Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing

Completed Research Paper

Introduction

Individuals and organizations are continuing to increase their reliance on networks and the Internet (Anandarajan 2002; Cheung et al. 2000; Lim and Teo 2005). While this connectivity offers numerous benefits (e.g., Banker and Kauffman, 2004), it also introduces a number of threats to networked users' financial and information security (Dellarocas 2005; Liang and 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 a Gartner Group study, e-mail phishing attacks cost individuals and businesses $3.2 billion in the United States alone in 2007; the same study found that 3.3 percent of all individuals who received a phishing email lost money as a result (Gartner 2007). (Leung and Bose 2008) showed that firms bear a significant portion of this cost, an idea corroborated by a 2009 industry study that found that 56 percent of phishing losses were absorbed by firms (Gartner 2009). Given that phishing is a relatively new phenomenon, it seems likely to remain an issue and potentially grow in magnitude unless measures are taken to ameliorate the threat (Sheng et al. 2010).

A significant body of research has focused on training individuals to avoid phishing schemes (e.g., (Dhamija et al. 2006; Jagatic et al. 2007; Kumaraguru et al. 2009a; 2009b; Technologies 2009), however relatively little research has focused on identifying those individuals who may be more susceptible to such scams or the situational factors that increase susceptibility. This paper seeks to fill that gap by exploring personality and situational constructs that may increase the likelihood of an individual falling prey to a phishing attack.

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

The results of our study provide several important contributions to IS research. Specifically, we demonstrate that several situational factors do, in fact, alter the effectiveness of phishing attempts. Further, we find that certain personality traits can impact an individual's susceptibility to such attacks. This paper discusses these findings in more detail and suggests potential avenues for further research in this area.

Literature Review

The threats posed by malicious online attacks have been researched in a number of studies covering several contexts (e.g., (Chan et al. 2005; D'Arcy and Hovav 2007; D'Arcy et al. 2009; Galletta and Polak 2003; Grazioli and Jarvenpaa 2000; Herath and Rao 2009a; 2009b; Johnston and Warkentin 2010; Kankanhalli et al. 2003; Liang and Xue 2009; Liang and Xue 2010; Siponen 2000; Siponen et al. 2006; Siponen and Vance 2010; Straub 1990; Straub and Goodhue 1991; Sun et al. 2006; Theoharidou et al. 2005). However, relatively few papers have focused on phishing specifically. In the paper most similar to our research, Sheng et al. (2010) focused on demographic characteristics (gender, age, education level) as predictors of phishing susceptibility. They found that women were more susceptible to phishing than men and that the 18- to 25-year-olds formed the most susceptible age group. Further, they found that training individuals regarding common phishing practices enabled potential victims to reduce their likelihood of being phished. The efficacy of training materials and tools in affecting phishing susceptibility has also

been found in other studies (Kumaraguru et al. 2009a; 2009b) and has been the primary focus of most other phishing-related studies.

In a related study study, (Jagatic et al. 2007) used an *ethical phishing* technique, in which a simulated, non-harmful phishing email is 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, then sent notifications using these known friends' identities to inform subjects that the university required subjects to click on a link in order to maintain certain services. Jagatic et al. found that, in addition to the majority of subjects being willing to provide login credentials through a "fraudulent" Web site; subjects were more likely to respond when the email appeared to have been sent from a known friend and were also more likely to respond to a message from the opposite gender. They also found that women in their study were more likely to click on provided links than men. This and the other existing phishing studies are summarized in Table 1.

Table 1. Summary of Phishing Studies in Information Systems

Study	Objective	Findings
Dhamija et al. (2006)	Examine user ability to identify authentic Web sites from fraudulent ones.	Subjects performed at a 40% error rate; no statistically significant factor or method was found for identifying fraudulent Web sites.
Jagatic et al. (2007)	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.
Leung and Bose (2008)	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)	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. (2009b)	Re-test of PhishGuru.	18-25-year-olds were most susceptible to phishing; PhishGuru was found to still be effective 28 days after training.
Sheng et al. (2010)	Examine whether gender, age and educational levels 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%.

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 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. When relevant, cited articles for constructs of interests were also reviewed to identify potentially useful constructs. This yielded a set of thirteen candidates, which merited further consideration.

We then proceeded to conduct a Delphi study[1]. The Delphi technique enables subjects to identify and produce a rank-ordered list of answers to given questions posed to the group. For this study, 75 full-time

[1] In conducting this study we followed the same methodological approach set forth in (Brancheau et al. 1996).

graduate students taking an "Electronic Commerce Strategies" course from a major university in the eastern US were recruited.

In the first round of information solicitation, subjects were asked to identify reasons people (themselves or others) might either (1) click and (2) not click on links in emails that were 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) 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[2], ultimately resulting in a list of sixteen rank-ordered candidate reasons[3].

The resulting lists from both the literature review and the Delphi study were then compared. We found twelve constructs[4] that were common between the previously identified constructs from the literature and the sixteen reasons for phishing described through the Delphi methodology, which we use as the basis for our exploratory study. As a result of this process, while not exhaustive, the set of constructs considered in this exploratory paper constitute an independently supported and reasonable starting point for research into phishing susceptibility antecedents.

Hypothesis Development

The twelve constructs identified can be broken 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 e-mail 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. However, we opted to control for message content as any argument or content in a message could be interpreted through a variety of ways in this study, that it would undermine the control of the study. To avoid any potentially confounding effects, we used 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). Accordingly, we propose that the sender of a message is an important predictor of phishing susceptibility due to the perceived credibility of a known source. 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 and Vanhuele 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 and Burgoon 2001; Petty and Wegener 1998).

We propose that known sources are able to use their familiar status and thereby influence others. This serves as the basis for an individual trusting the content of a message apparently sent from a known party and thereby suspending adequate evaluation of a fraudulent phishing attack. While this finding has

[2] In the final (third) round of the study, no additional constructs were suggested, indicating that the list had reached its stable state within the group of subjects.

[3] Although more reasons for phishing were identified through the Delphi method, several reasons (Specifically ones dealing with trust) only dealt with one construct.

[4] The Delphi study failed to show a reason for phishing that included one's stake or involvement with the phishing subject.

already been reported in a related study (Jagatic et al. 2007), we seek to examine this construct along with the set of other variables we introduce in this study. Such an examination would enable an evaluation of relative strength of various antecedents.

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

Link Type

The other message-specific variable we consider in our study is link type. By *link type*, we refer to the form of the uniform resource locator (URL) that appears in the email message. Here there are two options: numeric, in which an IP address is given (e.g., 103.45.3.79), and textual, in which the user sees the Web site's domain name (e.g., www.google.com).

Given that the textual form is the one most commonly seen by users, we speculate that a numeric address will raise a "red flag" that may alert users of a phishing email's impropriety. Further, the textual URL conveys more information regarding the page to which the link points, which, we propose, engenders trust. Of course, the apparent URL need not be the one to which a link leads, such that in the case of a phishing email, such trust 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 to consider: trust, distrust, curiosity, entertainment drive, boredom proneness, lack of focus, and risk propensity.

Trust and Distrust

Given the prominent role that influence plays in the success of phishing attacks, trust and distrust are crucial constructs to be considered. *Trust* constitutes the willingness to be vulnerable to another and rely upon him or her to perform an expected behavior (Mayer et al. 1995; McKnight et al. 2002; McKnight et al. 1998). *Distrust*, on the other hand, has been defined as the *un*willingness to become vulnerable to another given the expectation that he or she means to harm the truster (McKnight and Choudhury, 2006; McKnight et al. 2004). If the recipient of a phishing attack trusts the received email, he or she will rely on it, thus leading to vulnerability to it, thus increasing his or her likelihood of falling prey to it (Hovland and Weiss, 1951-1952; Petty et al. 1983; Petty and Wegener 1998; Shah and Jehn 1993; Sternthal et al. 1978).

Trust research has proposed and found that individuals have static dispositions to both trust and distrust others in general (McKnight and Choudhury 2006; McKnight et al. 1998; 2002; 2004). Given the lack of context and actual interaction with potentially unknown attackers, a person's innate general trusting and distrusting dispositions toward others in general are expected to have an effect on how the individual interacts.

Recent research into trust and distrust and their reflection in brain activity has identified trust and distrust as discrete constructs (Dimoka 2010). Along those same lines, other research has found evidence that it is possible for individuals to feel trust and distrust simultaneously (Komiak and Benbasat 2008). While knowledge in this area is still developing, given the exploratory nature of this paper we felt it important to allow for this idea of trust and distrust as related, but separate, concepts. As such, trust and distrust are measured and analyzed as separate candidate antecedents.

> *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 be exposed to novel experiences that motivate exploratory behaviors (Berlyne 1949; 1950; 1954; 1957; 1958). This drive is considered extensively within the Big Five factors psychological literature, which includes culture (Tupes & Christal, 1961), intellect (Digman, 1990), or openness (McRae & John, 1992); as used in this study, curiosity coincides particularly well with action (the inclination to try new activities) and ideas (the inclination to be intellectually curious) facets of the openness construct (Costa & McRae, 1992).

Links in email messages, especially unsolicited email messages, may appear to be an invitation to a new Web site that could offer new opportunities or experiences. Therefore, and given that more curious individuals have a heightened drive to seek novel experiences (Litman and Spielberger 2003; Lowenstein 1994; Speilberger and Starr 1994), individuals with higher levels of curiosity may be more likely to desire to click on unknown links in hopes of satisfying this drive.

> *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

Psychological research has defined *entertainment drive*, or the need for entertainment, as the desire for novel sources of recreation or pleasure (Brock and Livingston 2004), which coincides nicely with the action factor from the Big Five (Costa & McRae, 1992). This motivation has been closely linked to curiosity in the literature (Litman and Spielberger 2003). Similar to curiosity, individuals with high entertainment drives more frequently seek novel experiences that can provide amusement or recreation. As was hypothesized with curiosity, this entertainment-seeking behavior may result in subjects' desire to click on unknown links in hopes of attaining a new source of pleasure.

> *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.*

Boredom Proneness

Boredom proneness refers to an individual's disposition to feel that a current situation is uninteresting (Farmer and Sundberg 1986). As such, it acts as a counterpoint to entertainment drive; the latter seeks novel interactions and the former becomes uninterested in such interactions. Thus, building on the logic for entertainment drive, those with high levels of boredom proneness will tend to disengage from what they are currently experiencing. When presented by a new opportunity in the form of an unknown link, the individual will not be inherently interested in exploring it.

> *H7: Individuals with higher levels of boredom proneness will be less 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 high inabilities 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). As such, when an unknown link is presented to such a person, this lack of focus or lack of self-discipline results 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 lower abilities to focus on current tasks, such as reading one's email, will be more likely to click on links that would allow them to escape the current task.

> *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 their lives and to engage in potentially risky behaviors (Nicholson et al. 2005). Research has shown that risk propensity is effectively opposed to trust (Mayer et al. 1995; McKnight et al. 1998; 2002). Given the inclusion of trust in this study, it makes sense to also include risk propensity. In operationalizing this construct, we have elected to also look at various types of risk, including measures of propensity for taking risk in regards 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 behaviors 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

Besides 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. The 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 that an individual spends online across a wide array of available activities (Joiner et al. 2007; McKnight et al. 2002). Past research suggests that those who are more experienced in online activities are more likely to avoid shopping online due to perceived security concerns (Hoffman et al. 1999). Our expectation, then, is that a similar phenomenon will reveal itself within the email context and that an individual with greater online experience will have an increased understanding of 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 experiences or browsing that uncovered warnings or discussions about these schemes. We thus expect that one's experience on the Internet leads them to adopt some level 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

In this study, *Internet community identification* expresses the level of attachment between the individual and the Internet (Joiner et al. 2007). An individual with a higher level of Internet community attachment considers himself to be a 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, it's expected that an individual with higher Internet community identification would be more likely to click on an unknown link, since he may perceive that doing so may assist in deepening his online social interactions.

> *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

The construct of *Internet anxiety* reflects the user's general feeling of unease or apprehension toward the online environment. Unlike the previous two constructs, Internet anxiety creates a strong desire to avoid using the Internet or to mitigate one's exposure to it (Joiner et al. 2007). It has been found that such anxiety toward IT results in a significant decrease in a user's willingness to trust a system (Hwang & Kim, 2007) as well as users' perception of a system's usability (Hackbarth et al., 2003; Cowan et al., 2008).

Similarly, then, we expect that higher levels of such anxiety will result in a lower probability of a user clicking on an unknown link, due to the decreased level of trust felt towards the Internet and a perception that the Internet is difficult to use. 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.*

Summary of Hypotheses

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

Table 2. Summary of Hypotheses

#	Construct	Expectation
1	Known source of email	Higher susceptibility
2	Text-based link	Higher susceptibility
3	Disposition to trust	Higher susceptibility
4	Disposition to distrust	Lower susceptibility
5	Curiosity	Higher susceptibility
6	Entertainment drive	Higher susceptibility
7	Boredom proneness	Lower susceptibility
8	Lack of focus	Higher susceptibility
9	Risk propensity	Higher susceptibility
10	General Internet usage	Lower susceptibility
11	Internet community identification	Higher susceptibility
12	Internet anxiety	Lower susceptibility

Methodology

To more strongly infer causality between constructs and individuals' susceptibility to phishing scams, an experiment was conducted. For this experiment, 632 undergraduate psychology and information systems students were recruited from a large public university in the eastern US. Subjects were offered extra credit in their courses in return for their participation. Of these subjects, 53 percent were male and 44 percent were female (the other 3 percent declined to state gender). Mean age of subjects was 20.5 years (st. dev. 2.4 years) with 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 dataset sample size of 595.

Design and Procedures

The IRB-approved study consisted of a randomized 2 x 2 online experiment (known vs. unknown apparent email source *x* text link vs. numeric link). Subjects were directed to an online survey engine, then completed various instruments to collect the required stable personality traits used in the study as well as their email addresses. Subjects were then thanked for their participation then were led to believe that the experiment had ended (it had not).

Two weeks later, all subjects received a plain-text email that exhibited one of four treatments corresponding to the four cells of the 2x2 design (subjects were randomly assigned to each treatment). Emails appeared to have been sent by either a known source, an individual with whom subjects had interacted in signing up for the experiment, or an unknown source (a co-author of this study, from another school, who was unknown to the subjects). To avoid confounding effects that could be introduced by the message, we used a very simple email message. The subject line for all treatments was "Check this

out" in the same fashion as Jagatic et al. (2007). The body of the email message consisted of the same text "Check this out:", the remainder of the message then contained a link for the subject to click on. Subjects were presented with a link to an external Web site that was either shown as a 1) text-based URL or as 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. After several trials, we found how to set up the messages and what approach and software to use to mail them, to ensure delivery.

As with any other email, subjects receiving the experimental treatment email had the option to click on the link or not click on it. All links were encoded with a personalized id in order to identify subjects uniquely. Thus, when a subject 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 subject 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 coded as 1 and the apparent unknown source coded 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). Due to the exploratory nature of this research, each sub-construct (i.e., benevolence, competence, integrity, and trusting stance) was instantiated, but the general second-order construct of disposition to trust was not formed as we thought it useful to explore the effect of each sub-construct on susceptibility to phishing separately.

Disposition to distrust was, similar to the disposition to trust construct, measured using an instrument developed by McKnight et al. (2003). As with disposition to trust, the second-order construct was left out of the model in favor of the individual sub-constructs (i.e., malevolence, incompetence, deceit and distrusting stance).

Curiosity was measured along two aspects: diversive and specific. Previous instruments developed to measure epistemic curiosity have used this same approach and thus we follow established precedent (Litman and Spielberger 2003) by using both measures.

Entertainment drive was measured using a previously developed instrument (Brock and 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.

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

Lack of focus was measured using a previously validated instrument (Adler et al. 2006), available in both an extensive and short-version for determining the ability of an individual to focus. We opted to use the shorter version of the scale, rather than the very long instrument, given the need to measure so many other constructs.

Risk propensity was measured by 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: with the Internet community at large and 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, subjects' age, level of education, and gender 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[5]. Only highly loading items were used in construct calculation (i.e., >.70, representing that over 50% of the variance was captured for the indicator in the rotation).

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

Table 3. Construct Validity

Grouping	Construct	Subconstruct (# of items)	Cronbach's Alpha
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 (state) (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

[5] These results are available from the authors upon request

		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 identification (3)	n/a	.891

All constructs were formed based on the loadings from the rotated factor analysis (Aiken and West, 1991; Rossi and Anderson, 1982; Weinberg and Abramowitz, 2008)[6].

Analysis and Results

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

Table 4. Summary of Phishing Results by Treatment Conditions

	Known sender		Unknown sender		**Total**
Behavior	Text link	Numeric link	Text link	Numeric link	
Did not click	68 (11.4%)	68 (11.4%)	111 (18.7%)	102 (17.1%)	**349 (58.7%)**
Clicked	85 (14.3%)	51 (8.6%)	58 (9.7%)	52 (8.7%)	**246 (41.3%)**
Total	**153 (25.7%)**	**119 (20.0%)**	**169 (28.4%)**	**154 (25.8%)**	**595 (100%)**

Given the binary nature of the dependent variable, data were analyzed using multiple logistic regression models using STATA (v. 10.1). The first model reports the effects of the control variables on phishing susceptibility. The second model includes the treatment conditions in order to analyze the partial effect they have on the dependent variable. The last model includes all variables (See Table 5).

We then performed the same model analyses by treatment conditions in order to ascertain the effect that each variable had on phishing, while controlling for the type of treatment being experienced by the subject (See Table 6).

Table 5. Summary of Phishing Results for Partial and Full Models

	Baseline model		Treatment model		Full model	
Construct	Coef.	p	Coef.	p	Coef.	p
Age	0.065	0.146	0.066	0.154	0.075	0.122
Educ	**-0.203**	**0.000**	**-0.216**	**0.000**	**-0.203**	**0.000**
Gender	-0.213	0.218	-0.190	0.281	-0.181	0.391
Known source			**0.689**	**0.000**	**0.712**	**0.000**

[6] For example, the value for the sub-construct "competence" would be equal to c1 * .775 + c2 * .920 + c3 * .883.

Text link			0.312	0.074	**0.381**	**0.042**
Benevolence					0.057	0.643
Competence					-0.141	0.282
Integrity					0.120	0.362
Trusting stance					0.077	0.465
Malevolence					-0.085	0.433
Incompetence					0.013	0.912
Deceit					0.161	0.131
Distrusting stance					-0.138	0.236
Boredom proneness					1.023	0.068
Entertainment drive					0.051	0.588
Epistemic curiosity-diversive					0.056	0.787
Perpetual curiosity					0.005	0.983
Epistemic curiosity-state					0.028	0.867
Focus					-0.139	0.390
RP-recreational					0.100	0.376
RP-health					0.076	0.438
RP-career					0.050	0.751
RP-financial					**-0.365**	**0.011**
RP-safety					0.188	0.093
RP-social					0.051	0.652
Risk beliefs					**0.164**	**0.010**
General Internet usage					**0.423**	**0.002**
Internet anxiety					-0.120	0.455
Internet identification					**-0.131**	**0.010**
Constant	-0.452	0.592	-0.937	0.286	**-2.992**	**0.033**
LR Chi^2		22.790		42.490		93.150
Prob > Chi^2		0.000		0.000		0.000
Pseudo R^2		0.028		0.053		0.115

Table 6. Summary of Phishing Results by Treatment Conditions

	Unknown source		Known source		Numeric link		Text link	
Construct	Coef.	p	Coef.	p	Coef.	p	Coef.	p
Age	0.110	0.186	0.098	0.120	0.101	0.120	0.072	0.357
Educ	**-0.185**	**0.015**	**-0.264**	**0.001**	**-0.374**	**0.000**	-0.109	0.150
Gender	0.036	0.904	-0.405	0.247	-0.236	0.490	-0.207	0.477
Known source	na	na	na	na	0.527	0.085	**0.925**	**0.000**
Text link	0.098	0.707	**0.729**	**0.016**	na	na	na	na
Benevolence	0.246	0.145	-0.219	0.292	-0.043	0.830	0.154	0.363
Competence	0.000	1.000	-0.363	0.097	-0.174	0.425	-0.093	0.607
Integrity	-0.129	0.493	**0.536**	**0.016**	0.115	0.604	0.037	0.838
Trusting stance	0.106	0.466	-0.019	0.911	-0.214	0.222	0.175	0.243
Malevolence	0.067	0.661	-0.282	0.113	0.218	0.224	-0.275	0.077
Incompetence	-0.028	0.865	0.181	0.375	-0.134	0.476	0.120	0.492
Deceit	0.006	0.966	**0.408**	**0.026**	0.050	0.781	**0.311**	**0.038**

Distrusting stance	-0.212	0.175	-0.088	0.658	0.162	0.407	**-0.358**	**0.026**
Boredom proneness	0.662	0.412	1.435	0.114	1.203	0.239	1.026	0.154
Entertainment drive	0.167	0.229	-0.120	0.421	0.054	0.730	0.057	0.658
Epistemic curiosity-diversive	-0.076	0.790	0.233	0.491	0.391	0.293	-0.230	0.391
Perpetual curiosity	-0.165	0.583	0.109	0.773	0.127	0.742	-0.003	0.991
Epistemic curiosity-state	0.189	0.431	-0.112	0.676	0.021	0.936	0.046	0.848
Focus	0.205	0.364	**-0.654**	**0.018**	-0.137	0.618	-0.126	0.573
RP-recreational	0.016	0.918	0.228	0.219	0.300	0.111	0.048	0.758
RP-health	-0.024	0.869	0.167	0.266	0.228	0.141	-0.025	0.864
RP-career	0.031	0.883	0.090	0.736	0.194	0.470	0.052	0.815
RP-financial	-0.279	0.179	**-0.576**	**0.010**	**-0.627**	**0.017**	-0.372	0.055
RP-safety	0.121	0.453	0.288	0.105	0.240	0.192	0.117	0.449
RP-social	0.081	0.605	-0.024	0.895	0.100	0.609	0.094	0.536
Risk beliefs	0.072	0.426	**0.275**	**0.007**	0.177	0.086	0.153	0.083
General Internet usage	0.249	0.203	**0.857**	**0.001**	0.218	0.391	**0.551**	**0.003**
Internet anxiety	-0.016	0.934	-0.269	0.374	0.234	0.323	**-0.560**	**0.027**
Internet identification	**-0.203**	**0.005**	-0.086	0.304	**-0.289**	**0.000**	-0.034	0.633
Constant	-3.928	0.085	-2.104	0.291	-3.926	0.074	-1.705	0.409
n		323		272		273		322
LR Chi^2		33.660		78.390		73.870		53.380
Prob > Chi^2		0.000		0.000		0.000		0.003
Pseudo R^2		0.212		0.208		0.204		0.121

Discussion

Findings

The main objective of this study was to determine the message, personality traits, and Internet-related variables that are related to the likelihood that an individual would be susceptible for phishing by clicking on links in unsolicited e-mails. We found and measured several variables that can increase one's propensity for phishing. We analyzed these results at several levels of analysis (basic, treatment level and full model) and found several general predictors that we discuss here by theoretical framework.

Trust

Although no measure of trust or distrust was statistically significant as a main effect in predicting the susceptibility for phishing, further analysis revealed several interesting findings. First, as expected we find that trust will most likely have an effect on phishing susceptibility when the truster knows the trustee. Specifically, when the source of the e-mail is known by the truster to have integrity or a lack of deceitful intentions, than the truster will be more likely to click on e-mailed links. This result is more pronounced when the link is textually based, rather than a numeric link, which reverses this effect.

Second, we also find that it is likely for the truster to attribute distrusting attributes to unknown sources of e-mails, which reduces the likelihood of clicking on enclosed links. However, we note two exceptions. First, it is also possible that the truster attributes the unknown source of an unsolicited e-mail with benevolent intentions and will have an increased likelihood of clicking on a link when it is textual. Second, we also note an unexpected finding in that if the truster believes that the unknown sender of an e-mail is being deceitful, the truster has an increased likelihood of clicking on the link. Perhaps this increased likelihood of clicking on such links is to discover the intentions of this unknown sender, and how they attempt to trick the truster.

In summary, we find that trust tends to have an important effect on phishing susceptibility. It tends to increasing one's susceptibility when the sender of the e-mail is known, and to reduce this tendency when the sender is unknown and attributed to be deceitful.

Personality Traits

Surprisingly, we find few instances where personality traits showed an effect on phishing susceptibility, contrary to our predictions. We find that when individuals are unable to focus, they are less likely to click on e-mailed links from known sources. E-mail recipients with a tendency to not focus on given tasks may have increased tendencies to avoid e-mailed links given that they recognized the source and thereby have less incentive to attend to such a message. However, such a tendency to attend to messages from unknown sources was not found to be significant.

In summary, despite the expected effect of personality traits on phishing susceptibility, it produced no general effects, excluding two rather specific, yet powerful effects.

Internet Experience

The recipient's experience with the Internet was the most predictive grouping of variables tested in all of our models. We report two general, yet contradictory results. The more that the recipient used the Internet, the more likely he or she was to click on links in unsolicited e-mails. This likely occurred due to previous experience with such e-mails and the belief that the recipient will continue to avoid potential negative consequences in the future by continuing to engage in this risky behavior. However, a smaller negative effect on phishing susceptibility occurred when the individual strongly identified with the Internet: The more time that an individual spends on the Internet, the more likely that he or she will acquire expertise with threats or information about Internet threats and be better equipped to identify potential those threats and attacks.

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

Risk Tendencies

Our results revealed two consistent findings. First, individuals who are prone to engage in financial risks are less susceptible to phishing; this effect is present when the source of the e-mail is known, or contains a numeric link. Given that victims of phishing attempts often have their identities stolen, which could harm their finances, this finding is unsurprising. It is surprising to note that no further risk propensities produced a similar effect.

Special consideration must be given to the very unexpected finding that individuals who believe clicking on links in e-mails to be risky are also more prone to engage in such behaviors. This is found as a main effect, in regards to known sources only. We believe that such a finding can be explained by the psychological tendency to underestimate the possibility for negative consequences to occur for one's self and instead overestimate its effect for others, often called an optimistic or self-serving bias (Dhamija et al. 2006; Rhee et al. 2005).

In summary, we have both expected and unexpected findings with regard to risk tendencies. Rather than finding support for several risk propensities reducing one's phishing susceptibility, we find that only the financial risk tendency produces statistically significant results that reduce phishing susceptibility. However, we find that individuals are also falling prey to a self-serving bias in believing that they are more likely to identify phishing attempts and thereby may fall prey to actual phishing attempts, that they inappropriately believe to be legitimate communications.

Demographics and Manipulations

We further report that, contrary to previous studies (Jagatic et al. 2007; Kumaraguru et al. 2009a; Sheng et al. 2010), gender was not a statistically significant predictor of phishing in this study. Perhaps, given that this study regarded a variety of predictors and used e-mail as its phishing attempt, it systematically differs from these previous studies. Given the ubiquitous use of e-mail, perhaps it should be expected that both genders have been equally, and highly exposed to multiple phishing attempts and are thus equally prepared to identify and prevent phishing attempts. We also note a similar lack of results for age, which contradicts previous studies (Kumaraguru et al. 2009a; Sheng et al. 2010). Similar to gender, this lack of results may also be due to the ubiquitous nature of e-mail.

We did find that the level of education served as a strong deterrent of phishing. This effect was predictable and held for most models.

Most importantly, we find that our manipulations were very strong antecedents for phishing. 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. As expected, making the link more understandable and familiar to the recipient increased the likelihood of being phished.

Implications for Research

This study makes several contributions to the research on phishing. First, this is the first such large-scale study that focuses on several theoretical foundations to determine their effect on individuals' susceptibility towards phishing. By further explicating and testing these theories, we show which dimensions serve as accurate and reliable predictors of phishing susceptibility.

In particular, we show that the most important indicators regarding an individual's stable predictors of phishing susceptibility are determined by their previous experiences with the Internet. Namely, we find that frequent users of the Internet are also more susceptible to phishing. This effect is also offset by the individuals' anxiety towards the Internet or their identification with other users of the Internet. These findings highlight that individuals who use the Internet on a frequent basis will likely increase their susceptibility for hacking, beyond the number of attempts that they experience.

Further, the results are surprising in that they indicate the relatively ineffective power of personality traits and even trust in determining phishing susceptibility. Contrary to the strong theoretical bases that such individual differences variables should matter for phishing, our study indicates that very few of these variables are significant. It is possible that other personality traits would show better predictive power. Future research could determine whether security orientation, risk aversion, computer self-efficacy, etc. have predictive ability in regards to phishing susceptibility. Special attention should be given to non-static personality traits in future research as potential areas that researchers and managers could focus on to reduce the level of phishing susceptibility in at-risk individuals.

We also demonstrate that individuals operate under an optimistic bias regarding their own susceptibilities towards phishing. Specifically, they believe that given phishing behaviors are dangerous, however when attacked with such a behavior, they fall prey to it. The overconfidence in identifying actual phishing attempts causes the recipients of such attacks to have accurate beliefs, but belie them with their overly optimistic behaviors.

Lastly, we demonstrate that financial risk propensities as the only significant deterrent of phishing susceptibility. Although we expected that other risk propensities would also deter phishing susceptibilities, only the financial risk propensity produced such results. This indicates the importance of financial risk inherent in phishing attacks that can successfully alert phishing susceptibilities.

Implications for Practice

Our results indicate several ways in which individuals' susceptibilities for phishing can be successfully altered to encourage safer behaviors and practices. 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 e-mail filter protocols) can increase the abilities of e-mail users to identify and verify the actual identities of those sending messages that may or may not be phishing attempts. Further, by educating individuals about the dangers of relying on textual links, it would be further possible to avoid clicking on such links. However, even with education, individuals would still be overconfident in their abilities and thus fall prey to phishing attempts that they fail to identify, but this overconfidence could be limited through the use of education (Alba and Hutchinson 2000).

Second, by increasing the focus and direction of phishing education campaigns on the risk to finances, the natural risk propensities towards financial loss should also reduce the general susceptibility for phishing.

Third, educational campaigns should be directed towards the frequent usage of the Internet and the inherent danger that it has towards phishing susceptibility. 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 to fall prey to phishing attempts. Further, our results indicated that increased usage of the Internet is related to an increased susceptibility to phishing. Educating individuals about this danger may help to educate them and thereby avoid phishing attempts.

It is also possible that individuals with high Internet use, risk propensities, or boredom proneness can be the ones identified and equipped with tools that will provide warnings or block the links in phishing messages. An extra step might be required that could prevent loss.

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 or advertising campaigns should be made to alert individuals with such a tendency towards boredom. In particular, they should be informed of the propensity of phishing attacks to include suspicious URL addresses as links.

Conclusion

Individuals and organizations are very reliant on the Internet (Anandarajan 2002; Cheung et al. 2000; Lim and Teo 2005), despite the everyday risks of phishing attacks. This papers explores several constructs from IS, psychology and communication research streams to explain why certain individuals are more prone to phishing attacks than others. Our experimental results indicate that several of these constructs are important predictors of phishing success. These findings provide important insights for future research and practice focused on reducing the threat posed by phishing.

References

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

Aiken, L. S. and West, S. G. 1991. *Multiple Regression: Testing and Interpreting Interactions*, Newbury Park, London: Sage Publishing.

Alba, J. W. and Hutchinson, J. W. 2000. "Knowledge Calibration: What Consumers Know and What They Think They Know," *Journal of Consumer Research* (27:1), pp. 123-156.

Anandarajan, M. 2002. "Profiling Web Usage in the Workplace: A Behavior-Based Artificial Intelligence Approach," *Journal of Management Information Systems* (19:1), pp. 243-266.

Banker, R. D. and Kauffman, R. J. 2004. "The Evolution of Research on Information Systems: A Fiftieth-year Survey of the Literature in Management Science," *Management Science* (50:3), pp. 281-298.

Berlyne, D. E. 1949. "Interest as a Psychological Concept," *British Journal of Psychology* (39:1), pp. 184-185.

Berlyne, D. E. 1950. "Novelty and Curiosity as Determinants of Exploratory Behavior," *British Journal of Psychology* (41:1), pp. 48-50.

Berlyne, D. E. 1954. "A Theory of Human Curiosity," *British Journal of Psychology* (45:1), pp. 180-191.

Berlyne, D. E. 1957. "Determinants of Human Perceptual Curiosity," *Journal of Experimental Psychology* (53:2), pp. 399-404.

Berlyne, D. E. 1958. "The Influence of Complexity and Novelty in Visual Figures on Orienting Responses," *Journal of Experimental Psychology* (55:1), pp. 289-296.

Brancheau, J. C., Janz, B. D., and Wetherbe, J. C. 1996. "Key Issues in Information Systems Management: 1994-1995 SIM Delphi Results," *MIS Quarterly* (20:2), pp. 225-242.

Brock, T. C. and Livingston, S. D. 2004. "The Need for Entertainment Scale," in *The Psychology of Entertainment Media: Blurring the Lines Between Entertainment and Persuasion*, L. J. Shrum (Ed.), Mahwah, NJ: Lawrence Erlbaum Associates, pp. 255-274.

Burgoon, J. K. and Burgoon, M. 2001. "Expectancy Theories," in *Handbook of Language and Social Psychology*, W. P. Robinson, and H. Giles (Eds.), Sussex, England: John Wiley & Sons, pp. 79-101.

Chan, M., Woon, I. M. Y., 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), pp. 18-41.

Cheung, W., Chang, M. K., and Lai, V. S. 2000. "Prediction of Internet and World Wide Web Usage at Work: A Test of an Extended Triandis Model," *Decision Support Systems* (30:1), pp. 83-100.

Costa, P. T. and R. R. McRae (1985). The NEO Personality Inventory. Odessa, FL, Psychological Assessment Resources.

Costa, P. T. and R. R. McRae (1992). NEO PI-R Professional Manual. Odessa, FL, Psychological Assessment Resources.

Cowan, B. R., L. Vigentini, et al. (2008). "Exploring the relationship between anxiety and usability evaluation: An online study of Internet and wiki anxiety." Proceedings of IADIS (2008).

D'Arcy, J. and Hovav, A. 2007. "Deterring Internal Information Systems Misuse," *Communications of the ACM* (50:10), pp. 113-117.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (23:1), pp. 79-98.

Dellarocas, C. 2005. "Reputation Mechanisms," in *Handbooks in Information Systems*, A. B. Whinston (Ed.), Oxford, UK: Elsevier, pp. 629-660.

Dhamija, R., Tygar, J. D., and Hearst, M. A. 2006. "Why Phishing Works," *Proceedings of CHI*, pp. 581-590.

Digman, J. M. (1990). "Personality Structure: Emergence of the Five-Factor Model." Annual Review of Psychology 41(1990): 417-440.

Dimoka, A. 2010. "What Does the Brain Tell us about Trust and Distrust? Evidence from a Functional Neuroimaging Study," *MIS Quarterly* (34:2), pp. 373-396.

Farmer, R. and Sundberg, N. D. 1986. "Boredom Proneness - The Development and Correlates of a New Scale," *Journal of Personality Assessment* (50:1), pp. 4-17.

Galletta, D. F. and Polak, P. 2003. "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace," *SIG Workshop on HCI*, pp. 47-51.

Grazioli, S. and Jarvenpaa, S. L. 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), pp. 395-410.

Hackbarth, G., V. Grover, et al. (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.

Herath, T. and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:), pp. 154-165.

Herath, T. and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:1), pp. 106-125.

Hoffman, D. L., T. P. Novak, et al. (1999). "Building consumer trust online." Communications of the ACM 42(4): 80-85.

Holden, S. J. S. and Vanhuele, M. 1999. "Know the Name, Forget the Exposure: Brand Familiarity versus Memory of Exposure Context," *Psychology and Marketing* (16:6), pp. 479-496.

Hovland, C. I. and Weiss, W. 1951-1952. "The Influence of Source Credibility on Communication Effectiveness," *The Public Opinion Quarterly* (15:4), pp. 635-650.

Hwang, Y. and D. J. Kim (2007). "Customer self-service systems: The effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust." Decision Support Systems 43: 746-760.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (50:10), pp. 94-100.

Johnston, A. C. and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

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), pp. 1408-1420.

Joiner, R., Gavin, J., Duffield, J., Brosnan, M., Crook, C., Durndell, A., Maras, P., Miller, J., Scott, A. J., and Lovatt, P. 2005. "Gender, Internet Identification, and Internet Anxiety: Correlates of Internet Use," *CyberPsychology and Behavior* (8:4), pp. 371-378.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Komiak, S. Y. X. and Benbasat, I. 2008. "A Two-Process View of Trust and Distrust Building in Recommendation Agents: A Process-Tracing Study," *Journal of the Association for Information Systems* (9:12), pp. 727-747.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. 2009a. "School of Phish: A Real-World Evaluation of Anti-Phishing Training," *Symposium on Usable Privacy and Security*, July 15-17.

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), pp. 1-31.

Leung, A. C. M. and Bose, I. 2008. "Indirect Financial loss of Phishing to Global Market," *Proceedings of ICIS*, paper 5.

Liang, H. and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 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), pp. 394-413.

Lim, V. K. G. and Teo, T. S. H. 2005. "Prevalence, Perceived Seriousness, Justification and Regulation of Cyberloafing in Singapoer: An Exploratory Study," *Information and Management* (42:8), pp. 1081-1093.

Litman, J. A. and Spielberger, C. D. 2003. "Measuring Epistemic Curiosity and Its Diversive and Specific Components," *Journal of Personality Assessment* (80:1), pp. 75-86.

Lowenstein, G. 1994. "The Psychology of Curiousity: A Review and Reinterpretation," *Psychological Bulletin* (116:1), pp. 75-98.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), pp. 709-734.

McKnight, D. H. and Choudhury, V. 2006. "Distrust and Trust in B2C E-Commerce: Do they Differ?," *Proceedings of the International Conference on Electronic Commerce*, pp. 482-491.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334-359.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), pp. 473-490.

McKnight, D. H., Kacmar, C., and Choudhury, V. 2004. "Dispositional Trust and Distrust Distrust Distinctions in Predicting High- and Low-Risk Internet Expert Advice Site Perceptions," *E-Service Journal* (3:2), pp. 35-58.

McKnight, D. H., Kacmar, C., and Choudhury, V. 2003. "Whoops... Did I Use the Wrong Concepts to Predict E-Commerce Trust? Modeling the Risk-Related Effects of Trust verses Distrust Concepts," *Proceedings of HICSS*, pp. 182.

McRae, R. R. and O. P. John (1992). "An Introduction to the Five-Factor Model and Its Applications." Journal of Personality: 175-214.

Nicholson, N., Soane, E., Fenton-O'Creevy, M., and Willman, P. 2005. "Personality and Domain-specific Risk Taking," *Journal of Risk Research* (8:2), pp. 157-176.

Petty, R. E., Cacioppo, J. T., and Schumann, D. 1983. "Central and Peripheral Routes to Advertising Effectiveness: The Moderating Role of Involvement," *Journal of Consumer Research* (10:9), pp. 135-146.

Petty, R. E. and Wegener, D. T. 1998. "Attitude Change: Multiple Roles for Persuasion Variables," in *The handbook of Social Psychology* (Vol. 1), D. T. Gilbert, E. Fiske, and G. Lindzey (Eds.), New York, NY: McGraw-Hill, pp. 323-390.

Rhee, H.-S., Ryu, Y., and Kim, C.-T. 2005. "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security," *Proceedings of ICIS*, pp. 381-394.
Rossi, P. H. and Anderson, A. B. 1982. "The Factorial Survey Approach: An Introduction," in *Measuring Social Judgments*, H. Rossi and S. L. Nock (Eds.), Sage Publications pp. 15-67.
Shah, P. P. and Jehn, K. A. 1993. "Do Friends Perform Better than Acquantances? The Interaction of Friendship, Conflict, and Task," *Group Decision and Negotiation* (2:2), pp. 149-165.
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," *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), pp. 197-209.
Siponen, M., Pahnila, S., and Mahmood, A. 2006. "A New Model for Understanding Users' IS Security Compliance," *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), pp. 487-502.
Speilberger, C. D. and Starr, L. M. 1994. "Curiosity and Exploratory Behavior," in *Motivation: Theory and Research*, H. F. O'Neil and M. Drillings (Eds.), Nillsdale, NJ: Lawrence Erlbaum Associates, pp. 221-243.
Sternthal, B., Dholakia, R., and Leavitt, C. 1978. "The Persuasive Effect of Source Credibility: Tests of Cognitive Response," *The Journal of Consumer Research* (4:4), pp. 252-260.
Straub, D. W. 1990. "Effective IS Security," *Information Systems Research* (1:3), pp. 255-276.
Straub, D. W. and Goodhue, D. L. 1991. "Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security," *Information and Management* (20:1), pp. 13-27.
Sun, L., Srivastava, R. P., and Mock, T. J. 2006. "An Informaiton Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems* (22:4), pp. 109-142.
Technologies, W. S. 2009. "An Empirical Evaluation of PhishGuru Embedded Training," *White paper*, Wombat Security Technologies.
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), pp. 472-484.
Tupes, E. C. and R. E. Crhristal (1961). "Recurrent Personality Factors Based on Trait Ratings." United States Air Force Aeronautical Systems Division Technical Report: 61-97.
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), pp. 249-273.
Weinberg, S. L. and Abramowitz, S. K. 2008. *Statistics using SPSS: An Integrative Approach*, Cambridge, MA: Cambridge University Press.
Woon, I. M. Y., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," *Proceedings of ICIS*, pp. 367-380.