Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, December 2012, vol. 17, no.3
(http://www.arraydev.com/commerce/jibc/)

Victimized by Phishing: A Heuristic-Systematic Perspective

ZHENGCHUAN XU
Associate Professor, School of Management, Fudan University
Postal Address: **Zhengchuan Xu, Room 708, Siyuan Building, School of Management, Fudan University, shanghai, 200433, P.R.China**
Author's Organizational Website:
http://www.fdsm.fudan.edu.cn/teacher/preview.aspx?UID=16134
Email: **zcxu@fudan.edu.cn**
Dr. Zhengchuan XU earned his doctorate in computer sciences from Fudan University. His research interests include Information Security, mobile commerce, and Cultural and Cross-cultural Issues in IS. Dr. XU has published in journals such as European Journal of Information Systems, International Journal of Mobile Communication, and Communications of ACM.

WEI ZHANG *
Associate Professor, College of Management, UMass Boston
Postal Address: **Wei Zhang, UMass Boston, College of Management, 100 Morrissey Blvd., Boston, MA 0215, U.S.A.**
Author's Organizational Website:
http://www.umb.edu/academics/cm/faculty_staff/faculty/wei_zhang
Email: **wei.zhang@umb.edu**
Dr. Wei Zhang earned his doctorate in management information systems from Boston University. His research interests include Knowledge Management, Information Security, and Cultural and Cross-cultural Issues in IS. Dr. Zhang has published in journals such as Journal of Association for Information Systems, Social Work, and Communications of the Association for Information Systems.

* Corresponding author.

§ This research is supported by National Natural Science Foundation of China (71272076, 70972048).

Abstract

Phishing has become an ever-present, ever-increasing threat to information security, yet theory-based, systematic research on the behavioral aspect of this phenomenon is rather limited. In this paper, we propose the Heuristic-Systematic Model (HSM) as an overarching theory to solidify the theory base for this line of research. We note the theoretical synergy between HSM and other theories used in previous research, and illustrate how HSM can be used to develop a research model investigating the psychological mechanism underlying the effectiveness of phishing attacks.

Keywords: **Phishing, Information Security, Heuristic-Systematic Model, Victimization**

INTRODUCTION

The last two decades witnessed the dramatic advances in information and communication technologies that lead to easier, quicker, and more convenient access to information and, in particular, funds in electronic forms. Unfortunately, the ever-expanding Internet and communication networks have facilitated reaching not only regular businesses and their consumers but also users with malicious intentions, exposing valuable digital assets to potential criminals. Consequently, safeguarding the digital information and funds is becoming increasingly important to business survival and success in today's highly competitive marketplace.

One of the grave threats to digital assets is phishing. Phishing is an attempt to trick victims into giving away sensitive information (Furnell, 2007; Mitnick & Simon, 2002). While phishing in older days relied on carefully designed and executed schemas (Mitnick & Simon, 2002), nowadays phishing offenders often broadcast manipulative messages – through emails (Vishwanath, Herath, Chen, Wang, & Rao, 2011), instant messages (ComputerWeekly.com, 2009), or short messages (Fang, 2011) – to a large population. In these messages, phishers masquerade as credible businesses (American Express, eBay …) or government institutions (Internal Revenue Service, Registry of Motor Vehicles, …), leverage current events (political donations, Olympic tickets, aiding victims of natural disasters, …), and often incorporate languages invoking powerful emotions such as sympathy, fear, excitement, or urgency to coax people into responding (Wang, Chen, Herath, & Rao, 2009). Victims are usually caught off-guard at first glance and fail to verify the authenticity of the messages they receive. For example, in a widely reported case in China, phishers simply sent out text messages, instructing unsuspecting victims to provide their account information through a website resembling a well-known online banking portal (Fang, 2011).

Such seemingly simple deceptions proved to be surprisingly effective and led to enormous losses for the victimized individuals and organizations. Phishing has become an ever-present, ever-growing threat to online information security.

Figures from Symantec suggested an 81% rise in the first half of 2006, with more than 157,000 unique phishing messages being sent during this period (Symantec, 2006). Between 2010 and 2011, phishing activity level rises from 1 in 442.1 to 1 in 298 of all emails (Symantec, 2011). Although it is difficult to accurately measure the financial loss caused by phishing, it was estimated that phishing attacks cost business organizations and individual consumers billions of dollars (Bose & Leung, 2007; Geer, 2005).

To combat phishing attacks, a number of technical solutions have been developed, many focusing on automatic phishing detection (Dong, Clark, & Jacob, 2008). For example, most popular browsers today (e.g., Firefox, Internet Explorer) have phishing detection functions built-in, usually based on white- and black-listed websites. However, phishers evolve too. They keep improving their baiting techniques to match the advancements in detection technologies. More fundamentally, technology alone does not provide adequate protections as phishing attacks are designed to exploit human cognitive biases instead of technology loopholes (Mitnick & Simon, 2002). As such, psychological and behavioral factors play a more important role in how phishing works. However, research efforts in systematically identifying, describing, and analyzing the psychological and behavioral factors are rather limited other than a few notable exceptions (e.g. Vishwanath, et al., 2011; Wright & Marett, 2010).

This paper endeavors to solidify the theoretical base on which future research can be built to bridge the gap and to advance this line of research in the information security arena. We propose Heuristic-Systematic Model (HSM) – a mature and fruitful social psychology theory (Sheely Chaiken & Trope, 1999) – as an overarching theoretic framework to study phishing, especially victimization by phishing. HSM was first proposed in early 1980s. Over the years, HSM has evolved into a mature theory in social psychology, and has been widely used in research involving various validity-seeking contexts (Shelly Chaiken, Liberman, & Eagly, 1989). In this paper, we demonstrate the theoretical synergies between HSM and other theories that have been used in phishing studies. We also show how HSM can help to identify and organize human factors and psychological mechanisms associated with victimization by phishing.

We begin with a review of existing research on phishing. We then introduce the heuristic-systematic model and demonstrate why it is a good theoretic choice to phishing victimization research. To illustrate how HSM can be applied to studying phishing, we develop a preliminary research model on phishing victimization, followed by a brief suggestion on research method. A discussion on potential contributions concludes the paper.

LITERATURE REVIEW

As a social engineering technique, phishing is designed to exploit more human weaknesses than technical inferiority of targets (Mitnick & Simon, 2002). It attempts to take advantage of “the natural helpfulness of human users, their psychological weaknesses, and their tendencies to be unaware of the value of the information they possess and to be sloppy about shielding their information (Luo, Brody, Seazzu, & Burd, 2011, p1).” Most phishing attacks involve a message that appears to originate from a legitimate business such as a bank, a credit card company, or an authoritative department such as technical support or government agencies. In the message, the attackers try to coax the targets into taking certain actions that would compromise the targets' information security either immediately (e.g., giving out usernames and passwords over phishing web sites) or eventually (e.g., planting malwares into targets' computers to steal credentials or intercept usernames and passwords to online accounts) (APWG, 2010).

Drawing on the work of Allen (2006), Luo et al (2011) proposed a four-step model to describe how social engineering attacks are deployed (Figure 1). In this model, the attackers would first collect information on the targets that they then use to develop rapport with the targets and gain their trust. Once the trust is established, the attackers lure the targets to divulge sensitive information that will be used to execute the final attacks.

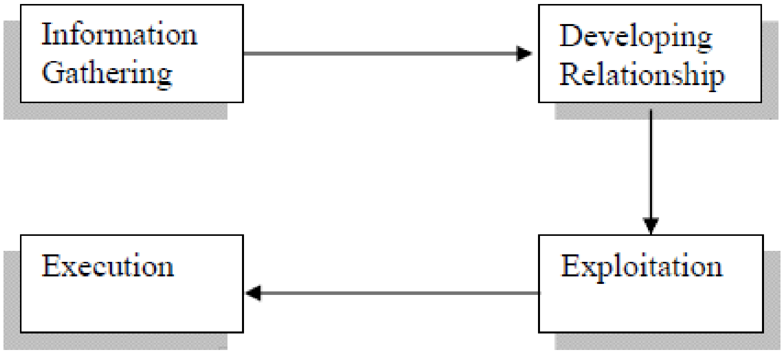

Figure 1: Four-step Social Engineering Attack (from Luo, et al., 2011)

Using this model, we can see how phishing deviates from other typical social engineering techniques. Todays' phishing attacks usually involve little information gathering and relationship developing, as most attacks now deliver the masqueraded messages through spamming to a large number of potential victims. The interactions between attackers and targets are rather limited to the exploitation stage when targets process the received messages (Vishwanath, et al., 2011). To maximize the chance of success, attackers utilize multiple strategies in their messages to cajole victims into actions (Workman, 2007). More interestingly, anecdotal evidences suggest that while the validities of the messages may not be difficult to disprove on a second thought, victims are often caught off-guard at first glance (Yi, 2011).

While phishing has received some research attention in recent years, theory-based, systematic studies are still rare. Two leading theoretical bases seem to emerge from limited studies so far. First, researchers appear to agree that much of effectiveness of phishing lies in that victims infer the validity of the manipulative messages not by mulling over the information content of the messages but relying on the cues around the messages such as source credibility and likeability (Workman, 2007), spelling, message design, and third party endorsement (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007). Such reliance on the cues has led researchers to Elaboration Likelihood Model (ELM) as a theoretic base for studying phishing (Vishwanath, et al., 2011; Workman, 2008b).

Elaboration Likelihood Model (Petty & Cacioppo, 1986) is a popular dual-process theory of information processing on persuasion (Sheely Chaiken & Trope, 1999).

Persuasion research studies how received messages can change people's attitudes. The gist of the dual-process theories holds that when being persuaded, people must first establish the validity of the received message. When doing so, in addition to the information content of the messages, people also consider the factors surrounding the messages (Gilbert, 1999). In ELM, persuasion through information content is considered the *central route*: people elaborate on the message and carefully and thoughtfully assess the validity of the information content of the message (Petty & Cacioppo, 1986, chapter 1). Any persuasion that does not elaborate on the message takes the *peripheral route* (Eagly & Chaiken, 1993). Typically, peripheral routes take advantage of the peripheral cues surrounding the message – such as source credibility and message length – to infer the validity of the message (Petty & Cacioppo, 1986). For example, people tend to believe that longer messages are more likely to be valid.

According to ELM, the extent of elaboration, i.e., issue-relevant thinking, is situated in the surrounding context. ELM uses the term *elaboration likelihood* to capture the probability of people taking the central route and the extent of elaboration (Petty & Cacioppo, 1986, p.7). The higher the information recipient's elaboration likelihood, the more likely he or she is to take the central route, and the more extensive elaboration is. Several factors are known to affect elaboration likelihood, including personality traits such as needs for cognition and contextual variables such as recipient expertise and recipient involvement (Petty & Cacioppo, 1986, Chapter 4). These factors work in two ways: by affecting one's motivation to engage in elaboration and/or by affecting one's ability to engage in elaboration.

When applied to phishing, ELM provides the theoretical tool that can describe and explain the situated roles played by various factors. Workman (2008a) effectively argued that personality traits such as normative commitment and disposition to trust may be related to phishing susceptibility because they reduce the elaboration likelihood. Vishwanath et al. (2011) showed that message source, composition elements, and message urgency served as peripheral cues when affecting phishing susceptibility, and peripheral processing was the dominant processing mode leading to phishing victimization.

Second, due to the deceptive nature of phishing attacks, phishing research also incorporated deception theories, most notably interpersonal deception theory and theory of deception (Vishwanath, et al., 2011). From the targeted victims' perspective, interpersonal deception theory (IDT) describes how deceptions can be detected by attending to the verbal and nonverbal cues that are telltales of deceptions (Griffin, 2006). IDT emphasizes the interactive nature of the interpersonal communication and continuing adjustment to targets' suspicions by deceivers (Buller, Burgoon, & Burgeon, 1996). While this emphasis may make IDT a great theoretical choice to study social engineering in general, it also limits its applicability to studying phishing attacks that are largely non-interactive.

Like IDT, the theory of deception makes notice of the cues that can reveal deception (Paul E. Johnson, Grazioli, Jamal, & Berryman, 2001; P.E. Johnson, Grazioli, Jamal, & Zualkernan, 1992). According to this theory, deception detection involves four distinct stages (Paul E. Johnson, et al., 2001): activation, hypothesis generation, hypothesis evaluation, and global assessment. During activation, possible cues suggesting discrepancies are noticed and suspicions are raised. Possible explanations to the discrepancies are proposed in the hypothesis generation stage and subsequently evaluated. Finally, all evaluated explanations are gauged and results are synthesized to reach a global assessment on whether a deception is detected.

Thus deception detection is inherently about information processing too (Grazioli, 2004). It focuses on "intentional deceptions characterized by relatively low interpersonality and interactivity (Grazioli, 2004, p151)," and was used to study internet consumer deceptions (Grazioli, 2004). Vishwanath *et al* (2011) also incorporated it into studying phishing attacks (Vishwanath, et al., 2011).

HEURISTIC-SYSTEMATIC MODEL

In this paper, we propose to use Heuristic-Systematic Model (HSM) as a primary theory base for studying phishing. Like ELM, HSM is also a dual-process theory of information processing (Sheely Chaiken & Trope, 1999) originated from persuasion research in social psychology. The dual-process in HSM involves two information processing modes: *systematic processing* carefully elaborate on the information content of the received message and *heuristic processing* takes advantage of the factors surrounding the messages – called heuristic cues in HSM – and uses associated heuristics to quickly make a validity assessment.

In HSM, both information processing modes can lead to decisions on the validity of received messages, but neither is automatic. HSM argues that systematic processing is more effortful and takes more cognitive resources such as time and energy than heuristic processing. Hence message recipient must be both motivated to initialize and capable of engaging in systematic processing. Systematic processing will be limited if a message recipient is not motivated to elaborate on the message, is not capable of making sense of the message, or does not have enough cognitive resource to adequately process the message. In fact, it may be more difficult for systematic processing to occur in real life than in laboratory research settings (Shelly Chaiken, et al., 1989).

On the other side, heuristic processing depends on the availability of cues and awareness of the heuristics associated with these cues. If a cue is not noticed by the message recipients, or if the message recipients are not aware of the implications of the cue, they cannot process the content heuristically. When conditions for both systematic and heuristic processing are met, HSM contends that both processing modes can and do occur concurrently. However, because extensive systematic processing "provides people with more judgment-relevant information" (Eagly & Chaiken, 1993, p328), high levels of systematic processing can *attenuate* the effects of heuristic processing, so much so that the validity assessment resulted from heuristic processing can be overturned (Shelly Chaiken, 1980).

Such attenuation effects were observed and confirmed in early studies of HSM (e.g. Shelly Chaiken, 1980). However, as researchers have since argued (Shelly Chaiken, et al., 1989), these results could be artificial because of the experimental manipulations that pitted contradictory heuristic cues against message content in experimental settings (e.g., using a message with weak content from a credible source).

When heuristic cues and message content are congruent with each other, dual-processing tends to generate consistent outcomes. Under such circumstances, heuristic processing may exert influence during message validity assessment over and above the influence of systematic processing, a phenomenon called *additive* effect in HSM (Maheswaran & Chaiken, 1991).

The notion of additive effects leads to the theoretical uniqueness of HSM among the dual-process theories family in the concept of *sufficiency threshold*. Sufficiency threshold refers to the "desired judgmental confidence" that people wish to reach when making decisions under a given circumstance (Eagly & Chaiken, 1993, p330). HSM argues that when message recipients engage in validity assessment, the level of their confidence in their assessment must reach or surpass sufficiency threshold for them to be comfortable with their judgment. They will continue processing the message as much as possible until the sufficiency threshold is attained or they will have to settle for a lower confidence level in their conclusions. Therefore, when heuristic processing alone cannot lead the message recipients to achieve the sufficiency threshold, it is likely that they will invoke systematic processing, even though it is more effortful and demands more cognitive resource (Shelly Chaiken, et al., 1989).

Although HSM and ELM have some commonalities, we prefer HSM to ELM for studying phishing victimization for two theoretical reasons. First, compared with peripheral route in ELM, HSM is more advanced about the heuristic processing (Eagly & Chaiken, 1993). ELM simply refers all persuasion without using central route as going through peripheral route. In comparison, HSM examines in details when and how heuristic cues can play a role. Given the reliance of phishing attacks on peripheral route/heuristic processing, HSM's more developed view of heuristic processing is better suited for studying phishing than ELM's view of peripheral route. Second, theoretical extensions such as additive effect and sufficiency threshold made HSM applicable to a wider range of validity-seeking contexts than ELM (Shelly Chaiken, et al., 1989). We demonstrate this further below as we propose our research framework for studying phishing victimization, explicitly incorporating sufficiency threshold into a proposed research model.

We also note the theoretical synergy between HSM and the theory of deception in the context of phishing. The four-stage deception detection model in which discrepancies are noticed, suspicion raised, more evidences sought, and more processing entailed could be explained through the lens of HSM as following: the presence of incongruent cues raises sufficiency threshold (activation), which leads the message recipient to increase the level of systematic processing (hypothesis generation and evaluation) (Maheswaran & Chaiken, 1991). In the context of phishing study, the phishing message is inherently invalid, thus a high level of systematic processing will likely dominate heuristic processing, leading to the correct identification of the phishing message (global assessment).

According to HSM, a factor affects persuasion effects in one or more of the following ways: 1) through heuristic processing; 2) through systematic processing; 3) through affecting the interactions between heuristic processing and systematic processing, and 4) through affecting sufficiency threshold. The nature of phishing attacks is to mislead message recipients into making an incorrect assessment of the validity of false messages.

Thus from HSM's perspective, the success of phishing attack depends on whether the attacker can 1) take advantage of deceptive heuristic cues, 2) provide a message that can stand systematic processing, 3) promote heuristic processing and/or suppressing systematic processing, and/or 4) reduce the sufficiency threshold so that the phishing messages won't be closely examined . In this sense, HSM provides an ideal theoretical framework to understand victimization by phishing.

THEORETICAL FRAMEWORK AND PROPOSITIONS

To illustrate how HSM can be employed to investigate phishing victimization, we build a preliminary research model with the factors identified under the guidance of HSM (Figure 2). We start with addressing the dual-processing of phishing messages by the targeted victims.

Dual Processes in Phishing

In previous HSM research, systematic processing has been assessed by examining the effect of the argument quality – "the strength or plausibility of persuasive argumentation" (Eagly & Chaiken, 1993, p325) – of the message on validity assessment. When systematic processing occurs, high quality arguments lead to favorable message assessment. In the research context of phishing attacks, the phishing messages are inherently false, but a more craftily composed message will be more deceptive and has a better chance surviving close examinations by message recipients. Hence in this study we refer argument quality to the deceptive strength of phishing messages.

Phishing messages of high level of argument quality are more deceptive, stand better to message recipients' systematic processing, and thus increase the likelihood that the targets be victimized. We propose:

Proposition 1: Message recipients will be more likely to be victimized by phishing messages with higher level of argument quality.

Heuristic processing depends on the heuristic cues that are readily available and popularly used. One heuristic cue that has been extensively studied (Sussman & Siegal, 2003; Zhang & Watts, 2008) and that phishing offenders particularly like to take advantage of is source credibility: phishing messages usually pretend to be from credible sources such as reputable businesses, authoritative departments, or even friends. The effectiveness of (false) source credibility has been repeatedly demonstrated in actual phishing attacks. Thus:

Proposition 2.1: Message recipients will be more likely to be victimized by phishing messages pretending to be from a source with higher level of source credibility.

Another heuristic cue that we propose to study in this study is genre conformity (Zhang & Watts 2003). Genres are "socially recognized types of communicative actions that are habitually enacted by members of a community to realize particular social purposes" (Orlikowski & Yates, 1994, p. 542). They serve as templates for communications (Orlikowski & Yates, 1994), and represent the association between communication formats and communication purposes (Yates, Orlikowski, & Okamura, 1999). As businesses communicate with their customers for certain purposes, over time certain communication patterns emerge, evolving into certain communication genres. .

Meanwhile, using the developed genre for certain communication helps to improve communication efficiency and effectiveness (Yates, et al., 1999). Today, communications between businesses and their customers are becoming increasingly electronic. Many businesses use templates when mass-communicating with customers. Such practices reinforce the development and use of electronic communication genres. Phishing offenders can abuse these genres by forging their messages to resemble legitimate messages (Workman, 2008b), biasing the recipients into believing the validity of the messages (Zhang & Watts 2003). In this study, we refer genre conformity to the extent to which the composition of a phishing message conforms to the relevant genre used by a legitimate message it attempts to mimic, and propose:

Proposition 2.2: Message recipients will be more likely to be victimized by phishing messages with higher level of genre conformity.

Interactions between Dual Processes in Phishing

Factors that can affect the extent of systematic processing and heuristic processing are typically modeled as moderators in research using dual-process theories. Such moderators include personality variables such as need for cognition (e.g. Cacioppo & Petty, 1982; Petty & Cacioppo, 1986) and contextual variables such as task importance or recipient involvement (e.g. Sussman & Siegal, 2003). In this study, we focus on one personality variable, need for cognition, and one contextual variable, pressure for immediate action, to illustrate how the extent of dual processes may be moderated.

Need for cognition refers to the intrinsic desire for a person to comprehend and structure environmental information. It captures individual differences in dispositions to engage in effortful cognitive activities. Previous research suggested that people with higher level of need for cognition are more likely to engage in systematic processing (Cacioppo & Petty, 1982; Petty & Cacioppo, 1986). Since phishing messages are inherently false, an increased level of systematic processing is more likely to reveal the fallacy of phishing messages, and thereby attenuate the effects of heuristic cues. Thus, messages recipients with higher level of need of cognition are less likely to be influenced by heuristic cues – source credibility and genre conformity in this study – and consequently less likely to be victimized. Thus we propose:

Proposition 3.1: Effect of source credibility on victimization will be less for message recipients with higher need for cognition than for those with lower need for cognition.

Proposition 3.2: Effect of genre conformity on victimization will be less for message recipients with higher need for cognition.

Proposition 3.3: Phishing Message recipients with higher need for cognition are less likely to be victimized.

Systematic processing demands cognitive resources such as time and energy. If message recipients are pressed to act quickly, systematic processing will be suppressed. Many phishing attacks attempt to exaggerate the urgency of the situation and press the message recipients into actions as quickly as possible, thus preventing them from engaging in an higher level of systematic processing. When this occurs, message recipients usually have to reply on heuristic processing, eventually manipulated by the phishing messages into make erroneous decisions.

Considering the increased reliance on heuristic processing under such circumstance, we posit,

Proposition 4.1: Phishing messages that impose time pressure increase the effect of source credibility.

Proposition 4.2: Phishing messages that impose time pressure increase the effect of genre conformity.

Proposition 4.3: Phishing message recipients are more likely to be victimized by phishing messages that impose time pressure increases.

Sufficiency Threshold and Phishing

Lastly, we explore how sufficiency threshold could play a role in phishing attacks. Pretexting is a commonly used technique in social engineering attacks, with which offenders use a pre-designed scenario to legitimize their interactions with potential victims, acquire their trust, reduce their suspicions, and eventually mislead them to damaging behaviors such as giving away sensitive information or performing actions that violate security policies (Mitnick & Simon, 2002).

From the HSM perspective, pretexting works because it lowers the sufficiency threshold of victims and avoids triggering systematic processing. In the context of phishing, pretexting may be difficult to design due to limited interactions between attackers and targeted victims, but it may simply be the result of coincidences. For example, a company may have experienced an email system failure just before their employees received phishing messages asking for their email account information. Thus pretexting in phishing, by design or not, can lower the sufficiency threshold of message recipients, and hence:

Proposition 5: Phishing attacks coupled with pretexting are more likely to victimize message recipients.

The effectiveness of phishing attacks depends on the effectiveness of heuristic cues in heuristic processing. Because of the inherently false nature of phishing messages, phishing attackers try their best not to trigger systematic processing as extensive systematic processing would reveal the fallacy in the messages. To maximize their effectiveness, phishing attackers always attempt to coordinate multiple cues (Vishwanath, et al., 2011). However, even in a craftily composed message, there can be incongruent cues. Such incongruent cues can raise the sufficiency threshold of message recipient, leading to a more thorough processing of the phishing message (Maheswaran & Chaiken, 1991). Examples of such incongruent cues include spelling and grammatical errors, inclusion of links in email, threats of disruptions in service, and use of company names that resemble well-known companies (Microsoft, 2012). Once recognized, they can potentially foil the best efforts of phishing attackers. Taking spelling errors as an example of incongruent cues, we propose:

Proposition 6: Phishing messages with spelling errors are less likely to victimize message recipients.

We present the proposed research framework graphically in Figure 2:

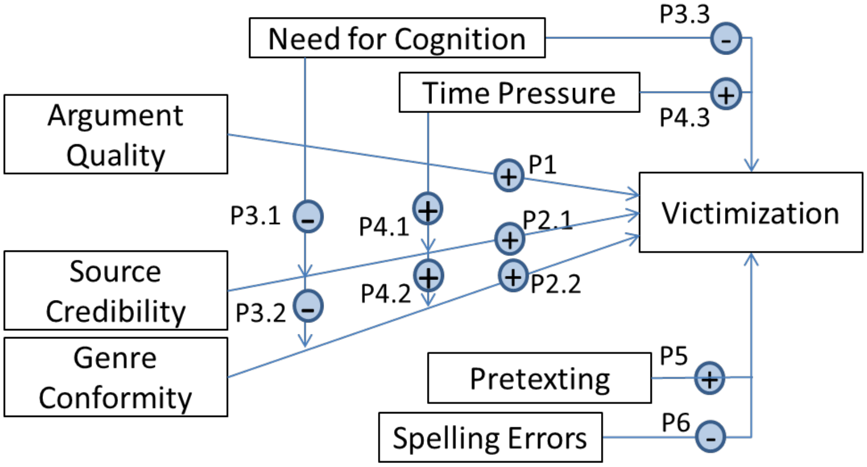

Figure 2: Proposed Research Framework

DISCUSSIONS

To the extent that phishing attacks have become a widespread threat to the security of digital assets, research in this area is still limited, hampered by a lack of behavioral perspective (Luo, et al., 2011) and weak theoretical foundation (Vishwanath, et al., 2011; Workman, 2008b). In this article we attempt to amend these limitations by proposing a mature theory from social psychology, the Heuristic-Systematic Model, as an effective theoretical foundation for future studies on phishing victimization. We argue that the core constructs included in HSM – heuristic processing, systematic processing, sufficiency threshold – and the mechanism in which HSM works – most notably attenuation effects and additive effects between heuristic processing and systematic processing – provide an ideal theoretical framework for us to understand phishing victimization. We also notice the synergy between HSM and other theories that have been used in previous studies in phishing.

To illustrate how HSM can be used for studying phishing, we build a prototype research model. The model identifies a few factors that can affect phishing victimization and explores how the factors work through the mechanisms as suggested by the HSM framework. The research framework, as presented in Figure 2, is admittedly preliminary. Nevertheless, it demonstrates how HSM can be used to help identify and organize factors that could work in phishing victimization and to explain how the identified factors work. In this sense, HSM can be the theoretical anchor for future phishing studies.

Based on HSM, two streams of future studies in phishing and phishing victimization are especially promising. First, HSM suggests that researchers pay particular attention to identifying new heuristic cues that can be exploited by phishing attackers. Previous research has focused on a rather limited set of heuristic cues, most noticeably source, composition, and urgency cues (Vishwanath, et al., 2011). A new cue, genre conformity, is included in the preliminary framework proposed in this article. However, given the important role heuristic cues play in phishing attacks and the proliferation of heuristic cues in electronic communications (Zhang & Watts, 2008), phishing attackers are likely to take advantage of other cues to attain the goal of victimization. It is of vital importance to identify these potentially harmful cues and investigate how they exactly work.

Second, as aforementioned, the success of phishing attack depends on whether the attacker can 1) take advantage of deceptive heuristic cues, 2) provide a message that can stand systematic processing, 3) promote heuristic processing and/or suppressing systematic processing, and/or 4) reduce the sufficiency threshold so that the phishing messages won't be closely examined. Thus HSM provides researchers with an effective framework to explaining how factors can lead to phishing victimizations. While the factors identified in the proposed model (Figure 2) are posited to work through one of the aforementioned ways, a single factor can work through multiple mechanisms. For example, in the proposed research model, we propose that time pressure works by promoting heuristic processing and suppressing systematic processing (propositions 4s). Other researchers have considered time pressure as a cue to elicit compliance from targeted victims (e.g. urgency cue in Vishwanath, et al., 2011). Clearly, HSM can be used to guide the design of future studies to clarify exactly how factors such as time pressure work in phishing.

While HSM provides a solid theoretical foundation for studies in phishing and phishing victimization, studies along this line of research can contribute significantly to HSM too. HSM was noted for its broad applicability in various valid-seeking contexts (Shelly Chaiken, et al., 1989), but most studies in HSM have been conducted under circumstance of positive persuasion. The current research context – phishing and phishing victimization – is inherently one of deception. It remains to be seen how well HSM works in this very different context. Applying HSM to phishing studies is thus much more than just testing HSM in yet another research context. It can push the boundaries of HSM in ways previous HSM research has not attempted.

We believe that this line of research can enrich HSM in several ways. First of all, further studies should and will identify and confirm new cues that can be exploited by phishing attackers, adding to the existing set of heuristic cues studied in previous research. Second, phishing provides a persuasion context where systematic processing and heuristic processing are inherently incongruent. Moreover, as phishing attackers try to exploit multiple cues simultaneously, the targeted victims may notice conflicting cues. Hence the interactions between the dual processing modes become more complicated and theoretically intriguing. What will happen to inconsistent cues? Will inconsistent heuristic cues lead to heuristic processing that cancel each other? Will the discovery of inconsistent cues itself serve as a cue that directly leads to the correct identification of phishing messages by targeted victims? Or must systematic processing be invoked to prevent phishing victimization at the presence of conflicting cues?

Thirdly, sufficiency threshold was hailed as one important theoretical advantage HSM enjoys over other dual-process models (Shelly Chaiken, et al., 1989), but few studies have explored this concept and its role in HSM (Maheswaran & Chaiken, 1991). Anecdotal evidences suggest that sufficiency threshold may play an important role in phishing victimization. We explicitly incorporate sufficiency threshold in the proposed research model (Proposition 5 and 6) and believe future studies along this line of exploration can lead to a better understanding of the role it plays in phishing particularly and in persuasion in general, thus contributing to HSM.

It is too early to speculate on the practical contributions that phishing studies guided by HSM can make against phishing attacks. Nevertheless, we are confident that insights generated from such studies can be of great practical value. We note that HSM not only identifies the influencing factors but also explains the mechanisms in which these factors work, thus making it possible to design counter-measures according to how each of the threating factors can work. Moreover, HSM research in disciplines such as marketing, advertising, communication, and information systems has successfully translated into actionable guidelines for practitioners, which bodes well for the practical implications of phishing studies guided by HSM.

CONCLUSION

To promote theoretically grounded research in phishing, we present in this article Heuristic-Systematic Model as an ideal theoretical foundation to guide and organize future research efforts in phishing. We offer a preliminary HSM-based research model to illustrate how HSM can be used for this purpose. We believe research along this line can not only inform phishing studies, but also advance HSM itself. Ultimately, we hope that the results from this line of research can pragmatically advise business decision-makers of how employees can deal with phishing attacks and social policy-makers of how public can recognize and circumvent phishing attacks.

REFERENCES

Allen, M. (2006). *Social engineering: A means to violate a computer system*: SANS Institute.

APWG. (2010). Phishing activity trends report, 2nd quartery 2010, from www.apwg.org

Bose, I., & Leung, A. C. M. (2007). Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *Communications of the AIS, 19*(24), 544–566.

Buller, D. B., Burgoon, J. K., & Burgeon, J. K. (1996). Interpersonal deception theory. [Article]. *Communication Theory, 6*(3), 203-242.

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*(1), 116-131. doi: 10.1037/0022-3514.42.1.116

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology, 39*(5), 752-766.

Chaiken, S., Liberman, A., & Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. In J. S. Uleman & J. A. Bargh (Eds.), *Unintended thought* (pp. 212-252). New York: Gilford Press.

Chaiken, S., & Trope, Y. (Eds.). (1999). *Dual-process theories in social psychology*. New York: The Guilford Press.

ComputerWeekly.com. (2009). Instant messaging phishing scam targets google gmail users Retrieved March 14, 2012, from http://www.computerweekly.com/news/2240088548/Instant-messaging-phishing-scam-targets-Google-Gmail-users

Dong, X., Clark, J. A., & Jacob, J. (2008). *User behavior-based phishing websites detection*. Paper presented at the International Multiconference on Computer Science and Information Technology, Wisla, Poland.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Orlando, FL: Harcourt, Brace, & Janovich.

Fang, L. (2011). Phishing websites resulting in loss of millions of savings: The implications Retrieved March 11, 2012, from http://news.xinhuanet.com/fortune/2011-02/09/c_121056758.htm

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security, 2007*(3), 10-15. doi: 10.1016/s1361-3723(07)70035-0

Geer, D. (2005). Security technologies go phishing. *Computer Archive, 38*(6), 18–21.

Gilbert, D. T. (1999). What the mind's not. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 3-11). New York: The Guilford Press.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation, 13*(2), 149-172.

Griffin, E. (2006). Interperonal deception theory of david buller & judee burgoon *Communication: A first look at communication theory* (pp. 97-109): McGraw-Hill.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y.-K. (2007). *What instills trust? A qualitative study of phishing.* Paper presented at the USEC'07, Lowlands, Scarborough, Trinidad/Tobago.

Johnson, P. E., Grazioli, S., Jamal, K., & Berryman, R. G. (2001). Detecting deception: Adversarial problem solving in a low base-rate world. *Cognitive Science, 25*(3), 355-392. doi: 10.1207/s15516709cog2503_2

Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes,* *53*(2), 173–203.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering – the neglected human factor for information security management. *Information Resource Management Journal, 24*(3), 1-8.

Maheswaran, D., & Chaiken, S. (1991). Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. *Journal of Personality and Social Psychology, 61*(1), 13-25.

Microsoft. (2012). How to recognize phishing email messages, links, or phone calls Retrieved May 17, 2012, 2012, from http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, Ind.: Wiley Publishing, Inc.

Orlikowski, W. J., & Yates, J. (1994). Genre repertoire: The structuring of communicative practices in organizations. *Administrative Science Quarterly, 39*, 541-574.

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion*. New York: Springer - Verlag.

Sussman, S. W., & Siegal, W. S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. *Information Systems Research, 14*(1), 47-65.

Symantec. (2006). Symantec internet security threat report – trends for january 06–june 06, from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCUQFjAA&url=http%3A%2F%2Fwww.symantec.com%2Fspecprog%2Fthreatreport%2Fent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf

Symantec. (2011). Symantec internet security threat report – 2011 trends, from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J., & 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), 576-586. doi: 10.1016/j.dss.2011.03.002

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An empirical exploration of the design pattern of phishing attacks. In S. J. Upadhyaya & H. R. Rao (Eds.), *Annals of emerging research in information assurance, security and privacy services*. Bingley, England: Emerald Publishers.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. [Article]. *Information Systems Security, 16*(6), 315-331. doi: 10.1080/10658980701788165

Workman, M. (2008a). A test of interventions for security threats from social engineering. *Information Management & Computer Security, 16*(5), 463-483.

Workman, M. (2008b). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674. doi: 10.1002/asi.20779

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. [Article]. *Journal of Management Information Systems, 27*(1), 273-303.

Yates, J., Orlikowski, W. J., & Okamura, K. (1999). Explicit and implicit structuring of genres in electronic communication: Reinforcement and change of social interaction. *Organization Science, 10*(1), 83-117.

Yi, X. (2011). Startling 300 seconds: Fake bank of china sites rob customers of tens of millions Retrieved March 12, 2012, from http://finance.qq.com/a/20110221/000786.htm

Zhang, W., & Watts , S. (2003). *Knowledge adoption in online communities of practice.* Paper presented at the ICIS 2003, Seattle.

Zhang, W., & Watts, S. (2008). Capitalizing on content: Information adoption in two online communities. *Journal of Association of Information Systems, 9*(2), 73-94.