European Journal of Information Systems (2017) 26, 564–584
© 2017 The OR Society. All rights reserved 0960-085X/17
www.palgrave.com/journals

EMPIRICAL RESEARCH

Which phish get caught? An exploratory study of individuals′ susceptibility to phishing

Gregory D. Moody[1], Dennis F. Galletta[2] and Brian Kimball Dunn[3]

[1] Lee Business School, University of Nevada-Las Vegas, 329 BEH, Las Vegas, NV 89154, USA; [2] Katz Graduate School of Business, University of Pittsburgh, 282 Mervis Hall, Pittsburgh, PA 15213, USA; [3] Hunstman School of Business, Utah State University, 3500 Old Main Hill, Logan, UT 84322, USA

Correspondence: Gregory D. Moody, Lee Business School, University of Nevada-Las Vegas, 329 BEH, Las Vegas, NV 89154, USA.
Tel: (702) 895-1365;
E-mail: greg.moody@unlv.edu

Special Issue Editors:
Paul Benjamin Lowry, Tamara Dinev, Robert Willison

Received: 31 January 2016
Last Revised: 9 June 2017
Accepted: 14 June 2017

Abstract
Phishing, or the practice of sending deceptive electronic communications to acquire private information from victims, results in significant financial losses to individuals and businesses. The first goal of this study is to identify situational and personality factors that explain why certain individuals are susceptible to such attacks. The second goal is to test those empirically, along with previously identified factors, to explain the likelihood that an individual will fall victim to a phishing attack. We employed the Delphi method to identify seven personality factors that may influence this susceptibility (trust, distrust, curiosity, entertainment drive, boredom proneness, lack of focus, and risk propensity). Our regression model included these as well as variables examined in previous studies. We find that emails sent from a known source significantly increase user susceptibility to phishing, as does a user's curiosity, risk propensity, general Internet usage, and Internet anxiety. In post hoc tests, we also find that trust and distrust can be significant predictors of susceptibility and that this significance is dependent on the characteristics of the message.

European Journal of Information Systems (2017) **26**(6), 564–584.
doi:10.1057/s41303-017-0058-x; published online 19 July 2017

Keywords: phishing; information security; deception; ethical phishing experiment

Introduction

Individuals and organizations continue to increase their reliance on the Internet (Anandarajan, 2002; Cheung *et al*, 2000; Lim & Teo, 2005). This connectivity offers numerous benefits (e.g. Banker & Kauffman, 2004) but also introduces a number of threats to networked users' financial and information security (Dellarocas, 2005; Liang & Xue, 2009; Woon *et al*, 2005). Among the more serious of these threats is *phishing*, an attempt to acquire private information from victims through deceptive electronic communication (Jagatic *et al*, 2007).

According to recent data, damage from email phishing attacks has reached a half billion dollars in the USA alone, representing an increase of 2.370% from 2015 (Mathews, 2017). An estimated 3.3% of all individuals who receive a phishing email lose money as a result (Gartner, 2007). Firms bear a significant portion of this cost (Leung & Bose, 2008); a 2009 industry study found that 56% of phishing losses were absorbed by firms (Gartner, 2009). Further, phishing attack incidents have continued to grow over the last several years (Romanosky, 2016), suggesting that phishing is likely to remain a significant problem for firms unless measures are taken to ameliorate the threat (Sheng *et al*, 2010).

To develop better ways to avoid the damage caused by these attacks, several studies have considered the antecedents of phishing attack success from a variety of angles, including individual characteristics of phishing victims (Sheng *et al*, 2010; Workman 2008; Wright & Marrett, 2010; Wright *et al*, 2010, 2014) and characteristics of the attacks themselves (Jagatic *et al*, 2007; Vishwanath *et al*, 2011). This paper seeks to further develop this body of knowledge by simultaneously exploring personality and situational constructs that may increase the likelihood of an individual falling prey to a phishing attack. The ability to identify these individual- and message-related factors would enable organizations and individuals to understand who might be more susceptible to phishing and thus design better interventions or training methods to help these individuals increase their ability to identify phishing attempts.

In this study, we have followed the procedure used by Wang & Benbasat (2008) in their exploratory study on trust in an e-commerce context. In their study, the researchers identified several potential antecedents from the literature and then evaluated them using data collected through experimentation. For our research, potential antecedent constructs were identified both via literature review and through a Delphi-method study. Data were then collected from subjects using a survey and an “ethical phishing” experiment; these were then analysed to determine the significance of any relationships between candidate antecedents and phishing susceptibility.

The results of our study demonstrate that several situational factors do, in fact, alter the effectiveness of phishing attempts. We also find that certain personality traits can significantly impact an individual’s susceptibility to such attacks; this impact, however, is small.

Literature review

The threats posed by Internet abuse, including malicious online attacks, have been researched in a number of studies covering several contexts (e.g. Anderson & Agarwal, 2010; Chan *et al*, 2005; D’Arcy & Hovav, 2007; D’Arcy *et al*, 2009; Galletta & Polak, 2003; Grazioli & Jarvenpaa, 2000; Herath & Rao, 2009a, b; Johnston & Warkentin, 2010; Kankanhalli *et al*, 2003; Liang & Xue, 2009, 2010; Siponen, 2000; Siponen *et al*, 2006; Siponen & Vance, 2010; Straub, 1990; Straub & Goodhue, 1991; Sun *et al*, 2006; Theoharidou *et al*, 2005). Comparatively few papers have examined phishing specifically.

Those phishing-specific papers have, however, revealed significant findings related to the antecedents of phishing susceptibility. These antecedents have been considered from two primary angles: the attributes of the recipient of the email and the attributes of the email itself.

Studying individual characteristics, Workman (2008) considered user susceptibility to phishing attacks from a social engineering perspective. Social engineering here refers to manipulating or tricking individuals into performing certain actions (Mitnick & Simon, 2002). This is similar to the elaboration likelihood model (Petty *et al*, 1983) used in marketing, whereby advertisements and person-to-person interaction (e.g. talking with a salesperson) persuade consumers into action. This sort of trickery has a strong relationship with fear appeals and protection motivation theory (PMT) (Rogers, 1975; Johnston & Warkentin, 2010) in that a user is motivated to protective action when a message stimulates a fear response. Phishing attacks can use this fear response to their advantage, however, if they can persuade users that clicking on a phishing link is the response needed to protect themselves. Using a persuasion perspective, Workman (2008) tested a set of a priori user attributes that includes normative commitment, continuance commitment, affective commitment, trust, obedience, and reactance, finding that all but the last of these significantly predicted susceptibility to phishing attacks. Individuals who are more prone to fall for advertising campaigns and ‘slick’ salespeople are also more prone to fall for phishing attacks designed to persuade individuals in the same manner as advertisements.

Wright & Marett (2010) performed a similar study but instead focused on experiential and dispositional a priori factors. Their experiment revealed that a phishing attack was successful in persuading users to divulge a secret code where those users had less related experience, which was measured in terms of computer self-efficacy, web experience, and security knowledge. They also found that those who were more suspicious of humanity were less likely to be deceived. Interestingly, neither disposition to trust nor risk preference was significantly predictive.

Wright *et al* (2010) also considered the cognitive process of deception detection. In a qualitative study interviewing experimental participants who had successfully detected a phishing attempt, the authors proposed a process model of detection similar to a model suggested by Grazioli (2004). According to this model, a phishing email provides given cues (e.g. sender identity, subject line, email content). These cues may activate suspicion within the recipient, particularly where the cues are inconsistent with a priori expectations. Successful detectors then proceed to confirm their suspicions through hypothesis creation and then investigation. According to the authors, this process leads to a decision about whether to comply with the request of the (phishing) email.

Sheng *et al* (2010) focused on demographic characteristics, including gender and age, as predictors of phishing susceptibility, finding that women were more susceptible to phishing than men and that 18- to 25-year-olds formed the most susceptible age group. Vishwanath *et al* (2011) found that the number of emails received in a day and the extent to which the individual perceived the email’s message to be relevant to the individual increased the stated likelihood of a person responding to a phishing email, whereas an individual’s attention to textual details decreased the likelihood.

Turning to the content of the email itself, Wright *et al* (2014) tested the effectiveness of various influence techniques used within the context of phishing emails. They found that a number of techniques were successful in significantly predicting user compliance. These included liking the perceived sender, reciprocity (implying that the sender has done things for the recipient), social proof (purporting that a given behaviour is the correct social behaviour), consistency (implying that a given behaviour is consistent with past behaviours), authority (the message indicates that it is from someone in authority), and scarcity (making an opportunity appear less available). They also found that implying fictitious shared experiences decreased the effectiveness of the attack; meanwhile, techniques that offered a higher degree of self-determination increased effectiveness. In this study, females were more susceptible to phishing than males.

Finally, Jagatic *et al* (2007) used an *ethical phishing* technique, in which a simulated, non-harmful phishing email was sent to experiment subjects to explore whether the gender and familiarity of the apparent email sender altered the recipient's susceptibility to phishing attacks. To do this, the researchers scraped friend information from student subjects via a social network site and then sent an email with the subject 'Hey, check this out' and a link to a domain that was clearly not owned by the university. After clicking on the link, the site required them to log in. The study found that, in addition to the majority of subjects being willing to provide login credentials through a website that was not genuine, subjects were also more likely to respond when the email appeared to have been sent from a known friend, and males were more likely to respond to a message that appeared to originate from a female. They also found, consistent with Wright *et al* (2014), that women were more likely to click on provided links than men.

These and the other phishing-specific studies are summarized in "Appendix" Table 13.

Construct identification

The exploratory nature of this study dictated that we identify candidate constructs to consider as potential drivers of susceptibility to phishing. Initial candidates were identified through careful review of relevant literature in the information systems (IS) field as well as the fields of psychology and communication. We reviewed articles in this IS security research stream that focused on online deception or fraud and phishing in particular. This yielded a set of 13 candidate constructs.

We then conducted a Delphi study using the same methodological approach as that set forth by Brancheau *et al* (1996). The Delphi technique enables expert subjects to identify and produce a rank-ordered list of answers to given questions posed to the group. Given that our study focused on perceiving impropriety within emails, we identified email users as our expert group and, thus, 40 part-time graduate students taking an e-commerce course at a major university in the eastern USA were recruited.

In the first round of information solicitation, subjects were asked to name reasons people (themselves or others) might either (1) click or (2) not click links in emails received from both known and unknown apparent sources. Participants were instructed to supply their own answers to these questions (i.e. they were not privy to candidate constructs identified through the literature review or to suggestions made by other participants) and to rank their own responses in order of importance. Following this initial round, suggested reasons were rank ordered based on the aggregated rankings supplied by subjects. This new, ordered list was submitted to the group for reordering and augmentation in two additional rounds (in the final round of the study, no additional constructs were suggested, indicating that the list had reached its stable state within the group of experts), ultimately resulting in a list of 16 rank-ordered candidate reasons. In some cases, multiple suggestions were judged to be reflective of a single construct (e.g. there were a number of variations on the trust construct).

The resulting lists from both the literature review and the Delphi study were then compared. We found 12 constructs that were common between the previously identified constructs from the literature and the 16 reasons for phishing generated through the Delphi methodology, which we used as the basis for our exploratory study. As a result of this process, the set of constructs considered in this exploratory paper, though not exhaustive, constitutes an independently supported set of phishing susceptibility antecedents. These constructs are summarized in Table 1.

To further vet these 12 identified constructs, described in the next section, we performed a second Delphi study using Amazon Mechanical Turk (MTurk). In this second study, 200 participants were recruited via MTurk, all of whom had previous work on the platform and had acceptance rates at over 90%. We chose this platform to ascertain whether general email users would provide results similar to those obtained from graduate students. Further, recent work has highlighted that MTurk workers

Table 1 Summary of constructs that drive the decision to click on links in emails as based on literature review and two Delphi studies

Known source of email	Curiosity	Risk propensity
Text-based link	Entertainment drive	General Internet usage
Disposition to trust	Boredom proneness	Internet community identification
Disposition to distrust	Lack of focus	Internet anxiety

are more diverse than individuals identified through traditional data sampling techniques used in most behavioural research and would thus better generalize to the general population of email users than the previous sample we relied upon (Steelman *et al*, 2014; Lowry *et al*, 2016).

The same 12 constructs were identified in the first round of the Delphi study, with the inclusion of one additional construct (i.e. the expectation of the email). Although the final ranked order of the 13 constructs did not exactly match that of the original Delphi study, it still converged on the same 12 ideas, with the additional construct that was ranked last.

We thus propose that the identified constructs from the literature review and the two supporting Delphi studies provide us with a comprehensive set of candidate antecedent traits that may significantly predict susceptibility to phishing.

Hypothesis development

The 12 constructs fall into three discrete categories: message characteristics, personality traits, and Internet experience. Each of these categories and the constructs themselves are described below along with the hypothesized effect of each construct.

Message characteristics

Through our search, we found three characteristics of email messages that might be expected to have an impact on phishing success rates: message source (i.e. the apparent sender), link type (words or numerals), and message content. These characteristics are consistent with those noted as email authentication cues in Wright *et al* (2010). However, as in the study by Jagatic *et al* (2007), we opted to control for message content and avoided confounding effects by using the same message for all subjects.

Message source By *message source*, we refer to the apparent identity of the sender of the email; this variable has been shown to have a significant effect on the likelihood of an individual clicking on a link inside an email message (Jagatic *et al*, 2007). Source credibility theory (Sternthal *et al*, 1978) proposes that individuals are more prone to believe and rely upon information from individuals who are perceived as credible by the recipient. Further, lacking contextual information regarding the expertise of a given source, the information recipient will consider a known source to be more credible than an unknown source (Holden & Vanheule, 1999; Sternthal *et al*, 1978). Research has long proposed and found that familiarity leads to preference, which also increases the likelihood of a source being able to exert influence on a recipient (Burgoon & Burgoon, 2001; Petty & Wegener, 1998; Wright *et al*, 2014). Accordingly, we hypothesize that the perceived sender of a message is an important predictor of phishing susceptibility due to the perceived credibility of a known source. Although this finding has already been reported (Jagatic *et al*, 2007), we seek to examine this construct simultaneously with a set of other variables. This examination will enable an evaluation of relative strengths of various antecedents.

H1 *Messages from perceived known sources will produce higher rates of individuals clicking on links in phishing emails as compared to messages from unknown sources.*

Link type We also consider link type in our study. By *link type*, we refer to the form of the uniform resource locator (URL) that appears in the email message. Within this study, we considered two different link types: numeric and textual. A numeric link is one in which the numeric Internet provider (IP) address of the destination web server is used in the URL (e.g. a numeric link might look like this: 136.142.58.29/hci/asp3.aspx?x=99992); textual, on the other hand, uses links that indicate the server's text-based domain name in the URL (e.g. a textual link might look like this: www.actualurl.com/hci/asp3.aspx?x=99992). Given that the textual form is the one most commonly seen by users, we expect that a numeric address will raise a 'red flag' and thus alert users of a phishing email's potentially negative outcomes. Vishwanath *et al* (2011) found that awareness of such textual details significantly correlated with stated likelihood to respond to an email. Further, the textual URL conveys more information regarding the page to which the link points, which, we propose, engenders trust. We note, however, that the apparent URL need not be the one to which a link leads. In such cases, trust based on link type would be unfounded. In our study, we expect to find that a textual URL provides more attractive 'bait' for the would-be victim.

H2 *Messages with textual links will produce higher rates of individuals clicking on links in phishing emails as compared to those with numeric links.*

Personality traits

Our review of psychology and IS research yielded a number of personality traits that may impact an individual's susceptibility to phishing attacks. Through this research as well as our Delphi study, we identified seven candidate personality factors: trust, distrust, curiosity, entertainment drive, boredom proneness, lack of focus, and risk propensity.

Trust and distrust Given the important role of influence in the success of phishing attacks, trust and distrust are crucial constructs for consideration. *Trust* constitutes the willingness to be vulnerable to another person and to rely on another person to perform an expected behaviour (McKnight *et al*, 1998, 2002; Dimoka 2010). *Distrust*, on the other hand, has been defined as the *unwillingness* to be vulnerable to another person and the expectation that another seeks to harm the individual (McKnight *et al*, 2002; Dimoka, 2010). Due to this willingness to make oneself vulnerable, or not, trust and distrust have been found to predict a user's intent to engage or interact with another party or entity, for instance in the context of an e-commerce transaction (e.g. van der Heijden *et al*, 2003; Gefen *et al*, 2003; Everard & Galletta, 2006; Pavlou & Dimoka 2006) and in broader information technology (IT) adoption contexts (e.g. Hart & Saunders, 1997; Carter & Belanger, 2005; Vance *et al*, 2008).

Especially given the lack of context and interaction with potentially unknown attackers, a person's innate general trusting and distrusting dispositions towards others in general should have an effect on how the individual interacts with received emails. This expectation has been confirmed in some, though not all, past research into phishing susceptibility (e.g. Workman, 2008; Wright *et al*, 2010; Wright & Marett, 2010). We propose the following hypotheses:

H3 *Individuals with higher dispositions to trust will be more likely to click on links in phishing emails than those with lower dispositions to trust.*

H4 *Individuals with higher dispositions to distrust will be less likely to click on links in phishing emails than those with lower dispositions to distrust.*

Curiosity Psychological research has defined *curiosity* as the desire to find and attain new knowledge and to be exposed to novel experiences that motivate exploratory behaviours (Berlyne, 1960). Curiosity has been equated with an openness to experience (Costa & McRae, 1992; McElroy *et al*, 2007) and, within the IT context, has been further defined as excitement about the possibilities made possible by a technology (Webster *et al*, 1993).

Agarwal and Karahanna (2000) suggest that curiosity reduces the cognitive burden associated with engaging with a technology, thus increasing the individual's likelihood of doing so. Indeed, those with higher innate curiosity have been found to seek new opportunities within the online environment (Tuten & Bosnjak, 2001; McElroy *et al*, 2007), including a higher propensity to interact with commercial emails (Chen *et al*, 2011). We expect, then, that a more-curious individual who receives a phishing email may likewise be driven by their curiosity to click on a link that a less-curious individual might not.

H5 *Individuals with higher levels of curiosity will be more likely to click on links in phishing emails than those with lower levels of curiosity.*

Entertainment drive and boredom proneness *Entertainment drive*, or the need for entertainment, is the desire for novel sources of recreation or pleasure (Brock & Livingston, 2004). This coincides closely with the idea of *hedonic motivation,* or the drive for pleasure, which has been considered extensively in the hedonic motivation systems literature (e.g. Lowry *et al*, 2013), as well as the concepts of joy and enjoyment (e.g. Agarwal & Karahanna, 2000; van der Heijden, 2004). Those with a high entertainment drive, then, are those who seek pleasure and who tend to prefer prolonged use of an enjoyable interaction (van der Heijden, 2004). Entertainment has also been suggested to relate to high levels of engagement within a hedonic information system context (Goh & Ping, 2014); indeed, those who perceived greater enjoyment in an IS interaction have also reported a higher intent to use that system (van der Heijden, 2004). Those with greater entertainment drive may have a predisposition to perceiving higher entertainment value through increased engagement. We thus expect that those with a greater innate drive for entertainment may be more likely to click on phishing links and be more susceptible to such attacks.

Boredom proneness refers to an individual's disposition to feel that a current situation is uninteresting (Farmer & Sundberg, 1986). As such, it acts as a complement to entertainment drive: those with a high entertainment drive seek novel interactions; likewise those with high boredom proneness are likely to find current interactions boring and are more prone to attend to distractions. Building on the logic for entertainment drive, those with high levels of boredom proneness will opt to engage in a new activity, since this new activity could help to alleviate the boredom of their current task, which may have become tedious.

H6 *Individuals with higher levels of entertainment drive will be more likely to click on links in phishing emails than those with lower levels of entertainment drive.*

H7 *Individuals with higher levels of boredom proneness will be more likely to click on links in phishing emails than those with lower levels of boredom proneness.*

Lack of focus In this study, *lack of focus* refers to a person's inability to continue with a current task (Adler *et al*, 2006). Like boredom proneness, individuals with a high inability to focus quickly move from experience to experience (Adler *et al*, 2006). This construct aligns with the self-discipline facet of the conscientiousness construct found within the Big Five factors literature; an individual with low self-discipline is easily distracted (Costa & McRae, 1992). When an unknown link is presented to such a person, this lack of focus or lack of self-discipline is theorized to result in the individual breaking away from the task he or she is currently pursuing (e.g. reading email) and electing to click on the link. Thus, we expect that those with a lower ability to focus on current tasks will be more likely to click on links that may provide escape from those tasks.

H8 *Individuals with higher lack of focus will be more likely to click on links in phishing emails than those with less lack of focus.*

Risk propensity *Risk propensity* refers to the individual's disposition to accept uncertainty in various aspects of life and to engage in potentially risky behaviours (Nicholson *et al*, 2005). Research has shown that risk propensity is effectively opposed to trust (McKnight *et al*, 1998, 2002). Given the inclusion of trust in this study, it therefore makes sense to also include risk propensity. Additionally, other studies have found risk-related factors to influence individuals' perceptions of emails (Chen *et al*, 2011; Wang *et al*, 2009).

In operationalizing the risk propensity construct, we have elected to also look at various types of risk, including measures of propensity for taking risk in regard to recreation, health, career, finances, safety, and social decision-making settings. Individuals who are inherently more willing to take risks are expected to be more willing to engage in risky behaviours online, such as clicking on unknown links in emails.

H9 *Individuals with higher risk propensity will be more likely to click on links in phishing emails than those with lower risk propensity.*

Internet experience

In addition to personality factors, experience with the Internet is likely to serve as a potentially viable proxy for the expertise and experience that an individual may have accrued through Internet usage, with the assumption that such experience would inculcate the individual against falling prey to phishing attacks. Indeed, Wright & Marett (2010) found that experiential factors such as computer self-efficacy and security knowledge significantly predicted deception success within the phishing context. Our literature review and Delphi study led to the identification of three experience-related constructs: general Internet usage, Internet community identification, and Internet anxiety.

General Internet usage *General Internet usage* refers to the cumulative amount of time an individual spends online across a wide array of available activities (Joiner *et al*, 2007; McKnight *et al*, 2002). Past research has found that more experienced online users were more likely to avoid shopping online due to perceived security concerns (Hoffman *et al*, 1999). Our expectation, then, is that a similar phenomenon of enhanced awareness of security concerns will reveal itself within the email context and that individuals with greater online experience will better understand potential online risks and, therefore, will be less likely to click on unknown links. This understanding is likely to stem from a higher likelihood of previous encounters with warnings or discussions about these schemes. We thus expect that one's experience on the Internet will have led to the development of expertise that would allow them to identify potential phishing attempts and thereby avoid such attacks.

H10 *Individuals with a higher level of general Internet usage will be less likely to click on links in phishing emails than those with lower levels of general Internet usage.*

Internet community identification *Internet community identification* expresses the level of attachment between the individual and the Internet (Joiner *et al*, 2007). An individual with a high level of Internet community attachment will feel like part of an online community (Joiner *et al*, 2005) and, as such, is likely to rely more heavily on the Internet (Joiner *et al*, 2007). Given this higher level of online association, we expect that an individual with higher Internet community identification would be more likely to click on an unknown link, since doing so may be perceived as a means of deepening online social interactions. Further, those who feel strong attachment to the Internet community will have a heightened sense of reciprocity towards other Internet users. This perceived reciprocity should likewise increase the email recipient's motivation to click on links in received emails, as he or she would like other Internet users to also heed his or her messages (Posey *et al*, 2009; Wasko & Faraj, 2005).

H11 *Individuals with a higher level of Internet community identification will be more likely to click on links in phishing emails than those with lower levels of Internet community identification.*

Internet anxiety *Internet anxiety* reflects a user's general feeling of unease or apprehension towards the online environment. Unlike the previous two constructs, Internet anxiety creates a strong desire to avoid using the Internet and/or mitigate one's exposure to it (Joiner *et al*, 2007). Such anxiety towards IT has been found to result in a significant decrease in a user's willingness to trust a system (Hwang & Kim, 2007) as well as perceptions of a system's usability (Hackbarth *et al*, 2003; Cowan *et al*, 2008). Similarly, then, we expect that higher levels of Internet anxiety will result in a lower probability of clicking on an unknown link due to perceptions of lower ease of use and trust online. Both of these perceptions will decrease the likelihood of individuals extending their usage of the Internet by exploring an unexpected and unknown link.

H12 *Individuals with a higher level of Internet anxiety will be less likely to click on links in phishing emails than those with lower levels of Internet anxiety.*

Table 2 Summary of hypotheses

#	*Construct*	*Expectation*
H1	Known source of email	Higher susceptibility
H2	Text-based link	Higher susceptibility
H3	Disposition to trust	Higher susceptibility
H4	Disposition to distrust	Lower susceptibility
H5	Curiosity	Higher susceptibility
H6	Entertainment drive	Higher susceptibility
H7	Boredom proneness	Higher susceptibility
H8	Lack of focus	Higher susceptibility
H9	Risk propensity	Higher susceptibility
H10	General Internet usage	Lower susceptibility
H11	Internet community identification	Higher susceptibility
H12	Internet anxiety	Lower susceptibility

Summary of hypotheses

The 12 hypotheses considered in this paper are summarized in Table 2.

Methodology

To explore relationships between constructs and individuals' susceptibility to phishing scams, an experiment was conducted. For this experiment, 632 undergraduate psychology and IS students were recruited from a large public university in the eastern USA. Subjects were offered extra credit in their courses in return for their participation. Of these subjects, 53% were male, 44% were female, and 3% declined to state gender. The mean age of the subjects was 20.5 years (st. dev. 2.4 years), with the subjects having completed a mean of 4.5 semesters of college (st. dev. 2.3 semesters). Thirty-seven subjects were removed from the pool due to missing data, resulting in a final data set sample size of 595, which provided adequate power to predict small effect sizes for this study.

Design and procedures

The institutional review board (IRB)-approved experiment consisted of a randomized 2 (known vs. unknown email source) × 2 (text link vs. numeric link) online questionnaire with a follow-up phishing email. Subjects were told that they were part of a study that was concerned with their attitudes and beliefs related to websites and how to find information on the Internet; they were not told about the true purpose of the study. Subjects were directed to an online survey system where they then completed various information-retrieval tasks that had nothing to do with the phishing study. Following this, they were directed to complete an instrument to measure the personality traits used in the study and provide their email addresses. Participants were then thanked for their participation and dismissed; they were thus led to believe that the experiment had ended when, in fact, it had not.

Two weeks later, all participants received a plain-text email that presented one of four randomly assigned treatments corresponding to the four cells of the 2 × 2 design. The emails appeared to have been sent by either a *known source*, the individual with whom subjects had interacted with in signing up for the experiment, or an unknown source (a Ph.D. student from a different college and unknown to the subjects). The 2-week lag time was chosen to minimize any priming effect caused by the laboratory experience and at the same time ensure that subjects in the known sender group would remember the experimenter from whom the email appeared to have been sent.

For the subject line and body of the email, we followed Jagatic *et al* (2007), including generic content not specific to individual participants. The subject line read 'Your interesting results from our study'. The body of the email message consisted of similarly ambiguous text: 'Hi. Thank you for your participation in our project. For more information about your participation, please click on the following link. <URL>. We think you will find this fascinating and helpful'. In doing so, we avoided possible confounding effects that could have been introduced by the almost infinite possibilities of message and message presentation (Jagatic *et al*, 2007). The link to an external website presented within the email was shown either as (1) a text-based URL or (2) a numeric IP address. We tested the messages to make sure the university's spam filter did not prevent the messages from being delivered.

Subjects receiving the experimental treatment email then chose whether or not to click on the link. All links were encoded with a personalized code to identify participants uniquely. Thus, when a participant clicked on a link, the server captured the identification and stored it in a log from which it could later be matched to the data given by the participant in the survey portion of the experiment.

Measures

Dependent variable *Susceptibility to phishing* was measured on a binary scale. Subjects were scored 1 if they clicked on the link in the email or 0 if they did not click on the link.

Treatments *Email source* was encoded as a binary variable with the apparent known source (i.e. the principal investigator [PI] for the study, who served as the contact point and had emailed each participant in the study) coded as 1 and the apparent unknown source (i.e. an unknown co-author on this project to whom the participants in the study had had no exposure) coded as 0.

Source link was also encoded as a binary variable. The text link was coded 1, and the numeric IP address link was coded 0.

Independent variables *Disposition to trust* was measured using a version of the trusting beliefs instrument developed by McKnight *et al* (2002). Each sub-construct (benevolence, competence, integrity, and trusting stance) was measured using this instrument.

Similarly, *disposition to distrust* was measured using an adapted instrument reported in Moody *et al* (2014). As with disposition to trust, the individual sub-constructs (malevolence, incompetence, deceit, and distrusting stance) were measured.

Curiosity was measured along two dimensions, diversive and specific. Previous instruments developed to measure epistemic curiosity have used this same approach, and thus we follow established precedent (Litman & Spielberger, 2003).

Entertainment drive was measured using a previously developed instrument (Brock & Livingston, 2004). Several questions from the original instrument were not utilized in this study due to poor loadings found in the instrument's original explication; only the 14 items with loadings over 0.5 were included in our survey.

Boredom proneness was measured using a previously validated instrument (Farmer & Sundberg, 1986).

Lack of focus was measured using a previously validated instrument (Adler *et al*, 2006), available in both an extensive and a short version for determining the ability of an individual to focus. We opted to use the shorter version of the scale to avoid participant survey fatigue.

Risk propensity was measured using the risk propensity scale developed by Nicholson *et al* (2005). This scale delineates risk propensity as different propensities within various facets of life: recreational, health, career, financial, safety, and social risks. In addition, a measure of *risk beliefs* was taken based on the scale developed by Malhotra *et al* (2004), which specifically measures the perceived risk inherent within the Internet.

General Internet usage was measured using a previously validated instrument, specific for this type of study (McKnight *et al*, 2002).

Internet community identification was measured based on the conceptualization of Joiner *et al* (2007), which considered two types of Internet identification: identification with the Internet community at large and identification with other Internet users. We followed this conceptualization and measured both types of identification through previously established instruments (Joiner *et al*, 2007).

Internet anxiety was likewise measured using a previously established instrument (Joiner *et al*, 2007).

Control variables In addition, subject age (measured in years), level of education (measured in number of semesters completed at the university level), and gender (0 = female, 1 = male) data were gathered for consideration as control variables.

Factor analysis All reflective items were entered into a confirmatory factor analysis. From this, only factors with an eigenvalue equal to or greater than 1.0 were retained. Results were then rotated to ascertain the loadings of each indicator on its respective construct. Only high-loading items were used in construct calculation; following Nunnally & Bernstein (1994), we used a 0.7 cut-off point to identify them.

Based on these factor groupings, the Cronbach's alpha score for each construct was obtained to demonstrate convergent validity. Results are shown in Table 3.

Table 3 Construct validity

Grouping	*Construct*	*Sub-construct (# of items)*	*Cronbach's α*
Personality traits	Disposition to trust	Benevolence (2)	.738
		Competence (3)	.852
		Integrity (2)	.763
		Trusting stance (3)	.853
	Disposition to distrust	Malevolence (3)	.786
		Incompetence (3)	.861
		Deceit (2)	.692
		Distrusting stance (4)	.813
	Curiosity	Epistemic curiosity (diversive) (5)	.876
		Epistemic curiosity (specific) (3)	.748
		Perpetual curiosity (7)	.830
	Boredom proneness (4)	n/a	.520
	Entertainment drive (5)	n/a	.834
	Focus (2)	n/a	.705
	Risk propensity	Recreational (2)	.824
		Health (2)	.831
		Career (2)	.800
		Financial (2)	.838
		Safety (2)	.876
		Social (2)	.872
	Risk beliefs (5)	n/a	.881
Internet experience	General Internet usage (2)	n/a	.653
	Internet anxiety (2)	n/a	.681
	Internet community identification (3)	n/a	.891

All constructs were formed using item weights based on the loadings from the rotated factor analysis (Aiken & West, 1991; Rossi & Anderson, 1982; Weinberg & Abramowitz, 2008).

Divergent validity was assessed by ascertaining that the items not only loaded on their intended constructs but that they did not load on other unrelated constructs.

Analysis and results

An overall descriptive view of the results among the four treatment conditions is shown in Table 4, with descriptive statistics and correlations among the antecedents in Table 5. We found that 41.3% of subjects clicked on the enclosed links in the unsolicited emails.

Convergent and discriminant validities were also assessed using STATA's confirmatory factor analysis (CFA) during the structural equation modelling (SEM) analysis. As per CB-SEM standards, the model fit for the measurement model was acceptable ($\chi^2_{432} = 1735.740$; $\chi^2/df = 4.02$; CFI $= 0.970$; TLI $= 0.956$; RMSEA $= 0.068$; SRMR $= 0.092$; CD $= 1.000$). Convergent validity was established by large and standardized loadings for all constructs' t values ($p < 0.001$) that exceeded statistical significance and by the ratio of factor loadings to their respective standard errors that exceeded $|10.0|$ ($p < 0.001$) (Hair *et al*, 2011). Divergent validity was established by assessing the average variance extracted (AVE) for each construct, and our analysis reveals that each construct's score was above acceptable levels. Furthermore, we report that construct correlations to other constructs were less than the square root of the AVE score. As a final check on discriminant validity, we correlated each item to the constructed construct scores and found that items more strongly load only on their respective constructs. These tests all support discriminant validity.

Given the binary nature of the dependent variable, data were analysed using multiple logistic regression reporting coefficients models using STATA (v. 14.1 SE). The model reports the effects of the control variables on phishing susceptibility. The second model includes the treatment conditions in order to analyse the partial effect they have on the dependent variable. The last model includes all variables noted in the hypotheses (see Table 6). We compared these results with an SEM, which is shown in the last column of the table. We further note that, given the low explanatory power of our models, we have relaxed the significance threshold for significance to explore the constructs and the roles they play in explaining phishing susceptibility.

Discussion

The main objective of this study was to determine the message, personality traits, and Internet-related variables that relate to the likelihood of an individual's susceptibility to phishing attacks. We found and measured several variables that can increase this susceptibility. We analysed these results at multiple levels (basic, treatment level, and full model) and found several predictors, which we discuss here (Table 7).

Table 4 Summary of phishing results by treatment conditions

Behaviour	*Known sender*		*Unknown sender*		*Total*
	Text link	*Numeric link*	*Text link*	*Numeric link*	
Did not click	68 (44.4%)	68 (57.1%)	111 (65.7%)	102 (66.2%)	349 (58.7%)
Clicked	85 (55.6%)	51 (42.9%)	58 (34.3%)	52 (33.8%)	246 (41.3%)
Total	153	119	169	154	595

Percentages in parentheses reflect the percentage in each treatment condition that clicked or did not click on the link.

Table 5 Measurement model statistics
***Note*: Bolded diagonals represent the square of the AVE**

Construct	*Mean*	*SD*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1. Disposition to trust	3.860	0.900	**0.858**									
2. Disposition to distrust	2.522	0.801	0.612	**0.813**								
3. Curiosity	1.778	0.363	−0.011	−0.026	**0.811**							
4. Entertainment drive	2.598	0.624	−0.036	0.084	0.073	**0.798**						
5. Boredom proneness	1.918	0.447	−0.077	−0.086	−0.089	−0.192	**0.733**					
6. Lack of focus	1.604	0.310	−0.082	−0.119	0.019	−0.193	0.461	**0.718**				
7. Risk propensity	2.450	1.002	−0.064	−0.087	0.067	−0.118	0.037	0.107	**0.805**			
8. General Internet usage	1.227	0.588	−0.022	−0.013	0.021	−0.078	0.068	0.096	0.085	**0.710**		
9. Internet community identification	2.038	0.624	−0.088	0.034	−0.056	0.276	−0.057	−0.006	0.052	−0.039	**0.899**	
10. Internet anxiety	3.045	0.518	0.044	0.202	−0.050	0.051	−0.003	−0.016	0.062	0.091	0.027	**0.734**

Table 6 Summary of phishing results for partial and full models
***Note*: Pseudo-*R*^{2} goodness of fit metric for OLS-based regression, akin to *R*^{2} from ML-based regression**

Construct	*Baseline model*		*Treatment model*		*Full model*		*SEM*	
	Coef.	*p*	*Coef.*	*p*	*Coef.*	*p*	*Coef.*	*p*
Age	0.028	0.691	0.033	0.646	−0.070	0.456	−0.082	0.490
Education	−0.026	0.669	−0.032	0.591	0.012	0.877	−0.003	0.983
Gender	−0.259	.239	−0.233	0.293	0.033	0.902	−0.047	0.591
H1. Known source of email			**0.519**	**0.019**	**0.339**	**0.078**	**0.159**	**0.050**
H2. Text-based link			−0.026	0.906	0.070	0.789	0.014	0.868
H3. Disposition to trust					0.075	0.683	0.028	0.751
H4. Disposition to distrust					−0.020	0.923	0.067	0.528
H5. Curiosity					**0.615**	**0.039**	**0.443**	**0.066**
H6. Entertainment drive					−0.088	0.706	0.121	0.198
H7. Boredom proneness					0.174	0.595	0.199	0.146
H8. Lack of focus					−0.003	0.994	−0.018	0.867
H9. Risk propensity					**0.197**	**0.041**	**0.183**	**0.033**
H10. General Internet usage					**0.326**	**0.037**	**0.197**	**0.072**
H11. Internet community identification					−0.232	0.100	−0.099	0.165
H12. Internet anxiety					**0.297**	**0.081**	**0.229**	**0.075**
Constant	.200	.880	−0.126	0.925	−1.167	0.611	n/a	n/a
Goodness of fit measures								
χ^2		39.66		108.91		280.61	$R^2 = 0.094$	
Prob > χ^2		0.667		0.330		0.093		
Pseudo-R^2		0.003		0.015		0.090		

Bold text indicates a significant correlation; $p < .010$.

Table 7 Summary of results

#	*Construct*	*Expectation*	*Result*	*Effect size*
H1	Known source of email	Higher susceptibility	Sig. (<.001)	.249
H2	Text-based link	Higher susceptibility	N.S.	.012
H3	Disposition to trust	Higher susceptibility	N.S.	.059
H4	Disposition to distrust	Lower susceptibility	N.S.	.060
H5	Curiosity	Higher susceptibility	Sig. (<.10)	.281
H6	Entertainment drive	Higher susceptibility	N.S.	.087
H7	Boredom proneness	Higher susceptibility	N.S.	.025
H8	Lack of focus	Higher susceptibility	N.S.	.012
H9	Risk propensity	Higher susceptibility	Sig. (<.05)	.200
H10	General Internet usage	Lower susceptibility	Sig. (<.10)	.281
H11	Internet community identification	Higher susceptibility	N.S.	.103
H12	Internet anxiety	Lower susceptibility	Sig. (<.10)	.215

Effect size is calculated using Cohen's *d*. Effect size interpretation: Medium effect sizes: between 0.20 and 0.50; Small effect sizes: less than 0.20.

Post hoc analysis

Further, given that these tests revealed that user susceptibility was significantly predicted by our manipulations, we performed several post hoc analyses to better understand the nature of these effects.

Trust and distrust Neither disposition to trust nor to distrust was statistically significant as a main effect in predicting the susceptibility for phishing, consistent with results from earlier studies (e.g. Wright & Marett, 2010). Each of these constructs was composed of four sub-constructs. We thus considered whether the impact of trust might be obscured by sub-constructs working in opposite directions. We followed the same analytical procedures as noted above, except that we included the sub-constructs of trust and distrust, rather than the full constructs, into the model for predicting phishing susceptibility. This further analysis revealed several interesting findings, summarized in Tables 8 (trust) and 9 (distrust).

Table 8 Summary of effects by the sub-constructs of trust

Construct	*Known source*				*Unknown source*			
	Text link		*Numeric link*		*Text link*		*Numeric link*	
	Coef.	*p*	*Coef.*	*p*	*Coef.*	*p*	*Coef.*	*p*
Benevolence	**−0.338**	**0.055**	**0.270**	**0.056**	0.238	0.213	0.168	0.641
Competence	0.081	0.799	**−0.370**	**0.077**	0.150	0.652	0.232	0.502
Integrity	**−0.240**	**0.059**	**−0.206**	**0.061**	**−0.485**	**0.098**	−0.239	0.527
Trusting stance	0.168	0.559	**0.648**	**0.041**	**0.426**	**0.088**	−0.180	0.454
Constant	2.124	0.135	−0.901	0.588	−1.022	0.447	0.201	0.887
Pseudo-R^2		0.049		0.049		0.039		0.001

Bolded values indicate significant results.

Table 9 Summary of effects by the sub-constructs of distrust

Construct	*Known source*				*Unknown source*			
	Text link		*Numeric link*		*Text link*		*Numeric link*	
	Coef.	*p*	*Coef.*	*p*	*Coef.*	*p*	*Coef.*	*p*
Malevolence	**−0.336**	**0.081**	**−0.257**	**0.059**	−0.016	0.971	0.456	0.120
Incompetence	−0.157	0.464	−0.149	0.654	0.134	0.654	−0.049	0.882
Deceit	**0.547**	**0.084**	**0.842**	**0.047**	**−0.552**	**0.055**	0.010	0.983
Distrusting stance	−0.357	0.103	**0.683**	**0.039**	0.111	0.724	−0.189	0.521
Constant	1.786	0.149	−1.281	0.299	0.411	0.691	−0.427	0.706
Pseudo-R^2		0.031		0.079		0.014		0.013

Bolded values indicate significant results.

First, we find that trust actually does appear to affect phishing susceptibility when the truster knows the trustee. This can be inferred from the number of significant relationships in the known source conditions. However, we see fewer significant effects for the unknown source conditions. Further, trust sub-constructs appear to become even more important when evaluating whether to click on a numeric link from a known source when compared to the text link. Thus, we infer that a general belief in the integrity of others becomes a mildly significant factor when the source of the email is known. However, the three significant results pertaining to the perceived integrity of others measure have negative directionality. This is a counter-intuitive finding in that, if one believes that others have their own interest at heart, one should be expected to be *more* trusting and, therefore, more willing to click on a phishing email link. It is an interesting finding that might indicate that trusting people are self-aware of their higher perception of integrity and might consciously decide to be more cautious as a result, paying attention to signals that they know might put them in danger. This provides an interesting avenue for future research.

We also find that trust is significant when the source of the email is known to the recipient yet the link is numeric. This is likely due to the mixed signals inherent within this situation. The source is known, and thus more likely to be trusted, yet the link is entirely unknown. Building on the work of Moody *et al* (2017), we propose that the mixed signals cause the individual to engage in deeper processing, as both trusting and distrusting signals are present within the situation. These mixed signals are likely to result in a level of suspicion, which can only be overcome by a conscious appraisal of trust.

Likewise, we find that distrust follows a similar pattern of (weakly) significant responses. Distrusting beliefs have a more significant role when the source of the email is known. Belief in the deceitfulness of others appears to be a particularly useful determinant. When the source of the email is known, this general deceit belief tends to increase the recipient's inclination to click on the link, an effect that is reversed when the source is unknown. On the other hand, when the recipient believes in general that others are intending to cause harm when possible (malevolence), they are less likely to click on the link, but only when the source is known.

Similar to the pattern of results regarding trusting beliefs, we find that the distrusting sub-constructs are most significant when the source of the email is known and the link is numeric. Again, this is likely due to the increased processing that occurs in response to mixed signals. We note that these post hoc analyses are quite exploratory, especially given that these tests are performed after our initial model shows that main effects are non-significant.

In summary, despite the lack of a main effect, we nevertheless find that the dispositions to trust and distrust have some effect on phishing susceptibility. Specifically, these dispositions tend to impact one's susceptibility when the sender of the email is known, especially with a numeric link, when compared to an unknown source.

These findings show that non-contextual, non-message characteristics can impact the decision to click on a link in an email. Past research has shown a mixed relationship between trust and phishing susceptibility. Workman (2008) and Wright *et al* (2010) found significant relationships, but Wright & Marett (2010) did not find significance. Our findings indicate that there may be important interactions to consider in understanding the salience of a priori trust dispositions, in particular with regard to the identity of the sender. This is especially important in considering spear phishing and other deception techniques involving a high amount of personal relevance and trust, particularly in situations involving social networks.

Our trust-related findings also have strong implications for IS behavioural security. A considerable body of the behavioural security literature involves PMT, which suggests that users will engage in self-protective behaviour when they believe that a threat is severe and that their behaviour can be effective in addressing it (Rogers, 1975; Johnston & Warkentin, 2010; Johnston *et al*, 2015; Boss *et al*, 2015). In doing so, most of this literature assumes that when a user appraises communication, the appraisal is considered on the merits of the communication alone. Only recently have researchers begun considering other factors that play a significant role in informing a user's threat-motivated action intentions. For instance, Posey *et al* (2015) considered employees' a priori sense of commitment to their organization in predicting protective behaviours on the basis of fear appeals.

Most IS-related PMT research considers behavioural intent in a positive context (e.g. a user responding to an employer's fear appeal responds by more carefully protecting login credentials). However, fear appeals can also be used by phishers as means of persuasion. As alluded to by Workman (2008), some of the concepts that work in consumer advertising can be effective in phishing attacks as well. Consider, for instance, a common phishing communication in which the recipient is told that a banking account has been compromised and that the recipient needs to log into their account to reset it. Such a communication makes a strong fear appeal and suggests to the recipient an easy, protective remedy (clicking and logging in, thus providing the user's credentials to the attacker). In such situations, it seems reasonable that the fear appeal used by the attackers is strengthened through other recipient-specific conditions, including trust.

While the e-commerce literature stream has shown that trust reduces complexity (Gefen & Straub, 2004) by allowing individuals to evaluate signals from others (Lowry *et al*, 2008), this logic has not been applied to behavioural security research. Where phishing messages are fear appeals, their success may depend on a sense of urgency or scarcity and/or an appeal to previously shared experiences between the sender and recipient (Wright *et al*, 2014). These shared experiences could reasonably be considered a proxy for trust. Our results show that trust differentially impacts the success of phishing messages. Further, this suggests that perceptions of trust towards the sender could either increase the probability of attack success (Lowry *et al*, 2008) or decrease it (Schul *et al*, 2004, 2008; Lowry & Moody, 2015). We have explicitly tested the assumed linkage of shared context between the potential victim and the sender of the phishing message by exploring how trust impacts phishing and call on future research to further investigate trust as part of the nomological network of behavioural information security, including its relationship to PMT.

Personality traits Contrary to our expectations, we found only two instances where personality traits had a main effect on phishing susceptibility: curiosity and risk propensity. We performed post hoc analysis, as before, to determine whether our identified personality traits have opposing relationships between the treatment conditions that might explain main effect non-significance. The results of our post hoc analysis, similar to that of trust and distrust, shown in Table 10, explore how personality trait main effects were altered by our manipulations.

Table 10 Summary of personality trait higher-order constructs by treatment conditions

Construct	*Known source*				*Unknown source*			
	Text link		*Numeric link*		*Text link*		*Numeric link*	
	Coef.	*p*	*Coef.*	*p*	*Coef.*	*p*	*Coef.*	*p*
Curiosity	**0.598**	**0.037**	**0.432**	**0.017**	−0.331	0.464	**0.707**	**0.016**
Entertainment drive	**−0.315**	**0.071**	**−0.651**	**0.018**	0.030	0.942	0.467	0.079
Boredom proneness	0.264	0.151	**0.698**	**0.040**	**−0.568**	**0.065**	**0.535**	**0.074**
Lack of focus	−0.031	0.286	0.361	0.525	**0.326**	**0.094**	−0.112	0.892
Risk propensity	**0.418**	**0.061**	0.091	0.787	−0.031	0.911	0.096	0.760
Constant	1.076	0.650	−0.576	0.812	0.187	0.925	−2.946	0.183
Pseudo-R^2		0.075		0.050		0.004		0.042

Bolded values indicate significant results.

Analysing manipulations in isolation, we find that curiosity has a significant effect on phishing susceptibility across three of the four conditions. Given the nature of the message, it is not surprising that curiosity was an important trait that impacted this decision.

Entertainment drive provided a counter-intuitive result in the known source condition, suppressing susceptibility. This was particularly surprising given the significant positive effect of curiosity. We suspect that an email received from a known source that was not known in an entertainment-oriented context may lead to an email click being considered ‘work’, or, at least, an option whose entertainment value is lower than alternative options. Having only communicated with the PI in an official capacity, it could be expected that any link from the person would be informational, and not entertaining, thus those who look for entertainment would be less likely to rely upon the known source. Especially given Wright *et al*’s (2014) finding of the significance of liking the sender in promoting susceptibility, we suspect this finding may reverse for known senders with whom the recipient has an entertainment-centred relationship.

Boredom proneness also had diverse results across the conditions. Specifically, we find a weakly significant effect for boredom proneness suppressing susceptibility when the message was from an unknown source but contained contextual information within the link. However, when the link provided no such information, then those prone to boredom were much more likely to click on the link. This highlights that when boredom-prone individuals receive an unexpected email lacking content cues, the recipient may be more likely to click on the link. Interestingly, this was generally the strongest effect in any of the models.

We also find that the lack of focus had a significant impact only when the source was not known but the link was textual. Risk propensity, despite having a significant main effect, was only significant in the known source, text link condition, when conditions were analysed individually.

These two findings suggest that, despite a dearth of significant main effects, personality traits may yet be an important consideration for phishing susceptibility. Past phishing susceptibility research has considered the predictive ability of dispositional factors such as suspicion and trust propensity (e.g. Workman, 2008; Wright *et al*, 2010; Wright & Marett, 2010). Our findings complement those by including, in addition, personality factors. Thus, practitioners can have a better sense of not only what training is important to help deflect phishing attacks but also know more about which people may be more in need of such training.

Additionally, as noted with regard to trust and distrust, the majority of phishing and IS behavioural security research has relied upon the theoretical background of PMT, which proposes that fear appeals persuade individuals to protect themselves from threats. User interpretations of content-based fear appeals have not undergone extensive scrutiny, but, in general, security research seems to assume that individuals will either behave rationally to protect themselves from threats or behave irrationally and not do so. Our results show that individual traits might alter how a persuasive message is interpreted, which complicates the job of researchers. As has been the case, PMT research should certainly include a personally relevant (Johnston *et al*, 2015) fear appeal (Boss *et al*, 2015) that considers the threat and the efficacy of the individual and the proposed response. However, future researchers should also consider how the context of the message might interact with individual differences among recipients and account for personality traits that might affect the message’s persuasive power.

Internet experience The recipient’s experience with the Internet was the most predictive grouping of variables tested in all of our models. Here we found two main effects: general Internet usage and Internet anxiety tend to increase phishing susceptibility. We also performed an additional post hoc analysis, entering only these constructs into our model, to see whether these effects are consistent across the manipulations. These results are summarized in Table 11.

First, the more a recipient used the Internet, the more likely that person was to click on links in unsolicited emails. This finding is contrary to that of prior research (Wright *et al*, 2010; Wright & Marett, 2010), where Internet experience was negatively related to phishing susceptibility. We speculate that experience could result

Table 11 Summary of Internet-related constructs by treatment conditions

Construct	*Known source*				*Unknown source*			
	Text link		*Numeric link*		*Text link*		*Numeric link*	
	Coef.	*p*	*Coef.*	*p*	*Coef.*	*p*	*Coef.*	*p*
General Internet usage	**0.423**	**0.031**	0.072	0.335	**0.289**	**0.092**	0.120	0.799
Internet community identification	**0.285**	**0.164**	**−0.458**	**0.030**	−0.232	0.234	**−0.747**	**0.025**
Internet anxiety	0.211	0.512	**0.662**	**0.064**	−0.031	0.939	0.104	0.826
Constant	−0.263	0.850	−2.180	0.335	1.030	0.492	1.006	0.571
Pseudo-R^2		0.018		0.067		0.006		0.049

Bolded values indicate significant results.

in greater susceptibility due to previous (benign) experience with such emails and the belief that the recipient will be able to continue to avoid potential negative consequences in the future. It may also be that people who use the Internet a lot may do so in part because of their willingness to click on various links. We note that this main effect appears largely driven by the text-based link conditions and not numeric links. Given these unexpected findings, this appears to be an area that would benefit from future research.

Second, we find that identification with the Internet community decreases susceptibility to phishing. The propensity to click on the link from the unexpected email is markedly lower when the link is numeric. It appears that those who identify with the Internet have acquired a level of expertise and therefore rightly note the unusualness of the link type and avoid clicking on it.

Lastly, we find that the main effect of Internet anxiety is largely driven by the anxiety produced when a numeric link is encountered from a known source. Again, building on the work of Moody *et al* (2016) and Grazioli (2004), this may occur in response to the competing signals that the recipient perceives due to the trust inherent in a known source but also due to the abnormality inherent within the numeric link, which will trigger suspicion.

In summary, the individual's experience with and attachment to the Internet were the two important factors in determining phishing susceptibility. Generally, individuals who are very frequent users of the Internet were more likely to click on links in emails. By contrast, individuals who have anxiety towards the Internet or who are strongly identified with other Internet users were less likely to click on the links.

In most prior research, when Internet experience is included as a control variable, it is presumed that its effect is constant across all manipulations. However, our results show that experience will only be significant when the context aligns with the experience. Thus, the less 'standard' a phishing attack is perceived to be, the less experience may be a factor.

Further, experience tends to rely upon habituated responses (Moody & Siponen, 2013). Phishing messages may trigger suspicion and thus require non-habituated responses (Moody *et al*, 2014). Ongoing IS research should thus consider when signals will result in non-standard contexts and thus preclude the expected effects of past Internet experience.

We also find that identification with the Internet community and Internet anxiety have significant outcomes on phishing susceptibility. Identification with the Internet community lowers the susceptibility, while Internet anxiety increases it. Both are unexpected findings, and additional research should replicate our study to make sure this was not simply found by chance. It is particularly difficult to explain why anxiety would increase susceptibility, but it is possible that some users with greater anxiety are also bothered by unresolved messages.

Demographics and manipulations

Contrary to previous studies (Jagatic *et al*, 2007; Kumaraguru *et al*, 2009b; Sheng *et al*, 2010; Wright *et al*, 2014), gender was not a statistically significant predictor of phishing in the present study. Given that this study used a variety of predictors and used email as its phishing attempt, it may systematically differ from these previous studies. With the ubiquitous use of email, perhaps it should be expected that both genders have been equally and highly exposed to multiple phishing attempts and are thus now equally prepared to identify and prevent phishing attempts. We also note a similar lack of results for age, which also contradicts previous studies (Kumaraguru *et al*, 2009b; Sheng *et al*, 2010). However, considering that our subjects were of similar age (standard deviation of 2.4 years) and that our analysis was performed with a limited range of data, this is not necessarily surprising. On the other hand, we found that the level of education served as a strong deterrent of phishing success. This effect was predictable and held for most models.

Our known versus unknown sender manipulation was a strong predictor of phishing susceptibility. Specifically, by sending a message from a known source, it is more likely that the recipient will fall prey to the phishing attempt. As expected, familiarity with the source generated enough trust that the recipients relied upon this relationship and were more likely to be phished.

General implications for research

This study makes several contributions to the research on phishing (these are summarized in Table 12). This is the first such large-scale experimental exploratory study that simultaneously considers several theoretical constructs to determine their effect on individuals' susceptibility to phishing and does so by using an objective dependent variable – tracking subjects' actual clicking behaviour. By further explicating and testing the underlying theories, we show which dimensions serve as accurate and reliable predictors of phishing susceptibility.

In particular, we show that the most important of the stable predictors of phishing susceptibility is previous experience with the Internet – that is, frequent users of the Internet are more susceptible to phishing. Perhaps previous safe usage leads individuals to feel greater comfort than may be warranted. Receiving many emails without any problems might allow Internet users to let down their guard. This effect can be impacted by the individual's anxiety towards the Internet and/or identification with other Internet users.

Our results advance the prior research on phishing and individual characteristics. Workman (2008) found that three types of commitment (affective, continuance, and normative) were the most important predictors of phishing. However, the results from this study did not find similar support for identification (commitment) to the Internet community. This juxtaposes with the findings of Wright & Marett (2010) that those with less experience

Table 12 Summary of findings and contributions for research

Finding	*Contribution*	*Source*
1a. Users receiving an email from a known source are more susceptible to phishing 1b. Users with a higher curiosity drive are more susceptible 1c. Users with a higher propensity to take risks are more susceptible 1d. Users who report greater usage of the Internet are less susceptible 1e. Users who report greater anxiety related to Internet usage are less susceptible	1. Both message source characteristics and a priori individual characteristics exhibit main effects for predicting a user's phishing susceptibility	Table 7
2a. Belief in the benevolence of others decreases susceptibility to phishing when the source of an email is known and a text link is used, but increases it when the source is known and a numeric link used 2b. Belief in the competence of others decreases susceptibility when the source of the email is known and a numeric link is used 2c. Belief in the integrity of others generally decreases susceptibility 2d. Trusting stance increases susceptibility for both known sources with numeric links and unknown sources with text links	2. Dispositions to trust is predictive of phishing susceptibility when sub-dimensions of the construct (benevolence, competence, integrity, trusting stance) are isolated	Table 8
3a. Belief in the malevolence of others decreased phishing susceptibility when the source of the email was known 3b. Belief in the deceitfulness of others increased susceptibility for known sources, but decreased it for unknown sources where a text link was used 3c. Distrusting stance increased susceptibility for emails from a known source where a numeric link was used	3. Disposition to distrust is predictive of phishing susceptibility when sub-dimensions of the construct (malevolence, deceit, distrusting stance) are isolated	Table 9
4a. Curiosity, generally, increases phishing susceptibility 4b. Entertainment drive has a negative impact on phishing susceptibility if it the email is perceived as coming from a known source. It has a positive impact when it the email comes from an unknown source with and uses a numeric URL 4c. Boredom proneness increases phishing susceptibility when the URL is numeric, but reduces phishing it when a text link is sent from an unknown source 4d. Lack of focus increases phishing susceptibility when a text URL is received from an unknown source 4e. Risk propensity increases phishing susceptibility when a text URL is received from a known source	4. Stable personality traits (curiosity, entertainment drive, boredom proneness, lack of focus, risk propensity) impact one's affect a user's susceptibility to being phished phishing. Specifically, curiosity, Internet anxiety, and risk propensities are of importance	Table 10
5a. General Internet experience increases phishing susceptibility when the link is text-based 5b. Internet community identification decreases susceptibility when the link is numeric 5c. Internet anxiety increases susceptibility when the email is sent from a known source and the link is numeric	5. Factors related to an individual's perception and use of the Internet predict phishing susceptibility	Table 11
6a. Phishing susceptibility was *not* significantly predicted using demographic factors of gender, age, and education	6. Unlike earlier studies, demographics were not significant predictors	Table 6

online and less computer self-efficacy were more likely to reveal a secret code. Perhaps the distinction between our findings and those of Wright and Marett's study is due to the differing contexts. Revealing an endogenous-to-the-experiment secret code is quite distinct from clicking on a link in an actual email.

This study was the first to explore personality traits in the phishing context, and we report that curiosity, Internet anxiety, and risk propensities are important predictors. These personality traits should be measured and controlled for in future studies on phishing susceptibility.

Like prior work, we also find that the context regarding the phishing email itself impacts whether the phishing attempt is successful. Specifically, along with all prior research on phishing, having a known source of the message drastically increases the user's phishing susceptibility.

We also demonstrate that individuals seem to have an optimistic bias regarding their own susceptibilities to phishing. Specifically, they understand the potential dangers of phishing attacks, but when presented with such an attack, they fall prey to it. In addition, whereas previous work (Wright & Marett, 2010) has not found significant results for risk disposition affecting phishing susceptibility, our study shows financial risk propensities to correlate significantly. This may indicate the salience of financial risk inherent in phishing attacks to financial risk-averse recipients.

Finally, our study considered both message-specific and a priori user constructs simultaneously. This enabled us to uncover significant interaction effects not studied in prior research.

Implications for practice

Our results suggest several ways in which an individual's phishing susceptibility can be lessened and safer behaviours and practices encouraged. First, given that the manipulations of the source and type of link were very consistent in producing increasing susceptibility for phishing, training programs can be created to focus on identifying and increasing individuals' awareness of such situations. Namely, technical authentications (e.g. private and public key encryption, digital signatures, and email filter protocols) can increase the abilities of email users to identify and verify the actual identities of those sending messages that may or may not be phishing attempts. Further, educating individuals about the dangers of relying on textual links would potentially help alleviate users' clicking on similar, harmful links. However, even with education, individuals may still be overconfident in their abilities and thus fall prey to phishing. Nevertheless, education and/or training should strongly emphasize the need to tame overconfidence (Alba & Hutchinson, 2000).

Second, by increasing the focus and direction of phishing education campaigns on the risk to finances, users' natural risk propensities towards financial loss may also reduce their susceptibility to phishing attacks.

Third, education campaigns should be directed towards frequent users of the Internet and the inherent susceptibility to phishing messages that they exhibit. Increased usage of the Internet will lead to greater likelihood that individuals will be confronted with numerous phishing attacks, which in turn increases their likelihood of falling prey to phishing attempts. It is also possible that individuals with high Internet use, risk propensities, or boredom proneness can be identified and thus given additional aide through stricter email filtering, more pervasive warnings, or other tools that help them to identify potentially harmful links in email messages.

Finally, given that the largest effect size in the model is related to individuals with boredom proneness and numeric links from known individuals, special education could be devised to alert individuals with such tendencies. In particular, they should be informed of the propensity of phishing attacks to include suspicious URL addresses as links.

Future research directions

Given the exploratory approach of this study, we expect that our findings will help open a number of doors for future researchers. For instance, our study yielded a number of findings that were tantalizing yet vexing with regard to their statistical significance. In considering the p values yielded by our analyses, a number of relationships were only weakly significant, with p values in the range between .05 and .1. We feel that part of this is due to our decision to investigate a large number of candidate antecedents simultaneously, some of which had not been previously found to strongly correlate to similar dependent variables (e.g. curiosity, lack of focus). As such, the experiment was not designed to enable us to focus specifically on any small subset (let alone any individual) antecedent construct.

Given this, however, the fact that our study found as many weakly significant results as it did suggests that many of these variables deserve further, focused investigation with regard to their influence on phishing susceptibility and related security concerns. For instance, our post hoc tests showed that boredom proneness weakly predicts susceptibility to phishing in cases of a known sender and a numeric link ($p = 0.040$), an unknown sender with a text link (negative direction, $p = 0.065$), and an unknown sender with a numeric link ($p = 0.074$). These results suggest that boredom and boredom proneness could, in fact, be not merely weak but rather excellent predictors of phishing susceptibility given the presence of other factors. Are certain messages and persuasion types particularly effective for boredom-prone individuals? Can priming users into a bored or less-bored state affect their susceptibility? Our results suggest that such questions would be worth exploring.

Indeed, our findings suggest that contextual cues are important in determining phishing susceptibility. Again, knowing the source of the email was found to have a significant main effect on susceptibility. We suspect that this main effect is due to the arousal of feelings of trust towards the sender, which in the known sender condition of our study was likely enhanced by participants being aware of having been part of a data collection prior to receipt of the experimental phishing email. It would be interesting for future researchers to further manipulate this degree of context and level of familiarity with the sender. If a sender is known through an on-campus encounter (as in our study), this may have a stronger or weaker effect than a sender known through other situations (e.g. known socially, known from work, having met and talked personally on several occasions, etc.).

Further, beyond the sender, the email content in our study was particularly simple and provided participants very few contextual cues as to its origin or intent. Instead, the content consisted of brief, generic, non-customized wording along with the phishing link. Although this message was similar to some actual phishing emails used in practice, it is important to acknowledge that, in practice, a diverse array of messaging types are used in phishing attacks. As such, it is possible that our findings may not generalize beyond phishing emails using similarly simple content. It would thus be important to investigate whether similar findings would continue to hold when tested across a greater variety of phishing email content types. For instance, it is easy to imagine an individual with a high curiosity drive being even more susceptible to messaging that appeals to this curiosity or for those with greater disposition to distrust to fall prey more easily to a strong fear appeal.

We also note that, unlike some prior studies, we saw no main effect for gender or age on phishing susceptibility. This could be the result of the passage of time (i.e. previous gender- and age-related differences might have diminished as a result of email recipients having become more experienced and/or knowledgeable), or it may be an artefact of our student sample. That said, we believe our sample was appropriate in that students represent a significant component of the population of potential phishing victims and that data collected from this sample do indicate the presence of some interesting relationships. However, these anomalous findings indicate the need to further investigate whether factors such as level of education may also be salient as well as whether the previously noted effects of age and gender have truly waned.

Finally, our research strongly suggests the need to conduct further research relating both context and a priori individual and personality-based factors to security-related behavioural intentions. As noted earlier, in many cases phishing emails make fear appeals, relying on constructs indicated in PMT, to result in users performing what they perceive to be effective self-protective behaviours, which, in fact, contribute to the success of the phishing attack. Recent research has begun to show that existing user dispositions affect the way that fear appeals translate into behavioural intentions (Posey *et al*, 2015). Our research further suggests that aspects related to phishing messaging (e.g. the identity of the sender, the type of link) in some cases result in the salience of personality-related and dispositional factors. We feel that further investigation into such phenomena is therefore called for. Other personality-related frameworks such as the five-factor model (e.g. Saville & Holdsworth, 1984) or dark triad personality traits (Paulhus & Williams, 2002) could enable researchers to understand more about how underlying personality traits affect user's security-related behaviours.

Conclusion

Individuals and organizations are reliant on the Internet (Anandarajan, 2002; Cheung *et al*, 2000; Lim & Teo, 2005) despite the everyday risks of phishing attacks and other malicious actions. This paper explores several constructs from IS, psychology, and communications research to better understand who is more susceptible to phishing schemes and why this is the case. Our experimental results indicate that a few personality and other individual factors are important predictors of phishing susceptibility. These findings provide important insights for future research and practice focused on reducing the threat posed by phishing.

About the Authors

Gregory D. Moody received his Ph.D. from the University of Pittsburgh and the University of Oulu. He has published in *ISR*, *MISQ*, *JMIS*, *JAIS*, *ISJ*, *I&M*, *JASIST*, and other journals. His interests include IS security and privacy, e-business (electronic markets, trust), and human–computer interaction (website browsing, entertainment).

Dennis F. Galletta is an AIS Fellow, was previously President of AIS, and is a recent LEO award winner. He also serves as Director of Doctoral Programs at Katz. He obtained his Ph.D. in MIS from the University of Minnesota, and his research interests cover end-user behaviour, attitudes, and performance, as well as behavioural security.

Brian Kimball Dunn received his Ph.D. in Information Systems from the Katz Graduate School of Business at the University of Pittsburgh. Prior to entering academia, he spent 10 years in corporate practice managing e-commerce and online marketing functions for large multi-national corporations.

References

Abbasi A, Zhang Z, Zimbra D, Chen H and Nunamaker JF (2010) Detecting fake websites: the contribution of statistical learning theory. *MIS Quarterly* **34**(3), 435–461.

Adler L, Kessler RC and Spencer T (2006) *The Value of Screening for Adults with ADHD*. Adult ADHD Self-Report Scale (ASES-v1.1) Symptom Checklist.

Agarwal R and Karahanna E (2000) Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. *MIS Quarterly* **24**(4), 665–694.

Aiken LS and West SG (1991) *Multiple Regression: Testing and Interpreting Interactions*. Sage Publishing, London.

Alba JW and Hutchinson JW (2000) Knowledge calibration: what consumers know and what they think they know. *Journal of Consumer Research* **27**(1), 123–156.

Alseadoon I, Chan T, Foo E and Gonzales Nieto J (2012, January) Who is more susceptible to phishing emails?: a Saudi Arabian study. In *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012*, pp 1–11, ACIS.

Alsharnouby M, Alaca F and Chiasson S (2015) Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies* **82**, 69–82.

Anandarajan M (2002) Profiling web usage in the workplace: a behavior-based artificial intelligence approach. *Journal of Management Information Systems* **19**(1), 243–266.

Anderson CL and Agarwal R (2010) Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly* **34**(3), 613–643.

Anderson BB, Vance A, Kirwan CB, Jenkins JL and Eargle D (2016) From warning to wallpaper: why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems* **33**(3), 713–743.

Banker RD and Kauffman RJ (2004) The evolution of research on information systems: a fiftieth-year survey of the literature in management science. *Management Science* **50**(3), 281–298.

Berlyne DE (1960) *Conflict, Arousal, and Curiosity*. McGraw-Hill, New York, NY.

Blythe M, Petrie H and Clark JA (2011, May) F for fake: four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 3469–3478, ACM.

Boss SR, Galletta DF, Lowry PB, Moody GD and Polak P (2015) What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* **39**(4), 837–864.

Brancheau JC, Janz BD and Wetherbe JC (1996) Key issues in information systems management: 1994–1995 SIM Delphi results. *MIS Quarterly* **20**(2), 225–242.

Brock TC and Livingston SD (2004) The need for entertainment scale. In *The Psychology of Entertainment Media: Blurring the Lines Between Entertainment and Persuasion* (Shrum LJ, Ed), pp 255–274, Lawrence Elbaum Associates, Mahwah, New Jersey.

Burgoon JK and Burgoon M (2001) Expectancy theories. In *Handbook of Language and Social Psychology* (Robinson WP and Giles H, Eds), pp 79–101, Wiley, Sussex, UK.

Carter L and Belanger F (2005) The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal* **15**(1), 5–25.

Chan M, Woon IMY and Kankanhalli A (2005) Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security* **1**(3), 18–41.

Chen R, Wang J, Herath T and Rao HR (2011) An investigation of email processing from a risky decision making perspective. *Decision Support Systems* **52**(1), 73–81.

Cheung W, Chang MK and Lai VS (2000) Prediction of Internet and World Wide Web usage at work: a test of an extended Triandis model. *Decision Support Systems* **30**(1), 83–100.

Costa PT and Mcrae RR (1992) *The NEO PI-R Professional Manual*. Psychological Assessment Resources, Odessa, Florida.

Cowan BR, Vigentini L and Jack MA (2008) Exploring the relationship between anxiety and usability evaluation: an online study of Internet and wiki anxiety. In *Proceedings of IADIS*.

D'Arcy J and Hovav A (2007) Deterring internal information systems misuse. *Communications of the ACM* **50**(10), 113–117.

D'Arcy J, Hovav A and Galletta DF (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research* **23**(1), 79–98.

Dellarocas C (2005) Reputation mechanisms. In *Handbooks in Information Systems* (Whinston AB, Ed), pp 629–660, Elsevier, Oxford, UK.

Dhamija R, Tygar JD and Hearst MA (2006) Why phishing works. In *Proceedings of CHI*, pp 581–590.

Dimoka A (2010) What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly* **34**(2), 373–396.

Egelman S, Cranor LF and Hong J (2008) You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065–1074.

Everard A and Galletta DF (2006) How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems* **22**(3), 55–95.

Farmer R and Sundberg ND (1986) Boredom proneness – the development and correlates of a new scale. *Journal of Personality Assessment* **50**(1), 4–17.

Fette I, Sadeh N and Tomasic A (2007) Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web*, pp 649–656.

Galletta DF and Polak P (2003) An empirical investigation of antecedents of internet abuse in the workplace. In *SIG Workshop on HCI*, pp 47–51.

Gartner (2007) Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks. http://www.gartner.com/newsroom/id/565125. Accessed 3 June 2017.

Gartner (2009) Gartner says number of phishing attacks on U.S. consumers increased 40 percent in 2008. http://www.gartner.com/newsroom/id/936913. Accessed 3 June 2017.

Gefen D, Karahanna E and Straub DW (2003) Inexperience and experience with online stores: the importance of TAM and trust. *IEEE Transactions on Engineering Management* **50**(3), 307–321.

Gefen D and Straub DW (2004) Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-products and e-services. *Omega* **32**(6), 407–424.

Goh KY and Ping JW (2014) Engaging consumers with advergames: An experimental evaluation of the interactivity, fit and expectancy. *Journal of the Association for Information Systems* **15**(7), 388–421.

Grazioli S (2004) 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), 149–172.

Grazioli S and Jarvenpaa SL (2000) Perils of internet fraud: an empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* **30**(4), 395–410.

Hackbarth G, Grover V and Mun YY (2003) Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use. *Information & Management* **40**(3), 221–232.

Hair JF, Ringle CM and Sarstedt M (2011) PLS-SEM: indeed a silver bullet. *Journal of Marketing Theory and Practice* **19**(2), 139–152.

Hart P and Saunders C (1997) Power and trust: critical factors in the adoption and use of electronic data interchange. *Organization Science* **8**(1), 23–42.

Herath T and Rao HR (2009a) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems* **47**(2), 154–165.

Herath T and Rao HR (2009b) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* **18**(1), 106–125.

Hoffman DL, Novak TP and Peralta M (1999) Building consumer trust online. *Communications of the ACM* **42**(4), 80–85.

Holden SJS and Vanheule M (1999) Know the name, forget the exposure: brand familiarity versus memory of exposure context. *Psychology and Marketing* **16**(6), 479–496.

Hwang Y and Kim DJ (2007) Customer self-service systems: the effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust. *Decision Support Systems* **43**(3), 746–760.

Jagatic TN, Johnson NA, Jakobsson M and Menczer F (2007) Social phishing. *Communications of the ACM* **50**(10), 94–100.

Johnston AC and Warkentin M (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* **34**(3), 549–566.

Johnston AC, Warkentin M and Siponen MT (2015) An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* **39**(1), 113–134.

Joiner R, Brosnan M, Duffield J, Gavin J and Maras P (2007) The relationship between internet identification, internet anxiety and internet use. *Computers in Human Behavior* **23**(3), 1408–1420.

Joiner R *et al* (2005) Gender, internet identification, and internet anxiety: correlates of internet use. *CyberPsychology and Behavior* **8**(4), 371–378.

Kankanhalli A, Teo HH, Tan BCY and Wei KK (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management* **23**(2), 139–154.

Kumaraguru P *et al* (2009a) School of phish: a real-world evaluation of anti-phishing training. In *Symposium on Usable Privacy and Security*.

Kumaraguru P, Sheng S, Acquisti A, Cranor L and Hong J (2009b) Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology* **10**(2), 1–31.

Leung ACM and Bose I (2008) Indirect financial loss of phishing to global market. In *Proceedings of ICIS*.

Liang H and Xue Y (2009) Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly* **33**(1), 71–90.

Liang H and Xue Y (2010) Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems* **11**(7), 394–413.

Lim VKG and Teo TSH (2005) Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: an exploratory study. *Information and Management* **42**(8), 1081–1093.

Litman JA and Spielberger CD (2003) Measuring epistemic curiosity and its diversive and specific components. *Journal of Personality Assessment* **80**(1), 75–86.

Lowry PB, Vance A, Moody G, Beckman B and Read A (2008) Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. *Journal of Management Information Systems* **24**(4), 199–224.

Lowry PB and Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal* **25**(5), 433–463.

Lowry PB, D'Arcy J, Hammer B and Moody GD (2016) "Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems* **25**(3), 232–240.

Lowry PB, Gaskin J, Twyman NW, Hammer B and Roberts TL (2013) Proposing the hedonic-motivation system adoption model (HMSAM) to increase understanding of adoption of hedonically motivated systems. *Journal of the Association for Information Systems* **14**(11), 617–671.

Malhotra NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research* **15**(4), 336–355.

Mathews L (2017) This gmail phishing attack is fooling even savvy users. Forbes.com, Jan 16. Available at: https://www.forbes.com/sites/leemathews/2017/01/16/gmail-phishing-attack-targets-yourcontacts/#644236eb5435.

Mcelroy JC, Hendrickson AR, Townsend AM and Demarie SM (2007) Dispositional factors in Internet use: personality versus cognitive style. *MIS Quarterly* **31**(4), 809–820.

McKnight DH, Choudury V and Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research* **13**(3), 334–359.

McKnight DH, Cummings LL and Chervany NL (1998) Initial trust formation in new organizational relationships. *Academy of Management Review* **23**(3), 473–490.

Mitnick K and Simon WL (2002) *The Art of Deception: Controlling the Human Element of Security*. Wiley, New York, New York.

Moody GD and Siponen M (2013) Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management* **50**(6), 322–335.

Moody GD, Galletta DF and Lowry PB (2014). When trust and distrust collide online: the engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications* **13**(4), 266–282.

Moody GD, Lowry PB and Galletta DF (2016) It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. *European Journal of Information Systems* 1–35.

Moody GD, Lowry PB and Galletta DF (2017) It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. *European Journal of Information Systems*. doi:10.1057/s41303-016-0027-9.

Nicholson N, Soane E, Fenton-O'Creevy M and Willman P (2005) Personality and domain-specific risk taking. *Journal of Risk Research* **8**(2), 157–176.

Nunnally JC and Bernstein IH (1994) *Psychometric Theory*. McGraw-Hill Humanities/Social Sciences/Languages, New York, New York.

Paulhus DL and Williams KM (2002) The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality* **36**(6), 556–563.

Pavlou PA and Dimoka A (2006) The nature and role of feedback text comments in online marketplaces: implications for trust building, price premiums, and seller differentiation. *Information Systems Research* **17**(4), 392–414.

Petty RE, Cacioppo JT and Schumann D (1983) Central and peripheral routes to advertising effectiveness: the moderating role of involvement. *Journal of Consumer Research* **10**(9), 135–146.

Petty RE and Wegener DT (1998) Attitude change: multiple roles for persuasion variables. In *The Handbook of Social Psychology* (Vol. 1) (Gilbert DT, Fiske E and Lindzey G, Eds.), pp 323–390, McGraw-Hill, New York, New York.

Posey C, Lowry PB, Roberts TL and Ellis S (2009) The culture-influenced online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems* **27**(4), 163–200.

Posey C, Roberts TL and Lowry PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* **32**(4), 179–214.

Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology* **91**(1), 93–114.

Romanosky S (2016) Examining the costs and causes of cyber incidents. FTC PrivacyCon, Washington DC, 14 January 2016.

Rossi PH and Anderson AB (1982) The factorial survey approach: an introduction. In *Measuring Social Judgments* (Rossi H and Nock SL, Eds), pp 15–67, Sage Publications, Beverly Hills, California.

Saville P and Holdsworth J (1984) *Occupational Personality Questionnaire Manual*, Escher, Surrey, England.

Schul Y, Mayo R, and Burnstein E (2004). Encoding under trust and distrust: the spontaneous activation of incongruent cognitions. *Journal of Personality and Social Psychology* **86**(5), 668.

Schul Y, Mayo R and Burnstein E (2008) The value of distrust. *Journal of Experimental Social Psychology* **44**(5), 1293–1302.

Sheng S, Holbrook M, Kumaraguru P, Cranor L and Downs J (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of CHI, pp 373–382.

Siponen M (2000) Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management and Computer Security* **8**(5), 197–209.

Siponen M, Pahnila S and Mahmood A (2006) A new model for understanding users' is security compliance. In *Proceedings of PACIS*, pp 644–657.

Siponen M and Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34**(1), 487–502.

Steelman Z, Hammer BI and Limayem M (2014) Data collection in the digital age: innovative alternatives to student samples. *MIS Quarterly* **38**(2), 355–378.

Sternthal B, Dholakia R and Leavitt C (1978) The persuasive effect of source credibility: tests of cognitive response. *Journal of Consumer Research* **4**(4), 252–260.

Straub DW (1990) Effective IS security. *Information Systems Research* **1**(3), 255–276.

Straub DW and Goodhue DL (1991) Security concerns of systems users: a study of perceptions of the adequacy of security. *Information and Management* **20**(1), 13–27.

Sun L, Srivastava RP and Mock TJ (2006) An information systems security risk assessment model under Dempster-Shafer theory of belief functions. *Journal of Management Information Systems* **22**(4), 109–142.

Theoharidou M, Kokolakis S, Karyda M and Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security* **24**(6), 472–484.

Tuten TL and Bosnjak M (2001) Understanding differences in web usage: the role of need for cognition and the five factor model of personality. *Social Behavior and Personality* **29**(4), 391–398.

van der Heijden H (2004) User acceptance of hedonic information systems. *MIS Quarterly* **28**(4), 695–704.

van der Heijden H, Verhagen T and Creemers M (2003) Understanding online purchase intentions: contributions from technology and trust perspectives. *European Journal of Information Systems* **12**(1), 41–48.

Vance A, Elie-Dit-Cosaque C and Straub DW (2008) Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of Management Information Systems* **24**(4), 73–100.

Vishwanath A, Herath T, Chen R, Wang J and Rao HR (2011) Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* **51**(3), 576–586.

Wang J, Chen R, Herath T and Rao HR (2009) Visual e-mail authentication and identification services: an investigation of the effects on e-mail use. *Decision Support Systems* **48**(1), 92–102.

Wang W and Benbasat I (2008) Attributions of trust in decision support technologies: a study of recommendation agents for e-commerce. *Journal of Management Information Systems* **24**(4), 249–273.

Wasko MM and Faraj S (2005) Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly* **29**(1), 35–37.

Webster J, Trevino LK and Ryan L (1993) The dimensionality and correlates of flow in human-computer interaction. *Computers in Human Behavior* **9**(4), 411–426.

Weinberg SL and Abramowitz SK (2008) *Statistics Using SPSS: An Integrative Approach.* Cambridge University Press, Cambridge, Massachusetts.

Woon IMY, Tan GW and Low R (2005) A protection motivation theory approach to home wireless security. In *Proceedings of ICIS*, pp 367–380.

Workman M (2008) 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), 1–12.

Wright RT, Chakraborty S, Basoglu A and Marett K (2010) Where did they go right? Understanding the deception in phishing communications. *Group Decisions and Negotiation* **19**(4), 391–416.

Wright RT, Jensen ML, Thatcher JB, Dinger M and Marett K (2014) Influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information Systems Research* **25**(2), 385–400.

Wright RT and Marett K (2010) The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *Journal of Management Information Systems* **27**(1), 273–303.

Appendix

See Table 13.

Table 13 Summary of related literature in chronological order

References	*Journal*	*Title*	*Objective*	*Findings*
Dhamija *et al* (2006)	CHI Proceedings	Why phishing works	Examine user ability to identify authentic websites from fraudulent ones	Subjects performed at a 40% error rate; no statistically significant factor or method was found for identifying fraudulent websites
Jagatic *et al* (2007)	Communications of the ACM	Social phishing	Determine whether identity and gender of email sender alters phishing susceptibility; used ethical phishing	Found that both the identity and gender of the sender matter; significant effect for females over males in terms of phishing susceptibility
Fette *et al* (2007)	WWW Conference Proceedings	Learning to detect phishing emails	Using design science to better detect phishing email (and websites)	Identified a set of criteria that could be used to successfully identify phishing emails
Workman (2008)	Journal of the American Society for Information Systems	Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security	Do elements that result in successful marketing campaigns also result in successful phishing attacks?	Found that normative commitment, continuance commitment, affective commitment, trust, and obedience all significantly predict both subjective and objective security behaviours
Egelman *et al* (2008)	CMU Institute for Software Research	You've been warned: an empirical study of web browser phishing warnings	Investigated whether active (vs. passive) warnings were effective	Active warnings are more effective at warning users off phishing websites than passive warnings
Leung and Bose (2008)	ICIS Proceedings	Indirect financial loss of phishing to global market	Determine whether announced phishing attacks by a company had a financial impact on firm value	All firms, regardless of size, showed a significant statistical drop in firm value when phishing attacks were announced
Kumaraguru *et al* (2009a, b)	Symposium on Usable Privacy and Security	School of phish: a real-world evaluation of anti-phishing training	Determine whether individuals can be trained to detect phishing attacks through a developed tool, PhishGuru	PhishGuru, and its underlying methodology, were shown to be effective in educating about phishing attacks
Kumaraguru *et al* (2009a, b)	ACM Transactions on Internet Technology	Teaching Johnny not to fall for phish	Re-test of PhishGuru	18–25-year-olds were most susceptible to phishing; PhishGuru was found to still be effective 28 days after training

Table 13 ***(Continued)***

References	*Journal*	*Title*	*Objective*	*Findings*
Sheng *et al* (2010)	CHI Proceedings	Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions	Examine whether gender, age, and educational level impact phishing susceptibility	18–25-year-olds were most susceptible to phishing, and women were more susceptible than men; training reduced phishing susceptibility by up to 40%
Wright *et al* (2010)	Group Decision and Negotiation	Where did they go right? Understanding the deception in phishing communications	Test Grazioli's Theory of Deception within the context of phishing emails; test experiential and dispositional factors in deception detection	Disposition to trust and web experience were both significant predictors of susceptibility. Developed process model of deception detection
Wright and Marett (2010)	Journal of MIS	The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived	Understand behavioural factors that increase susceptibility to successful phishing attacks	Experiential factors (computer self-efficacy, web experience, security knowledge) significantly predicted deception success. Of dispositional factors, only suspicion was significant (trust and risk were not)
Abbasi *et al* (2010)	MIS Quarterly	Detecting fake websites: the contribution of statistical learning theory	Use statistical learning theory to better enable automated detection of fake websites	Using design science techniques, a useful prototype was developed
Anderson and Agarwal (2010)	MIS Quarterly	Practicing safe computing: a multimedia empirical investigation of home computer user security behavioural intentions	What are antecedents of intent to perform secure behaviours among home computer users?	Security-related behaviour is predicted by a combination of cognitive, social, and psychological factors
Vishwanath *et al* (2011)	Decision Support Systems	Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model	Test phishing vulnerability using an information processing-focused model	Email load and perceived relevance increased vulnerability, but attention to detail decreased it. Limited support for significance of information processing
Blythe *et al* (2011)	CHI Proceedings	F for fake: four studies on how we fall for phish	Understand why people fall for phishing attacks	Brand logos increase likelihood of phishing success, and security-based language may also be persuasive
Alseadoon *et al* (2012)	ACIS Proceedings	Who is more susceptible to phishing emails? A Saudi Arabian study	Testing whether certain conditions result in user susceptibility to phishing emails	High openness, submissiveness, email experience, and "susceptibility" (lack of doubt specific to the email) predicted susceptibility
Wright *et al* (2014)	Information Systems Research	Influence techniques in phishing attacks: an examination of vulnerability and resistance	Testing various influence techniques for effectiveness within the email phishing context	Several influence techniques were significant predictors: liking, reciprocity, social proof, consistency, authority, and scarcity. Implying fictitious experiences decreased phishing effectiveness
Alsharnouby *et al* (2015)	International Journal of HCI	Why phishing still works: user strategies for combating phishing attacks	Investigate the extent to which browser security measures and greater awareness affect phishing susceptibility.	Users still fall for phishing and don't spend much time gazing at security measures, although those that do are less susceptible
Anderson *et al* (2016)	European Journal of Information Systems	How users perceive and respond to security messages: a NeuroIS research agenda and empirical study	Understand user behaviour towards security messages (e.g. warning against phishing) via NeuroIS techniques	Based on eye tracking, eye movement memory results in users becoming habituated to security messages. This effect can be diminished through altering the appearance of the message