in phishing detection (Downs et al. 2006a; Jakobsson et al. 2007; Tsow et al. 2007) [17,27,44]. These studies discuss the stimulus such as source of email, grammar and spelling, and email title. They however do not consider the potential roles of individual attributes (e.g., involvement, knowledge, and self-efficacy) with respect to how they affect phishing detection. A few studies have started examining the direct impacts of individual attributes on phishing detection success. The attributes that have been explored include gender (Dhamija et al. 2006) [16], phishing knowledge (Dhamija et al. 2006; Downs et al. 2007) [16,19], sender familiarity (Jagatic et al. 2007a) [25] and personality traits (Workman 2008) [47].

While this emerging body of research has expanded our understanding of online deception, there remain a number of important questions and assumptions that are unanswered. First, much of this research assumes that phishing emails are processed peripherally. Yet, how peripheral information processing ultimately influences the individuals' susceptibility to phishing based deception remains unclear. Second, research on the structural elements of phishing emails has found that individuals focus more on certain elements of these emails. Jakobsson (2007) [26] found that when subjects were asked to identify deceptive elements of phishing emails, the most important aspect they noted was spelling, grammar, and design, followed by the source of the message (URL, reply-to address). Follow-up research to-date has yet to pinpoint how these features interact with individual information processing goals or influence individual susceptibility. Finally, each study focuses on the direct effects of a different set of causative factors.

Further, the focus on one causative factor exclusively over another also ignores their combined effects (Barkhi 2002; Barkhi et al. 2007) [4,5]. It is possible, for instance, that some individuals, while they might have a personality that makes them susceptible to responding to phishing emails, are more involved in the processing of phishing emails and thereby better at detecting such attacks. It is also possible that some individuals elaborately process emails but do not have sufficient domain-specific knowledge to make an informed decision about the email.

Combining different factors into a single model would, therefore, provide a comprehensive, clearer view of the phishing deception process. A combined model would not only allow us to account for the

Table 1
Summary of prior literature.

Example publications	Research methodology	Major findings
Workman 2007 [46]	Questionnaire & onsite observation	Reveals the use of social engineering tactics such as commitment, reciprocation, and social proof within phishing attacks. Use OLS to validate their individual impacts to deceive online users.
Karakasiliotis et al 2006 [31]	Questionnaire	Explore the judgment criteria adopted by online users to detect phishing scams. Descriptive results show the impacts of visual factors, technical cues, and content characteristics on end user evaluation of suspicious emails
Jakobsson et al 2007 [27]	Lab experiment and interview	Qualitatively analyze how end users evaluate the various trust indicators (e.g., layout, legal disclaimer, and third party endorsements) in phishing email and web pages.
Tsow and Jakobsson 2007 [44]	Lab experiment	Explore the role of physical designs of stimulus. Use end user rating to examine how individuals respond differently to the variances in stimulus design when they judge phishing attacks
Jagatic et al 2007 [25]	Lab experiment	Test the effects of context-specific phishing attacks. Results show emails appear to come from friends produce a high victimization rate
Downs et al 2006a [17]	Interview	Follow mental models approach to interview average users and learn their decision making strategies in judging suspicious emails.
Downs et al 2007[19]	Interview	Explore the factors that are associated with falling for phishing attacks. The data suggests that deeper understanding of the web environment reduces vulnerability.
Dhamija et al 2006 [16]	Experiment	Provide empirical evidence of what malicious strategies are successful at deceiving online users. Results show that the standard security indicators are not effective for a substantial fraction of users.

mitigating role of various factors, but will also provide insights into the relative importance of each causative mechanism. Hence, in the current study we synthesize key elements from prior research and develop an integrated model that simultaneously evaluates the effects of personality based beliefs along with the mediating effects of cognitive and information processing factors on individual susceptibility to phishing based deception.

3. An integrated, information processing model of phishing vulnerability

3.1. Theoretical premise

Early psychology research demonstrated that individual decision-making, rather than follow a direct path from stimulus (S) to response (R), followed a more complex trajectory through interpretation (I) (Dewey 1896; Rogers 2003) [15,42]. In the scenario of interpersonal deception, the stimuli are the verbal and non-verbal cues that a deceiver presents to a receiver. While the deceiver may modify his/her behavior in response to the receiver's suspicions, Buller and Burgoon's (Buller et al. 1996) [12] Interpersonal Deception Theory (IDT) argues that identifying the verbal and non-verbal leakage cues that deceivers display during the process of deception is the key to detecting deception. Different than interpersonal deception, a phishing attack involves no interpersonal interactions but uses an e-mail as a means to reach potential victims. The stimulus presented to a receiver in a phishing attack is the e-mail, and the leakage cues are the content and the layout of the e-mail.

Similar to IDT in many respects, the Theory of Deception (Johnson et al. 1992) [28] more narrowly focuses on the information processing (or interpretation) involved during deception detection. According to the theory, individuals recognize deception by noticing and interpreting the inconsistencies between the deceptive event and their past experiences. The process of recognizing deception is decomposed into four stages: activation, where targets pay attention to deceptive information and detect anomalies; deception hypothesis generation, where individuals use prior knowledge to generate interpretative hypothesis to explain the anomalies; hypothesis evaluation, where the hypothesis formed in the previous stage are compared against some criteria; and finally, a global assessment stage, where the information is combined to form a single, synthetic assessment of deceptiveness. The assessment of deceptiveness is subjective and significantly relies on individual prior knowledge.

Another theory that has been extended to study the information processing (or interpretation) of the receiver is the Elaboration Likelihood Model (ELM) (Petty et al. 1986) [39]. Rooted in consumer behavioral theory, ELM was developed to explain how consumers respond and process stimuli such as persuasive advertising messages. Consumers process messages in one of two ways: (i) the central route, involves a diligent consideration of information based on its merits and comparisons to prior beliefs; (ii) the peripheral route, is where the consumer does not consider all the pros and cons of the message, but instead focuses on simple cues in the persuasion context. The level of involvement, measuring the relevance of the message to the receiver, is a central concept in ELM and serves as a scope condition that defines the extent of cognitive and information processing resources an individual is willing to expend towards a decision (Petty et al. 1983) [40].

More recent research suggests that decision-making processes are better represented as O-S-I-R models, where O is an additional concept that represents the cultural, motivational, and personality characteristics that individuals bring to the situation that influence their interpretation of the stimulus and their ultimate response (Markus et al. 1985; McLeod et al. 1994) [35,36]. Thus the O-S-I-R perspective captures both the contextual and cognitive elements of the decision process and hence, provides the foundation for our research model. The overall research model is built to explain the factors that best predict an individual's phishing susceptibility, our measurement for the response (R), operationalized as the likelihood to respond to phishing emails.

Our model focuses on four contextual factors: the individual's level of involvement (I), domain specific knowledge (I), technological efficacy (I), and email load (O). These contextual factors cover individual situational factors (represented by O) as well as the motivational and experiential factors influencing phishing message processing and interpreting (represented by I). Based on research in mediated cognitions and learning from the news (Eveland et al. 2003) [20], the information processing activities are structured into two discrete sub-processes: attention to the stimulus and elaboration the message. Further, because prior research points to differing levels of attention to specific elements within phishing emails (Jakobsson 2007) [26], our research distinguishes between attention to email source, email title or subject line, grammar and spelling, and urgency cues (S). Unlike prior research that argues for direct effects of either contextual factors or information processing, the model articulated herein argues that contextual factors influence phishing susceptibility indirectly by influencing information processing activities. In other words, the influence of cognitive and information processing activities on phishing susceptibility are tempered by the individuals levels of motivation, their personality based beliefs, their prior knowledge, and their day-to-day experiences. Thus, the research model provides an overarching theoretically driven structure to compare and contrast the influence of the key factors thought to influence phishing susceptibility.

Table 2 summarizes the theory element we use in the model along with the source of theory.

3.2. Hypothesis development

The hypotheses suggested by the research model are detailed below in terms of the key constructs laid out in previous subsection.

3.2.1. Information processing activities

Based on research in mediated cognitions and learning from the news (Eveland et al. 2003) [20], the information processing activities are structured into two discrete sub-processes: attention and elaboration.

Attention is the first stage in information processing and indicates the amount of mental focus given to specific elements of an event or object (Eveland et al. 2003) [20]. The concept of activation in the Theory of Deception (TOD) is similar to the notion of attention, with one important difference. In TOD, the notion of activation consists of allocating attention to cues based on the presence of discrepancies between what is observed and what is expected (Grazioli 2004) [22]. This treatment in TOD obfuscates mere attention to specific aspects of an email with detection of discrepancy, which potentially requires more detailed evaluation. The present research model (See Fig. 1), therefore, is more consistent with mediated information processing

Table 2
Theory element and source of theory.

Theory element	Source of theory
Leakage cues: attention to e-mail content and layout (S)	Interpersonal Deception Theory (Buller et al. 1996) [12] Theory of Deception (Johnson et al. 1992)[28]
Individual prior knowledge (domain specific knowledge and technological efficacy) (I)	Theory of Deception (Johnson et al. 1992) [28]
Involvement (I)	Elaboration Likelihood Model (Petty et al. 1986) [40]
E-mail load (O)	Individual situational factors

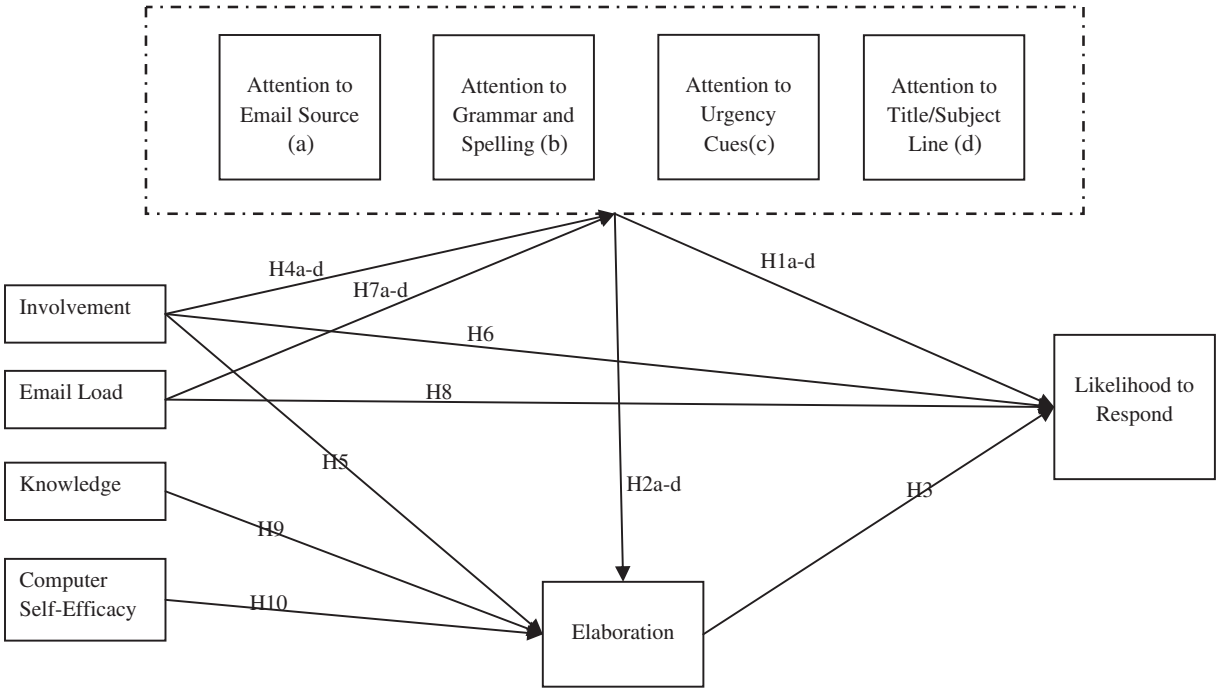

Fig. 1. Integrated, information processing model of phishing susceptibility.

models in defining and measuring attention merely in terms of whether or not an individual focuses on key elements of an email.

The model further distinguishes between the specific components of the phishing email that serve as stimuli. Recent qualitative experiments suggest that when comparing deceptive and authentic emails, individuals pay particular attention to the grammar and spelling used in the emails and the reply-to address or source of the email (Jakobsson 2007) [26]. Furthermore, because phishers utilize social engineering techniques to garner response, the research model tests the influence of two additional components: the title or subject line, and urgency cues in the phishing email. In phishing emails, the title serves as a lure, cueing individuals about the relevance of the message contained within the email. Urgency cues contained in the email invoke feelings of threat, fear, or scarcity, thereby attempting to short-circuit the evaluation process and elicit compliance.

The attention paid to each email component might have a distinctly different influence on the individual's likelihood to respond to the phishing email. Because title and urgency cues are designed to elicit compliance, attention to these elements would potentially increase the individual's likelihood to respond to the phishing email. In contrast, source information, and grammar and spelling have the potential to reveal the authenticity of the email and thereby reduce the individual's likelihood to respond to the request. Hence:

H1a. The level of attention to the email's source will be negatively related to the individual's likelihood to respond to phishing emails.

H1b. The level of attention to the grammar and spelling in the email will be negatively related to the individual's likelihood to respond to phishing emails.

H1c. The level of attention to the urgency cues will be positively related to the likelihood to respond to phishing emails.

H1d. The level of attention to the subject line will be positively related to the likelihood to respond to phishing emails.

Attention to cues is a necessary but not sufficient condition (Rigney 1978) [41] for detecting phishing based deception. In addition to paying attention to cues, individuals need to elaborate on the cues. Elaboration is the process through which individuals make conscious connections between the cues they observe and their prior knowledge (Perse 1990) [38]. The theory of deception (Johnson et al. 1992) decomposes detection–deception into discrete stages of activation, hypothesis generation, evaluation, and global assessment. These events occur during the process of elaboration (Eveland et al. 2003) [20]. The model posits that the process of generating hypotheses, evaluating hypotheses, and realizing that cues are inconsistent with prior understanding is a detailed information processing task that entails a comparison of cues with domain specific knowledge stored in one's memory during the process of elaboration.

The influence of elaboration in deception detection is supported by prior phishing research, much of which assumes that phishing emails are peripherally processed (e.g., (Workman 2007) [46]. Peripheral information processing occurs because individuals make simple inferences about an event based on simple cues in the persuasion context (Petty et al. 1983) [40]. In contrast, central information processing occurs when individuals diligently consider the information cues through the process of elaboration. The treatment of elaboration as pivotal to deception detection is also consistent with other models of mediated information processing such as the cognitive mediation models (Eveland et al. 2003) [20]. Empirical tests of these models have shown that individuals who elaborate on cues are more likely to comprehend, learn, retain and subsequently recall the information than individuals who merely pay attention to them (Cialdini 2001; Eveland et al. 2003) [13,20]. Hence, we posit that individuals fall victim to phishing emails because they fail to elaborate on the cues contained in the email, thereby failing to make connections between what they see and the knowledge stored in their memory. This failure to connect makes them more likely to ignore anomalous information and thereby more susceptive to phishing based deception.

H2a–d. The level of attention given to specific elements of the email (source, grammar and spelling, urgency cues, subject line) will be negatively related to the level of elaboration.

H3. Elaboration will be negatively related to the individual's likelihood to respond to phishing emails.

3.2.2. Involvement

The concept of involvement is central to understanding individual information processing. Involvement is defined as the perceived relevance of a particular message or event to an individual (Zaichkowsky 1985) [48]. Its influence on phishing susceptibility remains undetermined. Generally, information processing is more likely to occur when individuals find the information relevant to their needs and are thereby motivated to consciously evaluate it. Hence, we include involvement as a central, contextual factor and expect level of involvement to be positively associated with attention to specific elements of phishing emails and their elaboration.

H4a–d. The level of involvement will be positively related to the level of attention given to specific elements of the email ((a) source, (b) grammar and spelling, (c) urgency cues, (d) subject line).

H5. The level of involvement will be positively related to the level of elaboration.

In addition to an indirect influence, the research model also argues for a direct influence of level of involvement on phishing susceptibility. The notion is that individuals are sometimes likely to respond to an email subconsciously because of habitual email use patterns (Gopal et al. 2001) [21]. Anecdotal evidence from interviews conducted by the research team with two victims of a recent phishing attack, shows that many subjects reported responding to the phishing email without consciously attending to them. This suggests that some responses to phishing emails might be habitual, without the active engagement of information processing resources.

A habit is an automatic pattern of response or behavior that follows a fixed cognitive schema, triggered by an environmental stimulus and performed without active consideration (Bargh et al. 1994; LaRose et al. 2004) [3,32]. Emerging research suggests that a great deal of media consumption behavior might be habitual (Adams 2000; LaRose et al. 2003) [1,33]. Habitual behaviors are initially formed through active consideration, but through repetition, individuals become inattentive to the reasoning behind the media use. Hence, the mind no longer devotes attention resources to evaluating the behavior, thereby freeing itself for important decisions (LaRose et al. 2004) [32]. Email use might be a classic case of habitual media use. Many individuals report checking emails every morning or every time they encounter a device that allows access to email. Hence, phishing email responses might be partially conditioned by similar habitual response patterns, where individuals automatically respond to *relevant* emails without actively attending to them. The issue, however, is one of measuring habit. Because habit is subconscious, measuring it activates information processing in the respondent and makes it a conscious behavior. Hence, in the present piece, we do not directly measure habit. Instead, we focus on the construct of involvement and use it as an indicator of relevance, which is a necessary condition for the activation of habitual information processing (LaRose et al. 2004) [32]. We posit that individuals habitually responding to emails with little active attention are much more likely to respond to emails that appear relevant. Therefore, we expect level of involvement to be directly related to the individual's likelihood to respond to the phishing email.

H6. In addition to influencing attention and elaboration, the level of involvement will be positively related to the individual's likelihood to respond to a phishing email.

3.2.3. Email load

An important variable, often overlooked in phishing research, is the number of emails an individual receives in a given day. The volume of emails an individual receives has two potential consequences from a phishing detection stand-point. First, a large volume of emails might reduce the individual's ability to pay attention to specific elements of each email. Hence, larger email volumes could be negatively related to the level of attention paid to the specific elements of a phishing email. Second, a large volume of emails received might directly influence the likelihood to respond to a phishing email by resulting in individuals directly responding to email without consciously paying attention to the email.

H7. Email load will be negatively related to level of attention given to specific elements of the email (source, grammar and spelling, urgency cues, subject line).

H8. Email load will be positively related to the individual's likelihood to respond to a phishing email.

3.2.4. Domain-specific knowledge

Domain-specific knowledge subsumes experience, exposure, and learning within a single construct. Emerging research on online deception argues for increasing awareness, knowledge, and sensitivity training, as a solution to reducing individual phishing susceptibility (e.g., (Brios 2002) [11]. Consistent with these arguments, we expect increased domain specific knowledge to influence individual phishing susceptibility indirectly by influencing the individual's ability to effectively elaborate and find anomalous or deceptive information.

H9. Domain specific knowledge will be positively related to elaboration.

3.2.5. Computer self-efficacy

In addition to domain specific knowledge, the model also includes computer self-efficacy. Self-efficacy is the belief in one's ability to organize and execute a particular course of action (Bandura 1986) [2]. From the present perspective the focus is on computer self-efficacy, i.e., the beliefs in one's ability to use computing technology. To-date, the treatment of personality specific beliefs has focused on its direct effects on phishing susceptibility. In the present model, however, we argue for the position espoused by Socio Cognitive Theory (SCT) (Bandura 1986) [2], where self efficacy is thought to regulate behaviors by influencing the expected outcomes from the behavior. The comprehension of expected outcomes for a behavior, however, requires an in-depth assessment and processing of its potential. Because elaboration is the stage in cognitive information processing where such detailed assessments are made, we expect self efficacy to be positively associated with the degree of elaboration.

H10. Computer self-efficacy will positively be related to elaboration.

In closing, the research model (Fig. 1) posits that individuals get phished primarily because they do not actively engage in elaborate processing of the deceptive elements of an email. Rather, individuals pay attention to specific elements and directly respond to the email primarily because of inadequate elaboration and because of habitual media use patterns conditioned by high information loads. The next section presents the research methodology.

4. Methodology

The model was tested on a sample of actual intended victims of a series of phishing attacks. In the spring of 2008, email users at a major university in northeast USA were targets of two phishing attacks. The first email was received by all university email users on February 28, 2008 at 2:57 pm. The email, purportedly from the university email team, notified users of a forthcoming site upgrade and asked users to verify their email account information. The title or subject line of the email read “UPGRADE YOUR EMAIL ACCOUNT NOW.” The text of the email asked users for their user name, password, date of birth, security question, and security answer. Further, the email warned users that

they would permanently lose their email account if they did not send this information within 7 days of receipt of the solicitation.

On March 4, 2008, at 8:26 pm another phishing attack took place. This email, purportedly from the "Admin Help Desk," used the pretext of upgrading the email database and email account center for soliciting account use information. The subject line of the email read "Dear University Email Account Owner," while the body text began with the title "VERIFY YOUR UNIVERSITY EMAIL ACCOUNT NOW." Using the threat of account closure, the email asked university email users to provide their email username, password, date of birth, and country. Similar to the earlier attack, this email also warned users failing to update their account by responding to the email within 7 days.

The two phishing attacks provided an ideal opportunity for testing the research model. Within four weeks after the second attack, following IRB approval, the data collection effort began. This study was conducted to take advantage of a natural event where the phishing attacks were real with the attacking e-mails crafted by attackers and targeted towards a general university population.

In general phishing research is besotted by many adverse issues. Reaching a sample of phishing victims in an external environment is often difficult. The success rate of such attacks is relatively low, which makes it very difficult to collect data from real victims even in a nation-wide phishing attack. So far no study, to our knowledge, has been able to access a sufficiently large number of victims to make meaningful inferences. Many times, individuals may not know that they have been phished. If they realize that they have been phished and report a complaint to an agency such as APWG or FBI, getting access to this population is often difficult. In addition, depending on the time elapsed victims may not remember the facts related to the incident with precision or accuracy.

To carry out mock or simulated phishing attacks, i.e. conducting deceptive studies such as carrying out phishing attacks, in the academic environment is especially difficult because of reasons that include getting approval from IT personnel to carry out such attacks, and the opinions of ethics board in such deceptive tactics. Other alternative often used is to carry out lab experiments which are often criticized for having bias due to the Hawthorne effects. In other instances researchers have noted criticism from the experiment participants displaying anger over the deceptive tactics used (Jagatic et al. 2007) [25]. This natural event allowed the research team to take advantage of an otherwise difficult setting to mimic and reach the possible victims in a very narrow window of time by providing a unique opportunity to study phishing. When participating in the surveys, the respondents responded to natural events (i.e., the two phishing emails) that took place in their lives. We were therefore able to collect unbiased responses while avoiding Hawthorne effects which are likely to occur in lab experiments.

In order to capture reliable estimates from a large group of fairly homogenous targets of the phisher, the data collection effort focused on undergraduate students at this university rather than faculty, staff, and graduate students. The entire data were collected in less than two weeks, between April 22, 2008 and May 4, 2008.

Undergraduate students in the department of Communication and the Business School were contacted via email by their respective undergraduate student advisors. The email asked students to participate in a short web-survey about student email use. The link to the survey was embedded in the solicitation email. Students participating in the survey were given a chance to enter in a random drawing to win one from one hundred, $5 Starbucks gift cards.

Following the informed consent process, students were asked a series of questions about general email use. They were then randomly shown one of the two phishing emails. Respondents were next asked whether they recalled receiving the email, how likely they were to respond to the email, and whether they actually responded to the email. These questions were followed by a series of questions pertaining to measures from the research model. Next, respondents were shown the other phishing email followed by the same set of questions. The randomization procedure ensured that roughly half of all respondents were presented one email first followed by the other, while the order was reversed for the other half.

Overall, the data collection effort resulted in 325 completed responses. From these, 4 had responded to one of the emails, 4 responded to the other email; 1 respondent among these had responded to both phishing emails. Approximately 191 responses were from Communication undergraduates and the remaining 130 were Business majors in all departments. The average age of the respondent was 21 years ($SD = 3.19$) and 54% of the respondents were female.

Given the relatively large sample of intended victims ($N = 321$), a split-half procedure for model testing was employed following the suggestions of Joreskog et al. (1986) [29]. This is accomplished by randomly selecting half of the subjects for initial analysis and holding the second half back for a second round of confirmatory model testing. In the present study, the procedure resulted in two split-half samples with 161 and 160 respondents respectively.

4.1. Measures

For the most part, the current study used prior validated measures developed in the IS and communication literature. Table 3 details the measures used in the study along with their alpha reliabilities.

5. Results

The research model was tested and refined using AMOS 5 on the sample of 161 intended phishing victims. Goodness of fit was estimated using a combination of four fit indices (Holbert et al. 2002) [24]: chi-square (χ^2), relative chi-square (χ^2/df), *CFI* (comparative fit index), *NFI* (normed fit index), and *RMSEA* (root mean square error of approximation). *CFI* and *NFI* values range from 0 to 1, with 0.95 or higher indicating a good fit between the observed data and the specified model; *RMSEA* of .05 or less indicates a close fitting model (Joreskog et al. 1986) [29]. Table 4 presents the means and standard deviations of the measures.

The initial path model achieved a less than acceptable fit: $\chi^2 = 208.6$, $df = 17$, $p < .05$, $\chi^2/df = 18.57$, $CFI = 0.46$, $NFI = 0.49$, and $RMSEA = 0.28$. Modification indices suggested co-variances between the attention measures (source, grammar and spelling, urgency cues, subject line), and paths from computer self efficacy ➔ attention to title/subject line ($MI = 7.19$, $\Delta\ par = -1.21$), computer self efficacy ➔ attention to source ($MI = 10.39$, $\Delta\ par = -2.96$), and from domain specific knowledge ➔ attention to title/subject line ($MI = 1.23$, $\Delta\ par = 0.23$), and domain specific knowledge ➔ attention to source ($MI = 5.77$, $\Delta\ par = 1.49$). The re-specified model achieved an excellent fit: $\chi^2 = 12.28$, $df = 7$, $p = .09$, $\chi^2/df = 1.75$, $CFI = 0.99$, $NFI = 0.98$, and a $RMSEA = 0.04$. All the standardized regression weights were less than $+/-1$ and standard errors were neither excessively high nor low, indicating that there was no multi-collinearity in the data. The overall model predicted 31% of the cumulative attention paid to email elements (source, grammar and spelling, urgency cues, subject line), and 23% of level of elaboration, and 48% of the individual's likelihood to respond to phishing email.

The final model was validated and confirmed using the second sample ($N = 160$). The test of the model resulted in an excellent fit: $\chi^2 = 16.05$, $df = 7$, $p = .03$, $\chi^2/df = 2.29$, $CFI = 0.99$, $NFI = 0.97$, and a $RMSEA = 0.04$. In this test, the model predicted 22% of the cumulative attention paid to email elements (source, grammar and spelling, urgency cues, subject line), and 22% of level of elaboration, and 46% of the individual's likelihood to respond to phishing email.

The tests of the hypotheses are summarized in Table 5.

Hypothesis 1a posited that attention to email source would be *negatively* related to individual's likelihood to respond to the phishing email. In the validation sample, the path from email source attention

Table 3
Summary of construct measurement.

Construct	Supportive literature	Example item	Cronbach alpha
Involvement	(Zaichkowsky 1985) [48]; 9 items; 5-point scale where 1 = relevant	Relevant vs. irrelevant, essential vs. non-essential	0.95
Computer self-efficacy	(Compeau et al. 1995) [14]; 5 items; 5 point scale where 1 = strongly agree	It is easy for me learn to use a new email program without much help from others	0.87
Domain specific knowledge	4 item; 5-point scale where 1 = not at all knowledgeable	Knowledge about emails in general, about email based scams, about official emails received from the university	0.86
Email load		Average number of emails received on a given day	
Attention to sender source	(Eveland et al. 2003) [20]; 3 items; 5-point scale where 1 = none/not at all	Attention to sender name, senders email address, and the reply-to address	0.84
Attention to grammar	(Eveland et al. 2003) [20]; 4 items; 5-point scale where 1 = none/not at all	Attention to typographical errors in emails text, content, grammar in title and body of message	0.94
Attention to urgency	(Eveland et al. 2003) [20]; 3 items; 5-point scale where 1 = none/not at all	Attention to warnings, statements indicating urgency, and statements of a time bound nature	0.86
Elaboration	(Eveland et al. 2003) [20]; 6 items; 5-point scale where 1 = strongly agree	After looking at the email, you…; related what you saw to how you expect formal emails from the university	0.92
Likelihood to respond	1 item; 5-point where 1 = not at all likely	Direct question	

(scaled from 1 = none/not at all, i.e., no attention) to likelihood to respond (scaled 1 = not at all likely) was significant ($\beta = -0.27$, *c.r.* = −2.47, $p<.05$). Hence, hypothesis 1a was supported by the data.

Hypothesis 1b posited that level of grammar and spelling attention would be *negatively* related to the individual's likelihood to respond to the phishing email. In the validation sample, the path from grammar and spelling attention (scaled from 1 = none/not at all) to likelihood to respond (scaled 1 = not at all likely) was significant ($\beta = -0.29$, *c.r.* = −3.06, $p<.05$). Hence, hypothesis 1b was supported by the data.

Hypothesis 1c posited that the level of attention to urgency cues would be *positively* related to the individual's likelihood to respond to the phishing email. The path from urgency attention (scaled from 1 = none/not at all) to likelihood to respond (scaled 1 = not at all likely) was significant ($\beta = 0.23$, *c.r.* = 2.41, $p<.05$). Hence, hypothesis 1c was supported by the data.

Hypothesis 1d posited that the level of attention to the subject line would be *positively* related to the individual's likelihood to respond to the phishing email. The path from subject line attention (scaled from 1 = none/not at all) to likelihood to respond (scaled 1 = not at all likely) was significant ($\beta = 0.26$, *c.r.* = 2.52, $p<.05$). Hence, hypothesis 1d was supported by the data.

Hypothesis 2a–d posited that the level of attention given to the email's source, grammar and spelling, urgency cues, and subject line, respectively, would be negatively related to the level of elaboration. In the validation sample, the paths from level of source attention (attention scaled from 1 = none/not at all or no attention) to elaboration (scaled 1 = strongly agree or high elaboration), grammar attention to elaboration, and subject-line attention to elaboration were each negative but not significant. Only the path from attention to urgency cues to elaboration achieved significance ($\beta = -0.23$, *c.r.* = −2.40, $p<.05$). Hence, the data were in support of hypothesis 2d.

Hypothesis 3 posited that the level of elaboration would negatively influence the individual's likelihood to respond to the phishing email. The path from elaboration (scaled 1 = strongly agree or high elaboration) to likelihood to respond (scaled 1 = not at all likely) was negative but not significant ($\beta = -0.10$, *c.r.* = −1.21, $p>.05$). Hence, the data were only in support of the direction of hypothesis 3.

Hypothesis 4a–d posited that the level of involvement would be *positively* related to the level of attention given to the email's source, grammar and spelling, urgency cues, and subject line, respectively. In the validation sample, the path from involvement (scaled 1 = essential or central processing) to urgency attention (scaled from 1 = none/not at all, i.e., not much attention given) was significant ($\beta = -0.20$, *c.r.* = −2.46, $p<.05$); individual paths from involvement to source attention, grammar and spelling, and subject line were negative but did not achieve acceptable significance ($p>.05$). Hence, the data supported the direction of influence and partially supported the level of influence posited in hypothesis 4a–d.

Hypothesis 5 posited that the level of involvement would be *positively* related to elaboration. The path from level of involvement (scaled 1 = essential or central processing) to elaboration (scaled 1 = strongly agree, or high elaboration) in the research model was significant ($\beta = 0.20$, *c.r.* = 2.59, $p<.05$). Hence, the data were in support of hypothesis 5.

Hypothesis 6 posited that level of involvement would *positively* and directly influence individuals' likelihood to respond a phishing email. After influencing attention and elaboration, in the validation sample, the direct path from involvement (scaled 1 = essential, i.e., high involvement) to likelihood to respond (scaled 1 = not at all likely to respond) was significant ($\beta = -0.60$, *c.r.* = −9.31 $p<.05$). Hence, the data were in support of hypothesis 6.

Hypothesis 7a–d posited that email load would be *negatively* related to the level of attention given to the email's source, grammar and spelling, urgency cues, and subject line, respectively. The paths from email load (ratio level measure) to attention (scaled from 1 = none/not at all) to source, grammar and spelling, subject line, and urgency cues were negative but did not achieve acceptable significance ($p>.05$). Hence, the data supported the direction of influence but not the level of influence posited by hypothesis 7a–d, and, therefore, the hypothesis was rejected.

Hypothesis 8 posited that email load would be *negatively* related to likelihood to respond. In the validation sample, the direct path from email load (ratio level measure) to likelihood to respond (scaled 1 = not at all likely) was significant ($\beta = -0.23$, *c.r.* = −3.21, $p<.05$). Hence, the data were in support of hypothesis 8.

Table 4
Means and standard deviations of measures of phishing vulnerability (email 1).

Measure name	Split half $N = 161$		Split half $N = 160$	
	Mean	Std	Mean	Std
Level of involvement	3.34	1.14	3.46	1.08
Attention to email source	3.46	1.26	3.51	1.20
Attention to grammar and spelling	2.83	1.07	2.96	1.14
Attention to urgency cues	3.25	1.23	3.34	1.23
Attention to title/subject line	3.13	1.25	3.22	1.20
Elaboration	2.56	1.02	2.60	1.05
Likelihood to respond	2.08	1.30	2.01	1.24
Email load	19.46	33.87	19.10	32.74
Domain-specific knowledge	3.81	0.88	3.10	1.25
Computer self-efficacy	2.02	1.31	2.07	0.83

Table 5
Summary of hypotheses test.

Hypotheses	Results in initial sample ($N=161$)	Results in validation sample ($N=161$)	Overall conclusion
H1a	$\beta=-0.26$, *c.r.* $=-2.75$, $p<.05$	$\beta=-0.27$, *c.r.* $=-2.47$, $p<.05$	Supported
H1b	$\beta=-0.38$, *c.r.* $=-4.24$, $p<.05$	$\beta=-0.29$, *c.r.* $=-3.06$, $p<.05$	Supported
H1c	$\beta=2.73$, *c.r.* $=3.01$, $p<.05$	$\beta=0.23$, *c.r.* $=2.41$, $p<.05$	Supported
H1d	$\beta=0.31$, *c.r.* $=3.47$, $p<.05$	$\beta=0.26$, *c.r.* $=2.52$, $p<.05$	Supported
H2a–d	Source to elaboration: $p>.05$; grammar to elaboration: $p>.05$; subject line to elaboration: $p>.05$; Urgency to elaboration: $\beta=-0.29$, *c.r.* $=-3.15$, $p<.05$	Source to elaboration: $p>.05$; grammar to elaboration: $p>.05$; subject line to elaboration: $p>.05$; Urgency to elaboration: $\beta=-0.23$, *c.r.* $=-2.40$, $p<.05$	Only Urgency cues *are* significantly elaborated; all other cues are not significantly elaborated
H3	$\beta=-0.14$, *c.r.* $=-1.71$, $p>.05$	$\beta=-0.10$, *c.r.* $=-1.21$, $p>.05$	Direction as hypothesized, but the relationship was not significant
H4a–d	Involvement to urgency cues: $\beta=-0.19$, *c.r.* $=-2.38$, $p<.05$; Involvement to subject line: $\beta=-0.19$, *c.r.* $=-2.41$, $p<.05$; non-significant for others	Involvement to urgency cues: $\beta=-0.20$, *c.r.* $=-2.46$, $p<.05$; non-significant for others	Supported for urgency cues
H5	$\beta=0.19$, *c.r.* $=2.52$, $p<.05$	$\beta=0.20$, *c.r.* $=2.59$, $p<.05$	Supported
H6	$\beta=-0.53$, *c.r.* $=-8.23$, $p<.05$	$\beta=-0.60$, *c.r.* $=-9.31$, $p<.05$	Supported
H7a–d	$p>.05$ for all cues	$p>.05$ for all cues	Not supported
H8	$\beta=-0.26$, *c.r.* $=-3.26$, $p<.05$	$\beta=-0.23$, *c.r.* $=-3.21$, $p<.05$	Supported
H9	$\beta=-0.16$, *c.r.* $=-2.05$, $p<.05$	Non significant path	Partial support
H10	$\beta=0.30$, *c.r.* $=0.34$, $p>.05$	$\beta=0.170$, *c.r.* $=1.83$, $p>.05$	Not supported

Note. A hypothesis is considered supported only if both the samples yield consistent results; otherwise it is treated as partially supported.

Hypothesis 9 stated that domain specific knowledge would be *positively* related to level of elaboration. In the initial sample, the path from domain-specific knowledge (scaled 1 = none/not at all, 5 = very confident) to elaboration (scaled 1 = essential) was significant ($\beta=-0.16$, *c.r.* $=-2.05$, $p<.05$). In the validation sample, however, the same path from domain-specific knowledge to elaboration was insignificant. Hence, hypothesis 9 was considered partially supported.

Hypothesis 10 posited that efficacy would *positively* influence the level of elaboration. The direct path from computer self efficacy (1 = strongly agree/very confident) to elaboration (scaled 1 = essential) was significant ($\beta=0.17$, *c.r.* $=1.83$, $p>.05$). Hence, hypothesis 10 was not supported by the data.

In the final research model, the modification indices based additional paths from computer self-efficacy to attention to source ($\beta=-0.17$, *c.r.* $=-5.10$, $p<.05$) and attention to subject line ($\beta=-0.28$, *c.r.* $=-2.82$, $p<.05$) were significant. Again, the addition of paths from domain-specific knowledge to attention to subject line resulted in a non-significant path from computer self efficacy to title attention. Both paths, from computer self-efficacy to source attention ($\beta=-0.19$, *c.r.* $=-3.68$, $p<.05$) and from domain specific knowledge to source attention ($\beta=0.17$, *c.r.* $=2.71$, $p<.05$), remained significant.

6. Discussion

This research developed and tested an integrated, information processing model of phishing susceptibility. Based on the O-S-I-R perspective, the model posited that contextual variables would influence individual phishing susceptibility, indirectly, by influencing cognitive and information processing activities. The model was first refined using a sample of intended victims and then empirically validated using another sample of intended victims of a recent phishing attack. Overall, the data were in support of the causative structure, theoretical propositions, and causal relationships suggested by the research model. The final model achieved an excellent fit and predicted close to 50% of the individuals' likelihood to respond to phishing emails.

The model introduced and tested the influence of four contextual variables: level of involvement, email load, domain specific knowledge, and computer self-efficacy. The research was among the first to test the influence of involvement in the phishing detection process. Consistent with the research hypotheses, involvement positively influenced the level of attention and elaboration. While the influence of involvement on elaboration was significant, its influence on attention was significant only for urgency cues and non-significant for attention to source, grammar and spelling, and subject-line. Phishers use urgency cues to communicate fear, threat, and scarcity (Workman 2007) [46]. Such information cues are known to garner higher amounts of information processing resources (Shah et al. 2004) [43]. The finding, therefore, suggests that in the presence of a relevant email, individuals focus disproportionately on urgency cues, often ignoring other elements of the email such as its source and the grammar and spelling used in the email. Since these other elements aid the detection of deception (Jakobsson 2007) [26], the lack of attention to these elements increases the individual's likelihood to be phished.

In the phishing context no research to-date has accounted for the influence of habitual media use patterns on individual phishing susceptibility. Because habitual media use results in inattentiveness and automatic responses to patterned stimuli (LaRose et al. 2004) [32], its influence was tested through the direct path from involvement to likelihood to respond. This direct relationship between involvement and phishing susceptibility was both strong and significant. While the overall model predicted 46% of the variance in likelihood to respond, the model with complete mediation (where attention and elaboration completely mediated the influence of involvement) accounted for only 20% of the variance in likelihood to respond. This suggests that habitual media use patterns, where individuals inattentively respond to relevant emails, accounted for at least one half of the variance in phishing susceptibility. Hence, habitual patterns of email use were a major contributor to individual phishing susceptibility.

The model included another important, often overlooked variable: email load. The research posited that email load could foster inattentiveness and support habitual media use patterns, thereby directly influencing likelihood to respond. The results suggested that individuals were far more likely to respond to phishing emails in the presence of large email loads. This suggests that level of involvement, email load, and urgency cues in the email form a triad of important predictors of individual phishing susceptibility.

Based on SCT, the research posited that self efficacy would influence individual likelihood to respond to phishing emails, indirectly by influencing elaboration. This relationship was not supported by the data. Further, the research examined the role of domain-specific knowledge. Knowledge allows for deception-detection by helping recognize the elements of the information that are discrepant during the process of elaboration. Hence, domain-specific knowledge was seen to directly influence elaboration. We suspect that the observed insignificancy of self efficacy may be caused by the simultaneous presence of domain-specific knowledge in the research

model. When compared with self efficacy, domain specific knowledge offers online users with more accuracy and confidence in decision making. Therefore users may adopt domain knowledge and follow it in the engagement of elaboration. Furthermore, modification indices suggested that knowledge also influenced the extent of attention given to the email's subject line and email's source. The role of individual self-efficacy was universally diminished, except in determining the level of attention paid to email source, where self-efficacy was slightly more influential.

Based on research on mediated cognitions, ELM, and the Theory of Deception, the research model structured the cognitive, information processing activities that lead to deception detection into two discrete sub processes: attention was the first step, followed by elaboration. Attention is a necessary condition for information processing and hence, the research posited that attention would influence the likelihood to respond to the email. Unlike prior research that treats attention as a single construct, the model distinguished between four cues that could attract individual attention: the subject line or title, email source, urgency cues, grammar and spelling. Attention to each of these email elements would potentially influence individuals differently. Urgency cues, because they are designed to invoke feelings of threat, would have the strongest influence and individuals focusing on such cues would be significantly more likely to respond to the phishing email. Likewise, the title of email serves as a lure, invokes fear and urgency, and at other times, cues individuals about the email's relevance. Therefore, attention to urgency cues and the title or subject line increase the individuals' likelihood to comply and respond to the phishing email. In contrast, email source information would potentially reveal the legitimacy of the email. For instance, in the two phishing emails tested, the reply-to addresses were non-".edu" extensions. Likewise, the grammar and spelling used in phishing emails have been shown to influence the detection of phishing based deception because often these emails are poorly worded and contain typographical errors (Jakobsson 2007) [26]. Hence, attention to email source and attention to grammar and spelling would decrease the likelihood to be phished.

The results show individuals' levels of attention to urgency cues and email subject-lines are significantly more likely to trigger a response to phishing email, while their levels of attention to the email source and grammar and spellings used in the email are significantly less likely to trigger a response. Further, since most phishing emails are processed peripherally (Workman 2007) [46], the model posited that these email cues would not be elaborated upon. The data, for the most part, supported this proposition. While attention to source, title and grammar/spelling did not influence elaboration, attention to urgency cues did significantly influence elaboration. This suggests that similar to fear appeals, urgency cues garner higher amounts of information processing resources and trigger elaboration (Shah et al. 2004) [43]. Based on ELM, the research posited that elaboration would not be significantly related to the individuals' likelihood to respond. This was supported, suggesting that individuals made simple inferences about the email based on event based cues rather than diligently processing the information.

Overall, the findings suggest that individuals get phished for two main reasons. One reason is that they do not adequately process the information. Rather, they rely on simple cues, some of which have the potential to increase their susceptibility to phishing based deception. Domain specific knowledge gained through education, awareness, or experience, therefore, has a limited effect because the application of knowledge requires elaboration. Among the cues used by phishers, the urgency cues are by-far the most virulent. Such cues engender a higher degree of information processing. As a result, other deceptive clues in the email's source or the grammar and spelling in the email do not receive much elaboration. This overall effect is further strengthened by the individuals' media use habits, which is the other main reason people get phished. Habitual patterns of media use, in the presence of high levels of email load, tend to trigger automatic responses to relevant looking emails. That is, individuals exposed to relevant emails, with strongly worded urgency cues, in the presence of high email load, are significantly more likely to be phished. Together, relevance, urgency cues, and habitual media use patterns form a triad of influence and largely determine individuals' phishing susceptibility.

7. Limitations and conclusions

While the findings of the study sheds light on the process of phishing based deception, arguments could be made that the student sample used in the study was not representative of the general public. Though students are not representative of the average consumer, they are especially relevant in the context of email based deception because they tend to engage in more online behaviors and conduct more online commercial transactions that the average consumer.

Apart from student samples, there are least three additional limitations of the study. First, the study tested a limited number of phishing emails. Both the emails tested were similar in the types of information they asked for and the level of threat they posed. Other emails, such as those asking for social security numbers, banking information, and posing direct financial risks to the target, might result in increased deception. Moreover, differences in the quality of phishing emails might further heighten individual phishing susceptibility. This is a limitation of the email used rather than of the model and one would expect the activation of similar cognitive and behavioral variables, i.e., the model variables, when individuals fall victim to other phishing emails. Second, the study did not use a control condition. This was because it was difficult, if not impossible, to apriori select a set of features that did or did not exist in an email and control for its effects. Third, stemming from the lack of a control group, it is difficult to ascertain whether the effects found in the study are reflections of only phishing email processing or reflections of general email use behavior.

Most of these limitations can be overcome by future research. Future research could create a compendium of cues in deceptive and regular emails. These could be used to create exemplars of emails that could be tested in experimental settings. Future research needs to also focus on findings ways to directly measure habitual media use. Given the importance of this construct and the difficulty in measuring it directly without influencing the user, a sound measure of habit strength would further improve our understanding of the phishing deception process. Also, given the impact that urgency cues have on phishing based deception, future research could vary the degree of urgency, the types of warnings, threats, and cues, and evaluate its effects on victims. Finally, future research needs to focus on actual victims of phishing emails. Finding actual victims is always hard because few databases, websites, and business provide this information to researchers. Even in the present study, the number of actual victims was too few to allow for any statistically valid conclusions. A study focusing on actual phishing victims would of enormous significance because it would help validate the research model and further our understanding of phishing based deception.

The research is, however, noteworthy and contributes to our understanding of phishing based deception in the following ways. First, earlier research on phishing has focused on single sets of causative factors and has extended process models such as the Theory of Deception to understand phishing based deception. The present research is the first to integrate these different streams of research and test a variance based model of phishing susceptibility. Second, the model provides an overarching theoretical structure to understand the influence of and interrelationships between different causative mechanisms on phishing susceptibility. The model's theoretical structure is strongly supported by the data and its causative sequence accounted for close to 50% of the variance in individual phishing

susceptibility. Third, the model introduces and tests the influence of a number of important variables that has been ignored in online deception research. These include the influence of media habits, involvement, and email load along with the mitigating role of knowledge on self efficacy beliefs, and of knowledge and self efficacy on attention and elaboration. Finally, not only does the model provide insights into how individuals get phished, but it also provides a framework to test the influence of other variables. For instance, a researcher interested in studying the influence of an intervention, such as exposure to phishing related information on individual phishing susceptibility, could utilize the present model to better track its influence and causative sequence. Hence, the research makes a significant contribution to the study of phishing.

8. Implications

The following are the immediate implications of the current study. First, the influence of email load on likelihood to respond to phishing emails suggests that the more emails one receives, the more likely they are be deceived. The influence of load is further heightened when one not only receives but also responds to a large volume of emails. This means that spam blockers are imperative at one end to reduce the number of unnecessary emails that individuals receive that could potentially clutter their information processing and concomitant judgment. At the other end, individuals need to be extra careful when utilizing a single email account to respond to all their emails. Instead, an effective strategy is to utilize different email accounts for different purposes. So, an email address used solely for banking and another for personal communication with family and friends, increases attention and reduces the likelihood of chance-deception because of clutter.

Another implication of the current study is that individuals are more likely to attend to emails from known rather than unknown entities. That is, a phishing email purportedly from Key Bank might have little effect on individuals who do not transact with Key Bank, but is likely to be clicked on (passive deception) or responded to (active deception) by individuals with existing relationships with Key Bank. Many more websites today require valid email addresses for login purposes; many banks and financial institutions prefer to communicate exclusively via email. Hence, the more online relationships one maintains and the more they transact online, the more likely they are to fall victim to an email based scam.

A third, important implication of the current study is the lack of effect of technological efficacy and prior experience on phishing susceptiveness. Individuals fall victim to phishing and other email based scams because of a lack of cognitive involvement rather than a lack of ability. This means that individuals who consider themselves to be technological sophisticated are just as likely to be phished as are individuals who are not as technically sophisticated. Moreover, because individuals who are technically sophisticated tend to maintain and engage in more online relationships and thereby receive and respond to more emails, such individuals are far more likely to be targeted.

A fourth implication is the influence of habitual media use. Habitual media use is often ignored in most mass communication research. Patterns of habitual media use include ritualistic consumption practices such as checking a news website every morning or at different times during the day. Email use is a classic case of habitual media use. Individuals report that they habitually check emails at the beginning of the day; many individuals ritualistically check email throughout the day often at multiple locations (e.g., airport terminals, hospitals, and other public places). Devices such as Blackberry and iPhones have capitalized on this behavior and furthered the habit. Such devices, however, also increase the likelihood of passive deception – where one inadvertently clicks on an embedded link within an email and gets phished.

Habitual email use is particularly dangerous because these consumption habits once established continue with little further cognitive involvement. Hence, individuals who ritualistic read emails tend to engage in little cognitive deliberation about the established behavior and therefore much more likely to ignore nuances in the email that might reveal the deception. Habitual media use patterns are further complicated by other activities that might distract information processing. For instance, habitual email reception on a Blackberry while consuming breakfast, responding to emails while watching the kids at home, or reading emails while watching TV, might result in reduced attention and increased susceptibility to email based scams.

Overall, the strategy, often espoused by researchers, is vigilance. Vigilance is, however, a short term strategy, and it is difficult to maintain a high state of alert at all times. Rather, strategies that create safer rituals might be sustainable over the long term. One such ritual should be to earmark a certain, separate time each day for reading and responding to personal emails. Using a different time to read email and a different time to respond to them, increases the cognitive effort exerted during the process. Another strategy would be to use multiple email addresses for specific purposes. An email account for banking, an email account for personal communication, and an email account for business, might be one way to reduce clutter and catch seemingly out-of-place emails. Many email providers such as Yahoo and Gmail provide for multiple emails and disposable addresses; other services such as MailExpire and Mailinator provide free, temporary email addresses for use in websites that require an email address for login. Finally, individuals need to utilize spam blockers and other, widely available service based protections. Most of these blockers offer limited protection; many flag legitimate emails as well as suspected deceivers; and as neural programs, most of these protections work best after a large scale invasion has occurred and the system has been updated. Hence, the ultimate arbiter of legitimacy remains the individual user. Creating safer rituals seems to be the most viable solution for increasing information processing and reducing the individuals' susceptiveness to online, email based deception.

References

[1] W. Adams, How people watch television as investigated using focus group techniques, Journal of Broadcasting & Electronic Media (44) (2000) 78–94.
[2] A. Bandura, Social foundations of thought and action: a social cognitive theory, Prentice Hall, Englewood Cliffs, NJ, 1986.
[3] J.A. Bargh, P.M. Gollwitzer, Environmental control of goal directed action: automatic and strategic contingencies between situation and behavior, in: W.D. Spaulding (Ed.), Nebraska symposium on motivation, University of Nebraska Press, Lincoln, 1994, pp. 71–124.
[4] R. Barkhi, Cognitive style may mitigate the impact of communication channel, Information Management (39:8) (2002) 677.
[5] R. Barkhi, L. Wallace, The impact of personality types on purchasing decisions in virtual stores, Information Technology and Management 8 (4) (2007) 313–330.
[6] F. Belanger, J.S. Hiller, Framework for E-government: privacy implications, Business Process Management Journal 12 (1) (2006) 48–60.
[7] F. Belanger, J.S. Hiller, W.J. Smith, Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, The Journal of Strategic Information Systems 11 (3/4) (2002) 245–270.
[8] I. Bose, A.C.M. Leung, Unveiling the mask of phishing: threats, preventive measures, and responsibilities, Communications of the AIS 19 (24) (2007) 544–566.
[9] I. Bose, A.C.M. Leung, Assessing anti-phishing preparedness: a study of online banks in Hong Kong, Decision Support Systems 45 (4) (2008) 897–912.
[10] I. Bose and A.C.M. Leung. What Drives the Adoption of Anti-phishing Measures by Hong King Banks, Communications of the ACM 52 (8), 2009 141–143.
[11] D.P. Brios, J.F. George, R.W. Zmund, Inducing sensitivity to deception in order to improve decision making performance: a field study, MIS Quarterly (26) (2002) 119–144.
[12] D.B. Buller, J.K. Burgoon, Interpresonal deception theory, Communication Theory (6) (1996) 203–242.
[13] R.B. Cialdini, Influence: science and practice, Allyn & Bacon, Boston, 2001.
[14] D. Compeau, C. Higgins, Computer self efficacy: development of a measure and initial test, MIS Quarterly (19) (1995) 189–211.
[15] J. Dewey, The reflex arc concept in psychology, Psychological Review (3) (1896) 357–370.

[16] R. Dhamija, J.D. Tygar, M. Hearst, Why phishing works, Conference on Human Factors in Computing Systems, CHI-2006, Montreal, Quebec, Canada, 2006.
[17] J. Downs, M. Holbrook, L. Cranor, Decision strategies and susceptibility to phishing, The 2006 Symposium on Usable Privacy and Security, Pittsburgh, PA, 2006.
[18] J. Downs, M. Holbrook, L. Cranor, Decision strategies and susceptibility to phishing, Symposium on Usable Privacy and Security, Pittsburgh, PA, 2006.
[19] J. Downs, M. Holbrook, L. Cranor, Behavioral response to phishing risk, The Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit Pittsburgh, Pennsylvania, 2007.
[20] W.P. Eveland, D.V. Shah, N. Kwak, Assessing causality in the cognitive mediation model: a panel study of motivations, information processing, and learning during campaign 2000, Communication Research (30) (2003) 359–386.
[21] R. Gopal, Z. Walter, A. Tripathi, Ad mediation: new horizons in effective email advertising, Communications of the ACM 44 (2) (2001) 91–96.
[22] S. Grazioli, Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet, Group Decision and Negotiation 13 (2) (2004) 149–172.
[23] A. Gupta, B.-C. Su, Z. Walter, Risk profile and consumer shopping behavior in electronic and traditional channels, Decision Support Systems 38 (3) (2004) 347–367.
[24] R.L. Holbert, M.T. Stephenson, Structural equation modeling in the communication sciences, 1995–2000, Human Communication Research (28) (2002) 531–551.
[25] T. Jagatic, N. JohnSon, M. Jakobsson, F. Menczer, Social phishing, Communications of the ACM 50 (10) (2007) 94–100.
[26] M. Jakobsson, The human factor in phishing, Privacy & Security of Consumer Information, Indiana University, Bloomington, IN, 2007.
[27] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, What instills trust? A qualitative study of phishing, Usable Security (USEC'07), Lowlands, Scarborough, Trinidad/Tobago, 2007.
[28] P.E. Johnson, S. Grazioli, K. Jamal, I.A. Zualkernan, Success and failure in expert reasoning, Organizational Behavior and Human Decision Processes (53:2) (1992) 173–203.
[29] K.G. Joreskog, D. Sorbom, PRELIS: a program for multivariate data screening and data summarization, Scientific Software, Mooresville, IL, 1986.
[30] P. Kamaraguru, Y.W. Rhee, A. Acquisti, L. Cranor, E. Hong, E. Nunge, Protecting people from phishing: The design and evaluation of an embedded training email system, Carnegie Mellon University, 2006.
[31] A. Karakasiliotis, S.M. Furnell, M. Papadaki, Assessing end-user awareness of social engineering and phishing, The 7th Australian Information Warfare and Security Conference, Perth, Western Australia, 2006.
[32] R. LaRose, M.S. Eastin, A social cognitive theory of Internet uses and gratifications: toward a new model of media attendance, Journal of Broadcasting & Electronic Media (48) (2004) 358–377.
[33] R. LaRose, C.A. Lin, M.S. Eastin, Unregulated internet usage: addiction, habit or deficient self-regulation? Media Psychology (2003) 225–253.
[34] A. Litan, Phishing Attack Victims Likely Targets for Identity Theft, Gartner Group, 2004.
[35] H. Markus, R.B. Zajonc, The cognitive perspective in social psychology, in: G. Lindzey, E. Aronson (Eds.), The handbook of social psychology, Random House, New York, 1985, pp. 137–230.
[36] J.M. McLeod, G.M. Kosicki, D.M. McLeod, The expanding boundaries of political communication effects, in: J. Bryant, D. Zillmann (Eds.), Media effects: advances in theory and research, LEA, Hillsdale, NJ, 1994, pp. 123–162.
[37] L.A. McNall, S.G. Roch, The effects of electronic monitoring type on procedural justice, interpersonal justice, and privacy, Journal of Applied Social Psychology (37) (2007) 658–682.
[38] E.M. Perse, Audience selectivity and involvement in the newer media environment, Communication Research (17) (1990) 675–697.
[39] R.E. Petty, J.T. Cacioppo, The elaboration likelihood model of persuasion, Academic Press, New York, 1986, pp. 123–205.
[40] R.E. Petty, J.T., C., D. Schumann, Central and peripheral routes to advertising effectiveness: the moderating role of involvement, The Journal of Consumer Research 10 (2) (1983) 135–146.
[41] J.W. Rigney, Learning strategies: a theoretical perspective, in: H.F. O'Neill Jr. (Ed.), Learning strategies, Academic Press, New York, 1978, pp. 165–205.
[42] E.M. Rogers, Diffusion of innovations, 5th ed.Free Press, New York, 2003.
[43] D.V. Shah, N. Kwak, M. Schmierbach, J. Zubric, The interplay of news frames on cognitive complexity, Human Communication Research (30) (2004) 102–120.
[44] A. Tsow, M. Jakobbson, Deceit and design: a large user study of phishing, Indiana University, 2007.
[45] J. Wang, R. Chen, T. Herath, H.R. Rao, An empirical exploration of the design pattern of phishing attacks, in: S.J. Upadhyaya, H.R. Rao (Eds.), Annals of emerging research in information assurance, security and privacy services, Emerald Publishers, 2009.
[46] M. Workman, Wisecrackers: a theory grounded investigation of phishing and pretext social engineering threats to information security, Journal of the American Society of Information Science and Technology (59) (2007) 662–674.
[47] M. Workman, Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, Journal of the American Society for Information Science and Technology 59 (4) (2008) 662–674.
[48] J.L. Zaichkowsky, Measuring the involvement construct, The Journal of Consumer Research (12) (1985) 341–352.

Arun Vishwanath (Communication, SUNY at Buffalo) is Associate Professor at SUNY Buffalo's Department of Communication and an adjunct professor in the Department of Management Science and Systems. His research focuses on consumer behavior and it applies to technology adoption and technology mediated interactions. His present research focuses on consumer information processing and consumer sense making processes. Dr. Vishwanath has authored and presented close to two dozen papers in leading Communication and Information Science journals and conferences. He has received research funding from AHRQ (NIH) and from the NYS Sea Grant.

Tejaswini Herath is an Assistant Professor in the Faculty of Business at the Brock University, Canada. Previously she worked as a systems analyst and part-time lecturer at UNBC, Canada. Her research interests are in Information Assurance and include topics such as information security and privacy, diffusion of information assurance practices, economics of information security and risk management. Her work has been published in the Journal of Management Information Systems (JMIS) and International Journal of E-Government Research (IJEGR). In addition she has presented papers at leading conferences and contributed several book chapters.

Rui Chen is an Assistant Professor of Information Systems at Ball State University. His research interests are in the areas of information assurance, emergency management, coordination and collaboration, and information technology outsourcing. Some of his publications have appeared in *Journal of the AIS*, *Communications of the ACM*, and other journals. He is also a Microsoft Certified System Administrator (MCSE) and Database Administrator (MCDBA).

Jingguo Wang is an Assistant Professor of Information Systems. He graduated from SUNY-Buffalo. His work has been published in *Information Systems Research*, *IEEE Transactions on Systems, Man, and Cybernetics (Part C)*, *European Journal of Operational Research*, and other journals, and received best paper awards at AMCIS and the International Conference on Internet Monitoring and Protection. His current research interests are in the areas of cybercrime and information security, information search, and decision making.

H. R. Rao (MIS, SUNY @Buffalo) graduated from Purdue. He has edited four books including "Information Assurance in Financial Services (Idea Group, 2007)". He has authored or co-authored more than 150 technical papers, and has received best paper and best paper runner up awards at AMCIS and ICIS. He has received research funding from NSF and DoD. He was a Fulbright fellow in 2004. He is the recipient of the 2007 SUNY Chancellor's award for excellence.