# Extending Ecommerce Deception to Phishing

Completed Research Paper

**Ryan T. Wright**
Isenberg School of Business
University of Massachusetts
rwright@isenberg.umass.edu

**Kent Marett**
College of Business
Mississippi State University
kmarett@business.msstate.edu

**Jason B. Thatcher**
College of Business and Behavior Sciences
Clemson University
jthatch@clemson.edu

## Abstract

*Phishing threatens the information security of Internet users and corporations. Where most research focuses on the phisher's website, i.e., how to determine if a website is legitimate or not, this study examines the email that begins the phishing process. To understand why Internet consumers respond to phisher's emails by sharing sensitive information, we draw on models of e-commerce deception to explain the efficacy of phishing strategies (e.g., content and presentation) found in the content of email messages. To test our hypotheses, we conducted a field experiment that manipulated the content of phishing emails. Consistent with our hypotheses, we found content manipulations improved the likelihood of our subjects' conveying sensitive information. Further, we found that cognitive processes can influence a consumer's likelihood of being deceived. However, hypotheses about deception support mechanisms and presentation manipulations were not supported. In sum, we find support for the general theory of ecommerce deception as well as our cognitive processing explanations for phishing's effectiveness. The paper concludes with practical and research implications.*

**Keywords:** Phishing, Online deception, CMC deception, Deception, Field experiments, Ecommerce, Deception Theory, Computer-mediated communication and collaboration

## Introduction

Almost every Internet consumer has received a phishing email soliciting sensitive information. In a typical year, more than 65 million Americans received illegitimate emails seeking contact information, Social Security numbers, or financial information (Anti-Phishing Working Group 2013). 2013 was a record year for phishing attacks on corporations (Symantec 2014). Companies suffered major losses in both customer confidence and market share due to breaches caused by phishing attacks. For example, in late 2013, an employee for a firm that does the sub-contracting work for most of the Target stores fell for a phishing attack. Using this employee's login credentials, cybercriminals were able to not only gain access to Target's network, but to install software in 1700 stores that collected credit card information. This results in over 70 million customer's credit cards being compromised (Bjorhus 2014). Despite public awareness of the dangers of sharing information over the Internet, phishing attacks have increased by 200% and remain effective, with more than 2.85 million Internet consumers sharing sensitive information since 2008 (Anti-Phishing Working Group 2013).

Phishing is "a criminal mechanism employing both *social engineering* and *technological subterfuge* to steal consumers' personal identity data and financial account credentials." (Anti-Phishing Working Group 2013 p.2). *Technological subterfuge* involves schemes to plant malware on consumers' computers to steal usernames and passwords. *Social engineering* attacks use messages from purported legitimate sources to trick consumers into divulging sensitive information (Dhamija et al. 2006; RSA Security 2008). Email is phishers' primary *social engineering* tool (Anti-Phishing Working Group 2013). Typically, Internet consumers receive an unsolicited email, which offers a benefit in exchange for information. The consumers are asked either to click on a link in the email or directly respond to the email itself.

In order to better understand why consumers fall prey to phishing, it is important for research to examine the email message in a behavioral context. This is particularly important because email-only phishing attacks (sometimes referred to as spear phishing) are on the rise (Schwartz 2011). Typically, research has examined one of two methods for detecting a phishing email (Wright et al. Forthcoming). Either, there is an attempt to develop better techniques to filter phishing messages (i.e., spam filters) or to develop better deception detection support mechanisms (toolbars and plug-ins) that examine specific email properties. Unfortunately, neither filtering or deception detection support mechanisms have been very successful (Fette et al. 2007).

Hence, this study focuses on understanding why consumers respond to the content of phishing emails rather than the properties of the phishing web site itself. Prior research has examined behavioral characteristics, such as individual and situational characteristics that lead to phishing emails' effectiveness. For example, Wright and Marett (2010) focused on experiential and dispositional factors that increase the likelihood of detecting phishing. They found that experiential factors (e.g., computer self-efficacy, web experience and security knowledge) significantly influenced deception success. Further, they found that dispositional factors were less predictive of phishing e-mail's effectiveness, with only suspicion predicting deception success. Although extant research has provided initial evidence of behavioral reasons why deception tactics work there remain substantial opportunities to examine consumers' behaviors (Dhamija et al. 2006; Wright et al. 2010b). In particular, deception techniques and detection mechanisms, which are important in the deception process, have received limited attention (Xiao et al. 2011). More specifically, our study addresses the following research questions:

> *RQ1: What content-based properties of phishing emails increase the likelihood of sensitive information sharing?*
>
> *RQ2: What cognitive processing styles increase the likelihood of sensitive information sharing?*

Although researchers have started to explore the behavioral aspects of social engineering, inconsistent results may impede practitioners when applying this stream of research. Table 1 provides a summary of results in past phishing studies. For example, there has been mixed results with regard to whether online experience is a factor to the success of phishing message. Likewise, results for the impact of demographic factors like the gender of the intended victim have also been mixed. Taking together, the literature presented in Table 1 and other reviews of the phishing literature (Purkait 2012), it seems probable that there may be other underexplored factors that may impact one's appraisal of a phishing message. A clear theoretical framework is needed to guide researchers in their investigations of why phishing is effective. Also, it is important that any study on phishing incorporate an investigation of the properties in the email.

Social engineering research suggests that e-mails' content may also explain why Internet consumers are deceived by phishing emails. Social engineering principles were originally developed to help understand why consumers fall prey to illegitimate telephone, mail, or face-to-face solicitations for sensitive information such as credit card numbers or passwords (Mitnick et al. 2005). Consider a typical phishing email. There are three elements that social engineers suggest help deceive consumers. First, the option exists for the phisher to personalize the message. Although our sample email is not personalized to the individual consumer, it is focused on a narrow band of Internet consumers, the customers of a specific financial institution. Second, the email contains a "call to action," i.e., a specific timeframe for responding. Finally, the phisher may embed cues or information that improves message legitimacy. In our email, sender information is embedded in two locations, the graphic header and the text-based footer. Social engineering principles suggest that by incorporating such elements in emails phishers increase the likelihood that an Internet consumer will share information.

**Table 1. Results of Past Phishing Studies**

| Phishing Factors | Supported | Not Supported | Partially Supported |
|---|---|---|---|
| Online Experience | (Sheng et al. 2010) (Wright et al. 2010b) | (Downs et al. 2006) (Dhamija et al. 2006) (Jingguo et al. 2012) | |
| Security Awareness | (Jakobsson 2007; Wright et al. 2010b) (Mohebzada et al. 2012) | (Downs et al. 2006) (Dhamija et al. 2006) | (Jingguo et al. 2012) |
| Education | (Jagatic et al. 2007) (Sheng et al. 2010) | (Dhamija et al. 2006) | |
| Relationship with Sender | (Jagatic et al. 2007) | | (Kumaraguru et al. 2007b) |
| Women are more vulnerable | (Sheng et al. 2010) | (Dhamija et al. 2006) (Mohebzada et al. 2012) | |
| Age | (Sheng et al. 2010) | (Dhamija et al. 2006) (Mohebzada et al. 2012) | |
| Risk | (Sheng et al. 2010) | (Wright et al. 2010b) | |
| Trust | (Jakobsson 2007) | (Wright et al. 2010b) | |

Hence, this study empirically also examines how the content of phishing e-mails relates to the efficacy of Phishing e-mails. To do so, we leverage theoretical insights offered by Xiao and Benbasat (2011) to explain why message recipients may be prone to responding to phishing emails. The general goal of this study is help researchers and practitioners develop prescriptions or tools that enable Internet consumers to protect their data from phishers.

To investigate our question, we begin by tying current research on phishing to the deception information practices literature. Next, we identify a psychological theory that helps to explain deception detection. Specifically, we use the elaboration likelihood model (ELM; Petty et al. 1999) to explain the effectiveness of phishing tactics. Then, we describe our field experiment, which directly manipulated emails' content to evaluate whether different phishing tactics lead to Internet consumers' sharing information. We conclude with a discussion of our results implications for future phishing research and the suggestions this research can offer to practitioners.

## A Taxonomy of Phishing

To lure consumers into sharing information, phishers use deceptive techniques that seek to increase Internet consumers' perceptions of their messages or websites' legitimacy. *Deception* refers to "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver" of the message (Buller et al. 1996b pg. 121). The key word in the definition is "knowingly," as the intent of the sender (henceforth referred to as phisher) rules out including the transmission of false information by mistake or accident. Therefore, cues in the deceitful message are purposefully developed by a phisher, with careful thought given to how they influence the receiver's decision making (Dhamija et al. 2006).

Effective deceptive techniques avoid the appearance of "deviating" from what is normal. Burgoon and colleagues (2008) suggest that deceptive tactics are more effective when they create an outwardly realistic message. By doing so, phishers prevent triggering a state of suspicion in the message's receiver (Zhou et al. 2004). Within the field of information systems, deceptive tactics have been investigated in various experiments involving the falsification of personnel information within databases (Biros et al. 2002) and fraudulent e-commerce websites (Grazioli et al. 2003a; Grazioli et al. 2003b; Riquelme et al. 2004).

Prior research has developed many ways of classifying deception techniques in online and face-to-face interactions. Of particular interest to this study is the development of Information Manipulation Theory (McCornack 1992), which proposes that deceivers intentionally modify the quantity, quality, and manner in such a way as to divert message receivers attention. Researchers have since appropriated the theory to help explain deception conducted via computer-mediated communication (e.g. Johnson et al., 2001).

Drawing on the work of Buller, Burgoon, and colleagues (Buller et al. 1996a; Burgoon et al. 1994) and extending Johnson et al.'s (2001) implementation of Information Manipulation Theory, Xiao and Benbasat (2011) developed a three-part typology of online ecommerce deception techniques:

1. The manipulation of *information content*. In terms of e-commerce, this type of deception "refers to the direct alteration of the content of product information provided at an e-commerce website" (Xiao et al. 2011 p. 172).
2. The manipulation of *information presentation*, "which refers to the manipulation of the design of how product information is presented to consumers at in e-commerce website" (Xiao et al. 2011 p. 172).
3. "The manipulation of *information generation*, which refers to the manipulation of the dynamic production of product information at an e-commerce website, based on consumer interests, needs and/or preferences obtained explicitly or implicitly" (Xiao et al. 2011 p. 172).

While Xiao and Benbasat (2011) offer a typology of deception techniques (*content*, *presentation*, and *information generation* manipulations) that shape a phishing e-mail's authenticity, research has not empirically examined how these techniques effect Internet consumers' information sharing. In the following section, we describe a study that employs a theory-based approach to empirically test the effectiveness of these information manipulation tactics (See propositions 18 & 19 Xiao et al. 2011). Specifically, drawing from the Elaboration Likelihood Model (ELM), we describe the process through which Internet consumers appraise messages and test whether *content*-based or *presentation*-based manipulations lead to email recipients sharing information.

Due to the nature of the email of interactive websites, *information generation* manipulation is somewhat limited. Typically *information generation* is done in a back-and-forth communication between the systems (or deceiver) and the target of the deception. This includes personalization of deception information based on what the target is doing real-time. The closest attribute to information generation is the mass customization that we see in the real phishing email example, where an email is sent to many people some of which belong to the credit union. Phishing emails that lack customization, yet are allegedly from an institution that the consumer does business with, will have a high probability of deception detection or will be discarded without a thought. Therefore, *information generation* is outside the scope of this empirical research, as we will be controlling for personalization of the message through the experimental design.

## Cognitive Mechanisms in Deception Detection

To elicit sensitive information, phishers take advantage of how Internet consumers cognitively process messages that contain imperfect information. The cognitive psychology literature offers insight into individuals' decision-making when presented limited information (e.g., phishing emails rich in *content* and *presentation* tactics). Dual-processing theories explain how an outcome can result from one of two psychological processes that result in changes in mind-set and subsequent actions. The application of dual-process theories is common in psychology (Petty et al. 1986; Petty et al. 1981; Warden et al. 2006; Werner et al. 2002) and has been applied to explain a range of purchasing activities (Areni 2003), decision-making efforts (Nah et al. 2004), web personalization strategies (Tam et al. 2005), and even information technology acceptance (Bhattacherjee et al. 2006).

To examine the effectiveness of phishing, we leverage ELM, a dual processing theory, to explain why consumers respond to deceptive emails. This decision making process describes not only the role of beliefs, thoughts and perceptions, but also how individuals form them. ELM theorizes that "the classic sources (e.g., expertise), message (e.g., number of arguments), recipient (e.g., mood), and contextual (e.g., distraction) variables have an impact on attitudes towards objects, issues, and people." (Petty et al. 1999 pg. 42). These ideas are consistent with what Benbasat and Xiao (2011) refer to as the cognitive mechanisms' of stimulus, organism and response framework. Specifically, they suggest that "the deception detection process may result in consumers' belief that the e-commerce website is deceptive and subsequently lead to an avoidance behavior on the part of the consumers" (pg. 178). ELM suggests that the detection decision process occurs along a continuum that ranges from low cognition to high cognition. Under low conditions, individuals do not deeply think about the information that shapes their decisions. Under high conditions, individuals carefully scrutinize their choices and reflect on likely outcomes (Petty et al. 1986). Hence, when consumers rely on low cognition, they are more apt to decide to respond to deceptive emails.

Consistent with neuroscience research (Grèzes et al. 2005; Grèzes et al. 2004; Hughes et al. 2005) that suggests distinct areas of the brain are activated during decision making, ELM proposes that two cognitive processes shape decision-making, the central route and the peripheral route, and that motivation and the ability to process information drive which route will be utilized (Petty et al. 1986). The central route involves cognition-based processing and critical thinking, as the receiver of the message typically has the motivation and ability to closely scrutinize the information contained in a message, before either attitudinal change occurs or the receiver selects a course of action. The peripheral route is more unconscious, automatic, and associative, as the receiver of the message tends to rely on simple cues and readily available decision rules for making judgments, as opposed to the use of more thoughtful central processing. According to the ELM-based research, when individuals perceive a situation as complex or uncertain, they engage in central route processing, and exert effort to make the correct decision; that is, unless they perceive a situation as simple, in which case they rely on peripheral decision making (Feigenson 2006).

Beyond the context or uncertainty, researchers in marketing have investigated conditions under which consumers engage in central or peripheral processing. For example, Karmarkar and Tormala (2009) examined subjects' perceptions of a restaurant reviewer's expertise based solely on the message content. Of relevance to this study was the finding that readers who peripherally examined the message tended to be persuaded by the review, regardless if the reviewer was credible. Although ELM was developed as a means for understanding processing styles, some suggest that objective categorization of cues that prompt individuals to use either central or peripheral processing routes can yield insight into decision-making (Bitner et al. 1985).

## HYPOTHESIS DEVELOPMENT

Information content manipulation is the direct altering of content. In terms of phishing, *information content* can be manipulated or "socially engineered" to offer the appearance of normalcy. This type of deception involves manipulations of differing content-based information (Burgoon et al. 1996; McCornack et al. 1992). Past studies in deceptive communication indicate that most people are unlikely to detect deception if only attending to cues (e.g., misspelling, sender information) that proceed from the message, rather than analyzing the message for discrepancies (e.g., how truthful is the message) (Miller et al. 1993). Further, empirical tests of a deception detection model (See Park et al. 2001) point to greater accuracy in deception detection for messages that are manipulated to have more truthful content than lies (i.e., have a truthful bias). In other words, the messages with more lies are harder to detect than messages with a single lie. Therefore, we expect that phishers who utilize content-based tactics have a better chance of successfully duping message recipients into responding with the information that the phishers desire.

Xiao and Benbasat (2011) outline a typology of deception information practices as noted above. It is important to operationalize this conceptual typology in terms that describe phishers' operational-level techniques. The dimensions of operational-level technique in content manipulation are *completeness*, *clarity*, and *veridicality*. In phishing, we often find these types of content manipulation (Fette et al. 2007). We draw from Buller's work to define these terms. C*ompleteness* is the withholding of information either explicitly or implicitly. We can manipulate *completeness by using* personalized information. Further, *completeness* in the salutation of an email has variety between no personalization and no salutation, to complete personalized, such as "Dear John Smith".

*Clarity* is the manipulation of full information. In phishing this can include part of the message, or all or part of the sender's information. Finally, *veridicality* is content-manipulation based on false information given in the message. In many phishing emails, including the example of the real phishing message this can be a call to action, such as “please answer this email ASAP”. Phishing emails vary greatly in the types and levels of these three types of content-based manipulations. According to deception research, each of these tactics affects the likelihood of deception success (Buller et al. 1996a; Xiao et al. 2011). Therefore we predict:

> H1: A phishing message that contains content manipulations will have a greater chance of success than a message without this manipulation.
> H1A: A phishing message that contains completeness manipulations will have a greater chance of success than a message without this manipulation.
> H1B: A phishing message that contains clarity manipulations will have a greater chance of success than a message without this manipulation.
> H1C: A phishing message that contains veridicality manipulations will have a greater chance of success than a message without this manipulation.

## Types of Deception Techniques: Information Presentation

*Information presentation* manipulations involve modifying the properties and context surrounding a message to influence their interpretation by message receivers. Cues in this category tend to be external to the message content itself and have the potential to affect the receiver’s willingness to believe the message without even being exposed to the message content (Mondak 1993). For instance, to give the deceptive message a more authentic context, phishing efforts (as well as efforts at installing virulent code on targets’ computers) may mimic the source email address of a party familiar to the recipient. The logic is that an unsuspecting recipient of a phishing message would be more likely to be persuaded to share private information when a seemingly-familiar person requests it, such as a person in the same university network.

> H2: A phishing message with presentation manipulations will have a greater chance of success than a message without this manipulation.

## Deception Detection Support Mechanisms

The final two hypotheses focus on automated tools and cognitive processes that may aid phishing message recipients in detecting deception. As discussed by in Xiao and Benbasat (2011), most cognitive studies have shown that deception detection is little better than chance (Park et al. 2001). First, Hypothesis 3 examines any the availability of technology support that may help message recipients. Previous studies, mainly in the computer science field, have looked at technology-based solutions for combatting phishing. This includes the use of intelligent agents (Fu et al. 2006), analytics (Liu et al. 2006), and training systems (Kumaraguru et al. 2007a) that are designed to “red flag” messages originating from questionable domains. Further, research suggests that detection support mechanisms such as anti-phishing toolbars and spam filters marginally increase deception detection (Sheng et al. 2007). Still, researchers posit that deception detection is “more likely to occur when consumers are provided with mechanisms” (Xiao et al. 2011 p. 186). This includes technology-based mechanisms that identify anomalies or filter possible deceptive messages. Therefore, we propose that:

> H3: The availability of technology-based detection mechanisms to message receivers will negatively impact the success of the phishing message.

## Cognitive Mechanisms: Central and Peripheral Processing

Finally, the cognitive processes employed by message recipients are considered to be potential impediments toward phishing success. As discussed earlier, there is little agreement on the individual and situational factors that influence one’s susceptibility to phishing message. Instead, the current study examines how consumers’ deception detection process shapes decisions about phishing emails (see the cognitive mechanism in Xiao and Benbasat’s theoretical model). Following from ELM, successful phishing depends on receivers failing to detect the deceptive intent behind a message; thus, whether emails evoke central or peripheral processing is essential to a phisher’s ability to deceive Internet consumers. Research on deceptive communication has identified verbal and nonverbal cues that deceivers unwittingly send, which can reveal the false nature of the message (DePaulo et al. 2003; Ekman et al. 1991) in either face-to-face or computer-mediated exchanges. However, noticing the existence of verbal and nonverbal cues is difficult, and individuals recognizing them as indicators of deception is even more challenging (Levine et al. 1999).

Because email is a relatively lean medium compared to face-to-face communication (Dennis et al. 2008), the medium effectively filters most verbal and nonverbal cues identified in the deception and social engineering literatures. Email is less socially rich, making it likely to convey only paralinguistic cues to receivers (Rao et al. 2000). This means that noticing deceptive cues contained within an email requires a receiver to observe when its phrasing strays from that found in "normal" email messages in a highly noticeable way. Examples of cues in an email could include referring to a receiver in an awkward manner such as "doctor professor" or using phrases that vary from normal baseline language that the communicator has used in the past, such as a sudden increase in negative emotion or increased personal-distancing language (DePaulo et al. 2003). Absent highly noticeable cues, it is more likely that the receiver will detect deception through message content that is personally implausible or contradicts earlier content, i.e., internal inconsistencies or discrepancies (Miller et al. 1993).

Regardless of the type of tactic employed by phishers, ELM suggests that the key driver of deception detection will be which cognitive processing route is employed by Internet consumers (e.g., central or peripheral). If the central route is activated, which is theoretically resistant to persuasion, a person exerts relatively extensive effort to examine the information. However, if the peripheral route is activated, a consumer is likely to exert lower cognitive effort and invest less time examining information. Because the peripheral process is "relative temporary and susceptible to counter-persuasion" (Petty et al. 1999), Internet consumers who rely on peripheral processing are less likely to bring a higher level of cognitive resources to bear when evaluating the message. Therefore, when peripheral routes are triggered, an Internet consumer is more susceptible to deception.

Whether phishing emails evoke central or peripheral processing likely influences the efficacy of the phishing messages. According to Johnson and colleagues, detecting deceptive information, such as that found in phishing messages, is contingent on a sort of violation of expectancies. When the referring email appears to be normal, and therefore does not violate expectations and stimulate critical, central processing, receivers are more likely to accept the phishing messages as normal. In this circumstance, we suspect a kind of "transfer of processing" occurs, with a redirected Internet consumer transferring peripheral processing used to evaluate an email to assess the phishing website.

Based on our review of deception tactics and the ELM, we forward an additional hypothesis based on cognitive processing. This hypothesis examines whether central route processing decreases the likelihood that a receiver will be deceived. We propose:

> H4: Receivers who use peripheral route processing will be more likely to be deceived than receivers who use central route processing.

## Method

To evaluate our hypotheses, we conducted a field experiment. Two hundred twenty-four students enrolled in an introductory MIS course participated in our experiment. The average age of the students was 21.02 years, and slightly more than half were male (52%). All of the subjects possessed 5 years or more of Internet experience and had completed at least one online purchase. One subject acknowledged being a victim of phishing/identity theft previously and was removed from the study.

**Procedure.** Our field experiment was patterned after prior phishing research (Finn et al. 2008; Wright et al. 2010b). The experiment unfolded in three steps. First, unique passwords, which were referred to as the "Super Secure Code" (SSC), were issued to each subject the first week in class. The SSC provided access to specialized software in a controlled lab. To ensure the subjects understood that keeping the SSC private was important, we delivered it in an official university envelope that included the university logo and contact information and a signature across the seal of the envelope. The subject's name was printed on the outside of the envelope. The code was printed on official university letterhead with the injunction to "not disclose this [SSC] code to anyone." Finally, lab instructors explained to subjects that they should not share the SSC with anyone under any circumstance, as it could "breech the secure grading process and could affect their grade for the class." Subjects signed a non-disclosure agreement that they would abide by the class policy.

Second, eight weeks into the course, after class lectures on information security and online risks, the subjects received an email from a fictitious IT employee, "Jason Roth," that requested they disclose their "Super Secure Code" in order to help recover from a data management accident. This email contained combinations of four tactics used by phishers.

Third, included in a debriefing, we asked the subjects to provide information regarding their experience with the phishing email. We asked our subjects to locate the phishing message in their email accounts, if possible, and to complete a survey that captured demographic information and asked open-ended questions about their experience. The goal of this step was to determine whether the subject used anti-phishing software and to evaluate the form of cognitive processing used to evaluate the phishing email. The final part of the debriefing session was to let the subject know that the message was a part of the phishing experiment and that personal information would be destroyed upon completion of the data collection as per Institutional Review Board (IRB) requirements for this study. Students were also encouraged to contact the research team, or an IRB representative with any question, comments or concerns.

**Tactics.** Drawing on the hypotheses to guide the operationalization of this field study, we chose to manipulate the phishing message *presentation* by changing the sender's email domain. All email messages have an element of *presentation*. Our *presentation* manipulation used one of three email domains: 1) a generic "mail.com" account, 2) a spoofed address that appeared to be from the university.edu domain, and 3) a legitimate.edu address coordinated with the university behind the scenes. The legitimate ".edu" phishing email was sent using the university's mail servers. Accordingly, the spoofed emails were sent using an off-campus mail server configured to send emails that are addressed from the same ".edu" domain. This is a common tactic used by phishers. For example, one might receive an email from admin@paypa1.com when clearly the origin of the email is not the paypal.com domain.

The three types of manipulation for *content* were operationalized as: 1) manipulation by *clarity*, 2) manipulation by *completeness*, and 3) manipulation by *veridicality*. *Clarity* of the message was manipulated by supplying specific information to the recipient to gain trust. Clarity manipulations use specific semantics and mechanisms familiar to the recipient within the message to avoid suspicion (Burgoon et al. 1996). Clarification manipulations in phishing can often be represented by dropping names of people or organizations associated with the receivers. We operationalized this by adding a condition that included dropping the name of the subject's instructor into the body of the email. *Veridicality* is often seen as a call to action within a phishing message. We operationalized this with a request for an urgent response. Call to action is often utilized during deception interactions; this category's messages are either actual *veridicality* or apparent *veridicality* (Burgoon et al. 1996). Scholars have expanded the concept of *veridicality* within the context of e-commerce to include the idea of "decoying," whereby, the *veridicality* is manipulated by "distracting the victim's attention away from what is really going on" (Grazioli et al. 2003b p. 198). In the case of phishing, this is typically done by adding a sense of urgency.

The last *content* manipulation technique is *completeness*. Burgoon et al. (1996) define this manipulation as providing the right amount of information to fulfill the conversational demands. Information provided can take the form of many aspects of the message. In the case of phishing, personalization of the salutation is often used to provide *completeness*. We manipulated the phishing message accordingly: manipulated messages had the complete personalized salutation, and the other condition was more generic. In sum, there were four content conditions: 1) *completeness* (e.g., addressed the subject directly in the email), 2) *clarity* (e.g., used their instructor's name and their class's title in the email), 3) *veridicality* (e.g., asked the email be responded to immediately), and 4) low condition that had no content other than the call to respond to the email. Finally, the *presentation* of the message was operationalized by manipulating the sender's email platform: 1) real university.edu account that was sent from a university server (real.edu), 2) spoofed university.edu account that was sent from a spammer email server where any domain sent from a dedicated off-campus server, and 3) free email service mail.com (in this case mail.com). The phishing effort succeeded when a subject replied with the SSC.

**Evaluating H1 to H3.** A fractional factorial design (Pedhazur et al. 1991) was utilized used to evaluate the main effects of the phishing tactics' effectiveness (e.g, H1 to H3). This type of design was selected for two reasons. First, ideally in order to provide enough statistical power a full-factorial design 3x2x2x2 would include 24 treatment conditions that need a minimum of 25 subjects for each condition or 600 subjects total. Due to a limited amount of subjects available at the business school, we chose to test only for the main effects for each condition, allowing us to obtain enough power within constraints of our research site (Cook et al. 1979). Given the nature of phishing, the field experiment had to be run one time only with our maximum recruitment basis. In other words, as soon as the subjects were run through the field experiment no subjects can be recruited for several semesters so that the subjects would not contaminate our results thus allowing us the opportunity to execute this experiment every 3 or 4 years. We, therefore, made a decision to evaluate the main effect using a fractional 3, 3x1 design. Because each email included a sender, the research has no absence of a condition of the *presentation* manipulation team. By designing a fractional experiment, we empirically tested for the increase or decrease in likelihood that a subject would answer the phishing email with sensitive information.

**Evaluating H4.** Open ended responses collected during the debriefing were coded by three evaluators. The goal of this coding of each open-ended response was to determine which the elaboration route that the subject used in determining how to act on the phishing email. The independent raters, two of whom were on the research team and the other an industry expert, then evaluated each open-ended question using a three-step process (Denzin et al. 2003). First, all three evaluators agreed on the basic definitions of the coding choices. For the central route, it was determined that this type of process takes place "when individuals have the motivation and the ability to process information. Considerable cognitive effort tends to be allotted and issue-relevant thinking is typically engaged." Further, the peripheral route is activated "when individuals have an absence of focused examination. This means that the likelihood of the individual to elaborate is low and therefore less cognitive processing takes place." The evaluators were also given the ability to code the question as "undetermined" when there was not enough information to make a decision between the central route and the peripheral route. The research team understands that a subjects' retrospective recall of the cognitive process may introduce some bias and discuss possible biases in the limitation section.

Before the raters evaluated the transcripts, the raters were trained on the strict definitions of the processes according to the ELM. Further, group unison was defined and discussed at length. The raters' training took place over several sessions with a world expert on decision-making and cognition. Inter-rater reliability was tested using Fleiss's kappa, which is appropriate when three raters are used. Our analysis provided a kappa of .62, which indicates strong agreement among the raters (Landis et al. 1977). The items were not agreed upon were discussed and recoded independently. Only 2 cases the researchers could not agree on and were therefore discarded. The results of this coding provided the data necessary to complete the second step of the analysis, which was testing the research model in its entirety.

## Results

Results are presented in two sections. First, we analyzed subject responses to open ended questions and coded which cognitive process was used in the decision (e.g., central or peripheral). Second, we evaluated the main effects of the manipulations, deception detection mechanisms, and cognitive mechanisms using binary logistic regression. Through this two-step analysis, we answered specific questions regarding the effects that were drawn from the types of cues in the phishing message while also examining the subjects' cognitive processes suggested by elaboration theory. To test each hypothesis, we used a binary logistic model. This analytic technique was chosen because the dependent variable (DV) and most of the independent variables (IVs) were categorical (Pedhazur et al. 1991). Logistic regression is less susceptible problems tied to non-normal independent variable data making it an appropriate technique for using our data to evaluate the hypotheses. To ensure the linearity assumptions of logistic regression were met (Pedhazur et al. 1991), we used an analysis of the variance inflations factors (VIFs). Our results indicated VIFs of less than 0.2, suggesting that it was safe to use binary logistic regression to evaluate hypotheses using our dataset.

The IVs represent the *presentation* (1 = real.edu, 2 = spoofed.edu, and 3 = mail.com), the *content* conditions (1 = low condition with no content manipulation, 2 = *completeness*, 3 = *clarity*, and 4 = *veridicality*), the type of email system utilized by the subjects (*deception detection mechanisms* coded 1 through 7 for the different email systems), the type of cognitive process utilized by the subject (1 = unknown, 2 = central route  and 3 = peripheral route), and two control variables (sex and age). The dependent variable was binary (1 = answered with SSC and 2 = did not give SSC). The enter Wald method was used in the regression. This involves testing the model with all of the particular conditions. The final model was significant at p < .000 and had a Cox and Snell R-square of .462 and a Nagelkerke R-square of .593 (Mertler et al. 2001). Table 2 reports the results of the logistic regression. To determine the impact for each IV on our DV (if subjects were deceived), we first identified the statistically significant factors. These results show that for *content (H1)* that *clarity* was not significant; therefore, it does not influence successful deception any more or less than the low condition. In addition, we see that *completeness* and *veridicality* are both significant. Next, we examined the beta value to see if the influence was positive or negative.

A positive value would indicate that this condition would increase the likelihood of deception success. Completeness and veridicality were positive. Finally, we examined the odds ratio labeled Exp (B). The odds ratio is the factor that the IV increased (or decreased) the log odds of the DV (Pedhazur et al. 1991). The odds ratio is derived from probability of a condition over the baseline condition. For example, the odds ratio was 2.622 for the *completeness* manipulation. This indicates that the likelihood increased 2.6 times when this manipulation tactic was present over the low condition. The other statistically significant trait suggested by the analysis was *veridicality*. Using the same interpretation as *completeness*, when *veridicality* was used in the email there was a 3.19 times higher likelihood of the consumer sending his or her SSC. Finally, we see that the low condition was significant, and therefore, any *content* manipulation statistically influenced the deception outcome variable. In sum, evidence provided by the data shows that *content* (H1) and types of *content: completeness* (H1A) and *veridicality* (H1C) all statistically aided successful deception. However, *clarity* (H1B) did not aid in the likelihood of deception.

As the frequency statistics suggest, none of the *presentation* conditions (H2) were statistically significant factor in phishing deception. Next, we examined the detection mechanisms. Similar to the *presentation* manipulations, none of the detection mechanisms influenced deception (H3). Conversely, the cognitive processing mechanisms influenced the DV. The baseline undetermined processing was significant and therefore provides evidence that the cognitive process in general is influential. The peripheral route was positive, and therefore, the likelihood of deception increased by 4.6 times when this route was utilized. The central route was also statistically significant and, as ELM predicted, decreased the likelihood of deception by a factor of 0.74. This result provides evidence for H4. Finally, the control variables of sex and age were not significant in this model.

## Discussion

This study focused on understanding why phishing emails persuade Internet consumers to disclose sensitive information. To do so, we examined *content* and *presentation* deception techniques along with cognitive processes, which are either present in, or applied to, phishing messages sent to Internet consumers. To evaluate these factors, we conducted a field experiment that manipulated the presence of cues within email messages, while also controlling for the actual email that subjects evaluated, we examined the thought process behind their information processing. This differs from other research examining the cognitive processes utilized by phishing message recipients which relied on subjects to recall past phishing attacks (Vishwanath et al. 2011).  From a phishing perspective, our attack was a success. We gained the super secure codes of a quarter of our subjects, as well as other unsolicited information, including some subjects' cell phone numbers, student ID numbers, and even a few Social Security numbers. Our analysis suggests that two *content*-based phishing tactics (*completeness* and *veridicality*) are more likely to elicit sensitive information from our subjects than context-based tactics.

Further, our results were consistent with our ELM-based explanation for phishing effectiveness. Specifically, if a subject employed the central route to process our phishing email, deception was less likely. However, when a subject employed the peripheral route, subjects were more likely to be deceived.

When we evaluated the specific tactics, manipulating *content* through *completeness* and *veridicality* more effectively deceived our subjects. *Completeness* is one of the most frequently employed online deception tactics, as fabricating an event or circumstances can easily be applied to information intended for a mass audience (Wright et al. Forthcoming). Absent of clear deceptive cues (i.e., obvious fabrication or visible errors in the message), *completeness* may be effective because it evokes receivers' peripheral processing. For example, an email lacking errors that offers "nominal risk" such as their zip code or the spouses name may not evoke central processing. This may be due to the relatively small risk offered (i.e., it is not large enough to evoke concern about fraud). However, there is a continuum to risk. Wright and his colleagues (Wright et al. 2010a; Wright et al. 2010b) have previously shown that the dispositional factors, which includes risk, impact phishing efficacy. For example, some consumers will give very little information to anyone online due to their prospection of this being a high risk behavior, while others will give a great deal of detail online because they do not perceive it as high risk.

**Table 2. Results of the Binary Logistic Regression**

| Hypotheses | Variable | Beta | S.E. | Wald | df | Sig. | Exp(B) |
|---|---|---|---|---|---|---|---|
| Content | Low | | | 9.418 | 3 | 0.024 | |
| | Completeness | 0.964 | 0.560 | 2.965 | 1 | 0.045 | 2.622 |
| | Clarity | -0.282 | 0.639 | 0.194 | 1 | 0.659 | 0.754 |
| | Veridicality | 1.161 | 0.560 | 3.303 | 1 | 0.038 | 3.193 |
| Present | XXX.edu | | | 4.907 | 2 | 0.086 | |
| | spoof.edu | 0.808 | 0.494 | 2.675 | 1 | 0.102 | 2.243 |
| | mail.com | 0.559 | 0.544 | 5.531 | 1 | 0.133 | 1.185 |
| Detection Mechanisms | hotmail.com | | | 5.871 | 6 | 0.438 | |
| | XXX.edu | 0.441 | 0.567 | 0.604 | 1 | 0.437 | 1.554 |
| | yahoo.com | 0.245 | 0.651 | 0.142 | 1 | 0.707 | 1.278 |
| | gmail.com | -1.339 | 0.848 | 2.494 | 1 | 0.114 | 0.262 |
| | aol.com | -0.391 | 0.849 | 0.212 | 1 | 0.645 | 0.676 |
| | msn.com | 0.930 | 0.909 | 1.046 | 1 | 0.306 | 2.535 |
| | Other | -0.298 | 0.762 | 0.153 | 1 | 0.696 | 0.743 |
| Process | Undetermined | | | 40.894 | 2 | 0.000 | |
| | Peripheral | 1.530 | 0.738 | 4.295 | 1 | 0.038 | 4.617 |
| | Central | -1.738 | 0.701 | 6.148 | 1 | 0.013 | 0.176 |
| | Sex | -0.129 | 0.405 | 0.101 | 1 | 0.751 | 0.879 |
| | Age | 0.122 | 0.070 | 3.062 | 1 | 0.080 | 1.129 |
| | Constant | -6.468 | 2.070 | 9.767 | 1 | 0.002 | 0.002 |

In contrast to *completeness*, *veridicality* is a less commonly-employed phishing tactic, as it requires a deeper understanding of the target. In this case, we possessed the information necessary to tailor each message to each recipient. In an applied setting, such tailoring is possible only after a security breach, when phishers have obtained receivers' confidential information. For organizations, this suggests that sensitizing Internet consumers to security breaches when they occur is particularly important. While many firms make a practice of contacting account holders after a breach, we believe it is important for such contacts to include information on *veridicality* tactics that phishers may employ. For example, an insurance company that has data stolen may wish to inform customers about the range of ways that the stolen data may be used, from customizing emails to appear that they are from the company to competing insurance agencies or banking institutions. For individuals, this finding underscores the importance of limiting personal information's online availability that can be used to customize emails.

While the analysis did not offer support for the effectiveness of *clarity*, our findings offer insight germane to future research on this phishing strategy. To emulate real phishing tactics, we manipulated the sender's email address, not the sender's name. In our field experiment, subjects replied to "Jason Roth" fairly evenly across all three mail domains. According to the ELM, detecting a contextual manipulation such as *clarity* requires central route processing on the part of the receiver, and our results indicate that the subjects did not scrutinize the sender's email address. This finding is consistent with research that when receivers directly examine an embedded URL within a message, they can detect the false nature of that message (Berghel 2006). In future research, it would be useful for studies to evaluate how features of different *clarity* strategies, such as manipulating the sender's name as well as the domain name, shape Internet consumers' response to phishing attempts.

## Limitations

It is important to note our study's limitations. For example, one could cite our use of student subjects as a deficiency of our study: however, we believe it was appropriate for two reasons. First, students represent an important population of Internet consumers who are subject to phishing attempts. Our students routinely report receiving phishing emails on professional, personal, and school-related email accounts. Second, using a student population strengthened our experiment's internal validity. We were able to ensure our subjects received similar training as well as possessed similar information. Because of our control over these factors, we were able to conduct a more rigorous test of phishing tactics' efficacy.

We attempted to limit recall bias by explaining the motivation of the study only after we recorded the recall of their thought process when the message was received. It is our hope this this may somewhat limit recall bias that is introduced using this methodology. Although controlling for recall bias using this debriefing method is common in clinical psychology (e.g., controlling for recall bias in food intake; Friedenreich et al. 1991) there is limited use or understanding in the extant information systems literature. We therefore followed clinical psychology, which found that asking subjects prospectively and retrospective created no systematic different and there was little evidence of recall bias.

Also, we did not actually test whether central or peripheral processing centers in the brain were activated by our phishing attack. ELM provides a conceptual understanding of how phishing tactics work. We assessed central or peripheral processing through assessing respondents responses to open ended questions. To more rigorously assess cognitive processing, future research may wish to employ two additional tests. First, to evaluate processing, a research design could requires subjects to execute memory tests while processing deception emails. By manipulating attention and working memory, researchers may glean insights into the black box of cognitive mechanisms (Sip et al. 2008). Second it is possible to use fMRI measurement to investigate the centers of the brain engaged by deceptive phishing tactics (Abe et al. 2007; Grèzes et al. 2005; Grèzes et al. 2004; Hughes et al. 2005).

## Contributions

For research, this study offers several important contributions. First, this study extends the e-commerce deception theoretical model for describing Internet consumers' cognitive processes that render consumers susceptible to phishing. Our study offers an explanation for why phishing emails lead to deceiving Internet consumers. By doing so, our study contributes to the framework for future research that examines how and whether central or peripheral processing influences the efficacy of phishing attempts. Through adding ELM to the deception framework, we offer a means to understand, and empirically test, the role of cognitive mechanisms within the deception detection process.

Second, our study introduces a unique dependent variable to the deception detection literature. In prior work on deceptive communication, research focused on whether individuals could detect cues (Forrest et al. 2000; Reinhard et al. 2008) and whether ones behavioral profile affected intention to answer phishing email (Wright et al. 2010a; Wright et al. 2010b). In this study, we move beyond detecting deception to evaluating which phishing deception tactics shape actual behavior (i.e., distracting the receiver's attention to the point of being outright deceived). By doing so, we now have evidence within an online deception practice that the types of manipulations do impact deception outcomes. This extends the seminal work of Johnson et al. (Johnson et al. 1993; Johnson et al. 2001) and Buller, Burgoon et al. (Buller et al. 1996a; Buller et al. 1996b; Burgoon et al. 2008; Burgoon et al. 2004; Burgoon et al. 1996) to an online context.

For practice, this study offers implications for communication processing and information security. First, email provides functions for users that are not associated with other communication modalities, including task organization, personal archiving, and ubiquitous contact management (Whittaker et al. 2006). Internet users spend copious amounts of time and effort managing email functions, in addition to that which is necessary for dealing with an overloaded inbox (Bellotti et al. 2005). It should come as no surprise, then, if users appraise incoming messages with the less-intensive peripheral route than with central route processing. As this study indicates, Internet consumers can be fooled by phishing regardless of the detection mechanism. While we cannot say that the deception detection mechanism did not work for some subjects, we found no evidence that specific email phishing detection systems are effective.

Second, managers should offer opportunities for their employees to increase awareness of personal information security management (e.g., activate the central processing route). Indeed, research indicates that a significant portion of email security breaches are the result of users' naiveté about possible vulnerabilities and the users' own roles in maintaining security (Stanton et al. 2005). Recent work has demonstrated that user training programs and monitoring can be effective for improving user knowledge and compliance with security policies (D'Arcy et al. 2009), and similar training efforts are likely to be the best weapon in encouraging users to proceed with caution with regard to email. Central route processing is contingent upon an individual's level of motivation, so managers should seek opportunities to make users aware of the stakes involved and to motivate users to disseminate information judiciously.

## Conclusion

This research article set out to deepen understanding of why phishing emails lure unwary Internet consumers into sharing sensitive information. Where many studies have focused on the phisher's website, we examined the tactics manifest in the content of email messages. To explain why Internet consumers share sensitive information, we turned to the stimulus and deception detection process to understand the outcome. Overall, we found that the e-mail's content as well as Internet consumers' cognitive processing techniques influenced the effectiveness of Phishing tactics.

## References

Abe, N., Suzuki, M., Mori, E., Itoh, M., and Fujii, T. 2007. "Deceiving Others: Distinct Neural Responses of the Prefrontal Cortex and Amygdala in Simple Fabrication and Deception with Social Interactions," *Journal of Cognitive Neuroscience* (19:2), pp. 287-295.

Anti-Phishing Working Group. 2013. Phishing Activity Trends Report: Global Phishing. Retrieved January 8, 2014, at www.antiphishing.org.

Areni, C. S. 2003. "The Effects of Structural and Grammatical Variables on Persuasion: An Elaboration Likelihood Model Perspective," *Psychology & Marketing* (20:4), pp. 349-375.

Bellotti, V., Ducheneaut, N., Howard, M., Smith, I., and Grinter, R. 2005. "Quality Versus Quantity: E-mail-centric Task Management and its Relation with Overload," *Human-Computer Interaction* (20:1), pp. 89-138.

Berghel, H. 2006. "Phishing mongers and posers," *Communications of ACM* (49:4), pp. 21-25.

Bhattacherjee, A., and Sanford, C. 2006. "Influence Processes for Information Technology Acceptance: an Elaboration Likelihood Model," *MIS Quarterly* (30:4), pp. 805-825.

Biros, D., George, J., and Zmud, R. 2002. "Inducing sensitivity to deception in order to improve decision making performance: A field study," *MIS Quarterly* (26:2), pp. 119-144.

Bitner, M., and Obermiller, C. 1985. "The Elaboration Likelihood Model: Limitations and extensions in marketing.," *Advances in Consumer Research* (12), pp. 420-425.

Bjorhus, J. 2014. Target Breach Started as an E-mail Phishing Expedition. Retrieved April 22, 2014, at http://www.startribune.com/business/245226831.html

Buller, D., Burgoon, J., Buslig, A., and Roiger, J. 1996a. "Testing interpersonal deception theory: The language of interpersonal deception," *Communication Theory* (6:3), pp. 268-289.

Buller, D., and Burgoon, J. K. 1996b. "Interpersonal deception theory," *Communication Theory* (6:3), pp. 203-242.

Burgoon, J., Blair, J. P., and Strom, R. 2008. "Cognitive biases and nonverbal cue availability in detecting deception.," *Human Communication Research* (34:4), pp. 572-599.

Burgoon, J., Bonito, J., and Kam, K. 2004. "Communication and Trust Under Face-to-Face and Mediated Conditions: Implications for Leading from a Distance," in *Leadership at a Distance,* S. Weisband and L. Atwater (eds.), LEA: Mahweh, NJ.

Burgoon, J., Buller, D., Ebesu, A., and Rockwell, P. 1994. "Interpersonal deception: V. accuracy in deception detection," *Communication Monographs* (61), pp. 303-325.

Burgoon, J., Buller, D., Ebesu, A., White, C., and Rockwell, P. 1996. "Testing interpersonal deception theory: Effects of suspicion on communication behaviors and perceptions," *Communication Theory* (6:3), pp. 243-267.

Cook, T. D., and Campbell, D. T. 1979. "Quasi-Experiments: Interrupted Time-Series Designs," in *Quasi_Experimentation: Design & Analysis for Field Studies*, Houghton Mifflin Company, p. .

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* (20:1), pp. 79-98.

Dennis, A. R., Fuller, R. M., and Valacich, J. S. 2008. "Media, Tasks, and Communication Processes: a Theory of Media Synchronicity," *MIS Quarterly* (32:3), pp. 575-600.

Denzin, N. K., and Lincoln, Y. S. 2003. *Strategies of Qualitative Inquiry*, (Sage: London.

DePaulo, B., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., and Cooper, H. 2003. "Cues to Deception," *Psychological Bulletin* (129:1), pp. 74-118.

Dhamija, R., Tygar, J. D., and Hearst, M. Year. "Why Phishing Works," Computer Human Interaction Conference Montreal, QB, Canada, 2006, pp. 581-590

Downs, J. S., Holbrook, M. B., and Cranor, L. F. 2006. "Decision strategies and susceptibility to phishing," in *Proceedings of the second symposium on Usable privacy and security*, ACM: Pittsburgh, Pennsylvania, pp. 79-90.

Ekman, P., O'Sullivan, M., Friesen, W., and Scherer, K. 1991. "Face, Voice, and Body in Detecting Deceit," *Journal of Nonverbal Behavior* (15:2), pp. 125-135.

Feigenson, N. 2006. "Too Real? The Future of Virtual Reality Evidence," *Law & Policy* (28:2), pp. 271-293.

Fette, I., Sadeh, N., and Tomasic, A. Year. "Learning to Detect Phishing Emails," WWW Conference, ACM, Banff, Canada, 2007.

Finn, P., and Jakobsson, M. 2008. "Designing and conducting phishing experiments," *IEEE Technology and Society* (6:2), pp. 66-68.

Forrest, J., and Feldman, R. 2000. "Detecting deception and judge's involvement: Lower task involvement leads to better lie detection," *Personality and Social Psychology Bulletin* (26:1), pp. 118-125.

Friedenreich, C. M., Howe, G. R., and Miller, A. B. 1991. "An investigation of recall bias in the reporting of past food intake among breast cancer cases and controls," *Annals of Epidemiology* (1:5) 8//, pp. 439-453.

Fu, A. Y., Wenyin, L., and Deng, X. T. 2006. "Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD)," *IEEE Transactions on Dependable and Secure Computing* (3:4), pp. 301-311.

Grazioli, S., and Jarvenpaa, S. 2003a. "Consumer and business deception on the Internet: Content analysis of documentary evidence," *International Journal of Electronic Commerce* (7:4), pp. 93-118.

Grazioli, S., and Jarvenpaa, S. L. 2003b. "Deceived: Under Target Online," *Communications of the ACM* (46:12), pp. 195- 206.

Grèzes, J., Berthoz, S., and Passingham, R. E. 2005. "Amygdala activation when one is the target of deceit: Did he lie to you or to someone else? ," *NeuroImage* (30:2), pp. 601-608.

Grèzes, J., Frith, C., and Passingham, R. E. 2004. "Brain Mechanisms for Inferring Deceit in the Actions of Others," *The Journal of Neuroscience* (24:24), pp. 5500-5505.

Hughes, C., Farrow, T. F. D., Hopwood, M.-C., Pratt, A., Hunter, M. D., and Spence, S. A. 2005. "Recent Developments in Deception Research " *Current Psychiatry Reviews* (1:3), pp. 273-279.

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

Jakobsson, M. 2007. "The human factor in phishing," *Privacy & Security of Consumer Information* (7), pp. 1-19.

Jingguo, W., Herath, T., Rui, C., Vishwanath, A., and Rao, H. R. 2012. "Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email," *Professional Communication, IEEE Transactions on* (55:4), pp. 345-362.

Johnson, P., Grazioli, S., and Jamal, K. 1993. "Fraud detection: Intentionality and deception in cognition," *Accounting, Organizations and Society* (18:5), pp. 467-488.

Johnson, P. E., Grazioli, S., Jamal, K., and Berryman, R. G. 2001. "Detecting deception: adversarial problem solving in a low base-rate world," *Cognitive Science* (25), pp. 355-392.

Karmarkar, U. R., and Tormala, Z. L. 2009. "Believe Me, I Have No Idea What I'm Talking About: The Effects of Source Certainty on Consumer Involvement and Persuasion," *Journal of Consumer Research* (36:6), pp. 1033-1049.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., and Nunge, E. Year. "Protecting People from Phishing: The Design and Evalaution of an Embedded Training Email Systems," Computer Human Interaction (CHI), ACM Press, San Jose, CA, 2007a.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., and Hong, J. 2007b. "Getting users to pay attention to anti-phishing education: evaluation of retention and transfer," in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, ACM: Pittsburgh, Pennsylvania, pp. 70-81.

Landis, J. R., and Koch, G. G. 1977. "The measurement of observer agreement for categorical data," *Biometrics* (33), pp. 159-174.

Levine, T., Park, H. S., and McCornack, S. 1999. "Accuracy in detecting truths and lies: Documenting the 'veracity effect'," *Communication Monographs* (66), pp. 125-144.

Liu, W., Deng, X., Huang, G., and Fu, A. Y. 2006. "An antiphishing strategy based on visual similarity assessment," *IEEE Internet Computing* (10:2), pp. 58-65.

McCornack, S. A. (1992). Information manipulation theory. *Communications Monographs*, *59*(1), 1-16.

McCornack, S., and Levine, T. 1992. "When lovers become leery: The relationship between suspicion and accuracy in detecting deception," *Communication Monographs* (57), pp. 219-230.

Mertler, C., and Vannatta, R. 2001. *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*, (Pyrczak Publishing: Los Angeles, CA.

Miller, G. R., and Stiff, J. B. 1993. *Deceptive Communication*, (Sage Publications: London.

Mitnick, K. D., and Simon, W. 2005. *The Art of Intrusion*, (Wiley Publishing, Inc.: Indianapolis, ID.

Mohebzada, J. G., El Zarka, A., Bhojani, A. H., and Darwish, A. Year. "Phishing in a university community: Two large scale phishing experiments," Innovations in Information Technology (IIT), 2012 International Conference on2012, pp. 249-254.

Mondak, J. 1993. "Public opinion and heuristic processing of source cues," *Political Behavior* (15:2), pp. 167-192.

Nah, F. F.-H., and Benbasat, I. 2004. "Knowledge-based Support in a Group Decision Making Context: An Expert-Novice Comparison," *Journal of the Association for Information Systems* (5:3), pp. 125-150.

Nan, X. 2009. "The Influence of Source Credibility on Attitude Certainty: Exploring the Moderating Effects of Timing of Source Identification and Individual Need for Cognition," *Psychology & Marketing* (26:4), pp. 321-332.

Park, H. S., and Levine, T. R. 2001. "A probability model of accuracy in deception detection experiments.," *Communication Monographs* (68), pp. 201-210.

Pedhazur, E. J., and Schmelkin, L. P. 1991. *Measurement, Design and Analysis: An Integrated Approach*, (Lawrence Erlbaum Associates: Hillsdale, NJ.

Petty, R. E., and Cacioppo, J. T. (eds.) *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. Springer-Verlag, New York, 1986.

Petty, R. E., Cacioppo, J. T., and Goldman, R. 1981. "Personal Involvement as a Determinant of Argument-Based Persuasion," *Journal of Personality and Social Psychology* (41:5), pp. 847-855.

Petty, R. E., and Wegener, D. T. 1999. "The Elaboration Likelihood Model: Current Status and Controversie," in *Dual Process Theories in Social Psychology,* S. Chaiken and Y.Trope (eds.), Guilford Press: New York, pp. 41–72.

Purkait, S. 2012. "Phishing counter measures and their effectiveness – Literature review. ," *Information Management & Computer Security* (20:5), pp. 382-420.

Rao, S., and Lim, J. Year. "The Impact of Involuntary Cues on Media Effects," 33rd Hawaii International Conference of System Science,, IEEE, The Big Island, 2000.

Reinhard, M., and Sporer, S. 2008. "Verbal and nonverbal behavior as a basis for credibility attribution: The impact of task involvement and cognitive capacity," *Journal of Experimental Social Psychology* (44:3), pp. 477-488.

Riquelme, H., and Kegeng, W. 2004. "The unintended effects of hidden assumptions: Biases on the Internet. ," *Online Information Review* (28:6), pp. 444-453.

RSA Security 2008. "Protecting against phishing by implementing strong two-factor authentication."

Schwartz, M. J. 2011. Spear Phishing Attacks on the Rise. Retrieved June 8, 2011, at http://www.informationweek.com/news/security/attacks/230500025.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010. "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the 28th international conference on Human factors in computing systems*, ACM: Atlanta, Georgia, USA, pp. 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. Year. "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," Symposium On Usable Privacy and Security (SOUPS), ACM Press, Pittsburgh, PA, 2007.

Sip, K. E., Roepstorff, A., McGregor, W., and Frith, C. D. 2008. "Detecting deception: the scope and limits," *Trends in Cognitive Sciences* (12:2), pp. 48-53.

Stanton, J., Stam, K., Mastrangelo, P., and Jolton, J. 2005. "Analysis of end user security behaviors," *Computers & Security* (24:2), pp. 124-133.

Symantec. 2014. Internet Security Threat Report 2014. Volume 189. Retrieved April 22, 2014, at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Tam, K. Y., and Ho, S. Y. 2005. "Web Personalization as a Persuasion Strategy: An Elaboration Likelihood Model Perspective," *Information Systems Research* (16:3) September 2005, pp. 271-291.

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

Warden, C. A., Wann-Yih, W., and Dungchun, T. 2006. "Online Shopping Interface Components: Relative Importance as Peripheral and Central Cues," *CyberPsychology & Behavior* (9:3), pp. 285-296.

Werner, C. M., Stoll, R., Birch, P., and White, F. H. 2002. "Clinical Validation and Cognitive Elaboration: Signs That Encourage Sustained Recycling," *Basic & Applied Social Psychology* (24:3), pp. 185-203.

Whittaker, S., Bellotti, V., and Gwizdka, J. 2006. "Email in personal information management," *Communications of the ACM* (49:1), pp. 68-73.

Wright, R., Chakraborty, S., Basoglu, A., and Marett, K. 2010a. "Where did they go right? Investigating deception cues in a phishing context," *Group Decision and Negotiation* (19:4), pp. 391-416.

Wright, R., and Marett, K. 2010b. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273-303.

Wright, R. T., Jensen, M. J., Thatcher, J. B., Dinger, M., and Marett, K. Forthcoming. "Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (Forthcoming).

Xiao, B., and Benbasat, I. 2011. "Product-Related Deception in E-Commerce: A Theoretical Perspective," *MIS Quarterly* (35:1), pp. 169-195.

Zhou, L., Burgoon, J. K., Twitchell, D. P., Qin, T., and Nunamaker, J. 2004. "A Comparison of classification methods for predicting deception in computer-mediated communication," *Journal of Management Information Systems* (20:4), pp. 139-166.