Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration

Xin (Robert) Luo [a,*], Wei Zhang [b], Stephen Burd [a], Alessandro Seazzu [a]

[a] Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA

[b] University of Massachusetts Boston, USA

ARTICLE INFO

Article history:
Received 30 May 2012
Received in revised form
18 November 2012
Accepted 11 December 2012

Keywords:
Phishing
Victimization
Explorative study
Social engineering
Heuristic–Systematic Model

ABSTRACT

To the extent that phishing has become a serious threat to information security, there has been rather limited theory-grounded research on this burgeoning phenomenon. In this paper, we develop a theoretical model of victimization by phishing based on the Heuristic–Systematic Model of information processing. We argue that the Heuristic–Systematic Model offers an ideal theoretical framework for investigating the psychological mechanism underlying the effectiveness of phishing attacks. An exploratory experiment is presented to validate the research model based on the theory.

1. Introduction

"Phishing is the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by assuming another's identity in an official-looking email, IM, etc. The user is provided with a convenient link in the same email that takes the email recipient to a fake webpage appearing to be that of a trustworthy company. When the user enters his personal information on the fake page, it is then captured by the fraudster." (USLegal.com, 2011)

Phishing is common, though exact statistics and incidence rates are difficult to come by due to the highly distributed nature of email and the World Wide Web. PhishTank, an organization that tracks phishing attacks verified 31,850 unique phishing attacks during July 2012 (PhiskTank, 2012). Of course, the actual incidence of phishing attacks is much higher since each attack can target millions of Internet users.

The success rate of phishing attacks is unknown, though controlled experiments often achieve alarmingly high success rates. For example, a controlled experiment was conducted by Master's students taking an information assurance course taught by one of the authors at a state university in 2010. The attack targeted 105 faculty and staff members via their University email addresses. Within 22 min of sending the phishing email, 38 (36.19%) people clicked the counterfeit link and 16 (15.24%) people submitted a valid username and password when prompted to login with their credentials. A controlled experiment using Indiana University students achieved a 15% success rate in a control group and a 72% success rate when the attack was modified to incorporate

* Corresponding author. Tel.: +1 505 277 8875; fax: +1 505 277 7108.
E-mail address: Luo@mgt.unm.edu (X.(Robert) Luo).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2012.12.003

victim-specific information from social networking sources (Jagatic et al., 2007).

One important reason for phishing attack success is that attacks are designed to exploit human cognitive biases instead of technology loopholes. Phishing offenders often masquerade as a credible figure and broadcast manipulative messages – through emails, instant messages, or short messages – to a large population. While the validity of the messages may not be difficult to disprove with some investigation, victims are usually caught off-guard at first glance. Victimization by phishing thus bypasses technological controls by manipulating human tendencies and information processing. As such, psychological and behavioral factors arguably play a more important role. Prior studies have attempted to investigate factors such as the influence of experiential and dispositional cues (Wright and Marett, 2010), individual differences in phishing susceptibility (Vishwanath et al., 2011), information carelessness (Workman, 2008), the severity of the phishing attack (Chen et al., 2011), and pragmatic preparedness of practitioners (Bose and Leung, 2008). However, little research has attempted to identify, describe, analyze, and organize those factors systematically. No study, to our best knowledge, has been able to systematically describe the psychological mechanism underlying the effectiveness of phishing attacks.

This paper endeavors to bridge that gap. Drawing on the Heuristic–Systematic Model, a dual-process theory of information processing, we conducted a qualitative study that investigates the human factors and psychological mechanisms associated with phishing attacks. We begin by introducing the Heuristic–Systematic Model and explaining how and why it can be applied to study victimization by phishing. We then develop a research model and follow with a description of an explorative study and discussion of research results. A short discussion on theoretical and pragmatic contributions that the model might provide concludes the paper.

2. Theoretical foundation

The Heuristic–Systematic Model (HSM) is a model of information processing (Chen and Chaiken, 1999) that originated from persuasion research in social psychology. Persuasion research studies how received messages can change people's attitudes. The gist of the HSM holds that when being persuaded, people first establish the validity of the received message using a combination of heuristics and systematic processing with the precise mix determined by multiple factors.

The HSM and closely-related models such as the Elaboration Likelihood Model (Petty and Wegener, 1999) are called *dual-process models* because they incorporate two information processing modes:

- ***Heuristic processing*** takes advantage of the factors embedded within or surrounding a message (called *heuristic cues*) such as its source, format, length, and subject, to quickly make a validity assessment.
- ***Systematic processing*** carefully researches the message's information content to make a validity assessment.

Compared with heuristic processing, systematic processing is more effortful and takes more time and cognitive resources. According to the HSM, people will tend to limit their investment of time and cognitive resources if they lack motivation or capability. Among the factors that may affect people to invest or not invest cognitive resources are:

- Perceived importance of the decision outcome
- Perceived risks
- Time and other pressures
- Skill level
- Distractions

In a similar fashion to Simon and Newell's description of satisficing (Newell and Simon, 1972), the HSM recognizes that people do not necessarily strive to generate validity assessments with the highest possible reliability or accuracy. They will stop processing when they feel their assessments are good enough. This notion led to HSM's inclusion of a unique concept called the *sufficiency threshold*—the "desired judgmental confidence" that people wish to reach when making decisions under a given circumstance (Eagly and Chaiken, 1993). HSM argues that when people engage in validity assessment, confidence in their assessment must reach or surpass the 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. Thus, when heuristic processing alone cannot lead message recipients to achieve the sufficiency threshold, it is likely that they will invoke systematic processing, even though it requires more effort.

On the other hand, not all decisions are worthy of the exhaustive effort required to generate high reliability or accuracy. People can adjust the sufficiency threshold and their decision-making effort based on their perceptions of importance and risks, available time and cognitive resources, social pressures, their own skill levels, and the results of initial heuristic processing. Of course, their perceptions of importance and especially risk are sometimes flawed.

Moreover, HSM contends that heuristic and systematic processing modes can and do occur concurrently. Potential interactions include:

- **Additivity** (reinforcement)—Heuristic and systematic processing may lead to the same conclusion and confidence in that conclusion will be higher than with either technique alone
- **Bias**—Heuristic processing may generate initial conclusions that bias the nature and scope of systematic processing
- **Attenuation**—Systematic processing may produce conclusions that limit or overturn those of heuristic processing

3. HSM model applications

The HSM and other dual-process information processing models have been supported and applied in many published studies in the social psychology literature such as Fabrigar et al. (1998), Maheswaran and Chaiken (1991), Rothman and Hardin (1997), and Sloman. Further support and application

is found in the marketing-related literature including Maheswaran et al. (1992), Aaker and Maheswaran, Frías et al. (2008), and Fishbein and Middlestadt.

Researchers in various computer- and information-related subfields have also supported and applied the HSM to user evaluation of trust and credibility in online scenarios such as Patrick et al. (2005), Wirth et al. (2007), Sundar (2008), and Hilligoss and Rieh (2007). Researchers that analyzed an experiment where students evaluated results returned by search engines concluded "… different degrees of heuristic and systematic processing occurred, depending on the situational demands as well as the Web experience and the domain specific involvement of the user (Wirth et al., 2007)." Researchers that analyzed digital media credibility evaluations by young people also found evidence that heuristic processing can lead directly to quick decisions (Sundar, 2008).

In an article summarizing the skills that users need to assess the credibility of online information, the authors proposed a model of Web site credibility assessment shown in Fig. 1 (Metzger, 2007). Note that the model explicitly incorporates aspects of the HSM including motivation, ability (skill), and both heuristic and systematic processing.

4. Phishing and the HSM model

Researchers have argued that HSM can be applied to broader validity-seeking contexts than other dual-process theories such as ELM (Chen and Chaiken, 1999). Aforementioned applications of HSM to studying search engine and web site credibility demonstrate its theoretical versatility. Phishing study can be another area where HSM can be fruitfully applied.

Messages used in phishing attacks contain at least some false content which can usually be identified with sufficient systematic processing. Thus the most common way to improve the success rate of phishing attacks is to mislead targeted victims into making a quick but incorrect assessment of the validity of the message. Therefore heuristic processing plays an important role in phishing victimization. From HSM's perspective, the success of a phishing attack depends on whether the attacker can achieve the following objectives individually or in combination:

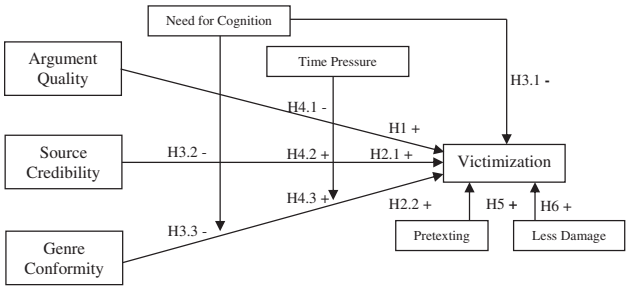


Fig. 2 – Proposed research model.

1) Provide a message that can withstand systematic processing so that targeted victims will make wrong assessment of message validity even after closely examining the message
2) Promote heuristic processing based on false cues so that targeted victims will make a quick but incorrect decision on message validity
3) Suppress systematic processing so that targeted victims have to rely on quick but error-prone heuristic processing
4) Reduce the sufficiency threshold so that targeted victims will not initiate systematic processing

To illustrate how HSM can be employed to investigate phishing, we present a preliminary research model (Fig. 2). 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 and Chaiken, 1993) – of the message on validity assessment. When systematic processing occurs, high-quality arguments lead to favorable message assessment. In the current research context of phishing attacks, false messages are used with the intention to mislead the message recipients. A high level of argument quality that can withstand message recipients' systematic processing increases the likelihood of victimization. Therefore, we hypothesize:

H1. Message recipients will be more likely to be victimized by phishing messages with high argument quality.

Heuristic processing depends on readily available heuristic cues. One heuristic cue that has been extensively studied

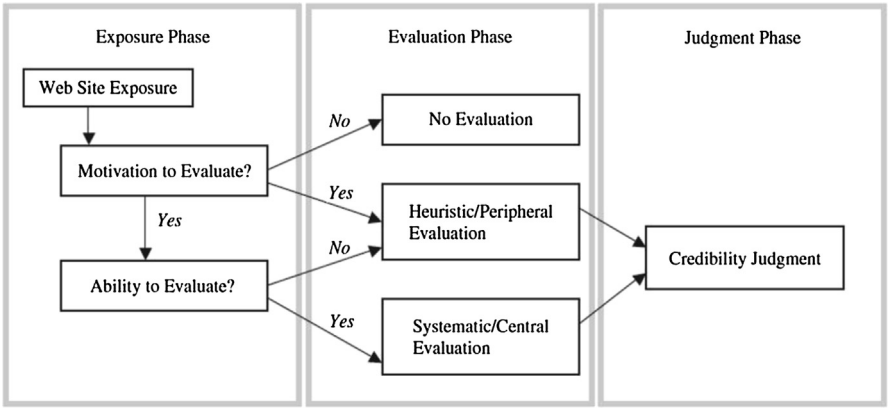


Fig. 1 – Dual-processing model of Web site credibility assessment (Metzger, 2007).

(Sussman and Siegal, 2003; Zhang and Watts, 2008) and that phishing offenders often employ is *source credibility*: Most phishing messages assume a false source identity—usually, a credible source such as a friend or authoritative department. The effectiveness of (false) source credibility has been repeatedly demonstrated in actual phishing attacks, thus:

H2.1. 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 is *genre conformity*. Genres are "socially recognized types of communicative actions that are habitually enacted by members of a community to realize particular social purposes" (Orlikowski and Yates, 1994). Genres serve as templates for communication. They represent the association between communication formats and communication purposes (Yates et al., 1999) and help to improve communication efficiency and effectiveness.

For example, as businesses usually develop specific communication genres to communicate with their customers. For example, email messages from a bank to its customers might employ consistent use of logos, fonts, phrases, and overall organization. Over time, customers become accustomed to these characteristics and use them as heuristic cues of authenticity. Phishing offenders can abuse these genres by creating messages that resemble legitimate messages and mislead the recipients into believing that the messages are valid (Zhang and Watts, 2003).

In this research model, we define genre conformity as 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 posit:

H2.2. Message recipients will be more likely to be victimized by phishing messages with higher level of genre conformity.

Factors that can affect the extent of systematic processing and heuristic processing are typically modeled as moderators in research using dual-process theories (e.g., Sussman and Siegal, 2003; Zhang and Watts, 2008). In this research model, we focus on one personality variable, *need for cognition*, and one contextual variable, *pressure for immediate action*. Need for cognition refers to the intrinsic desire for a person to comprehend and structure environmental information. It captures individual differences in predisposition to engage in effortful cognitive activities (Cacioppo and Petty, 1982; Petty and Cacioppo, 1986). Previous research suggests that people with a higher level of need for cognition are more likely to engage in systematic processing and less likely to be influenced by heuristic processing. Since an increased level of systematic processing is more likely to reveal the false content in a phishing message, recipients with higher level of need of cognition are less likely to be victimized. Thus we hypothesize:

H3.1 Message recipients with higher need for cognition is less likely to be victimized.
H3.2 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.
H3.3 Effect of genre conformity on victimization will be less for message recipients with higher need for cognition.

Systematic processing demands time and cognitive resources. Systematic processing is suppressed if message recipients are distracted or are pressed for time. Some phishing attacks attempt to exaggerate the urgency of responding to or acting on the message as soon as possible, thus suppressing systematic processing. Under such circumstances, message recipients usually have to rely on heuristic processing to make decisions, which are often incorrect due to bogus heuristic cues. Thus, we hypothesize,

H4.1 Phishing messages that impose more time pressure decrease the effect of argument quality.
H4.2 Phishing messages that impose more time pressure increase the effect of source credibility.
H4.3 Phishing messages that impose more time pressure increase the effect of genre conformity.

Lastly, we explore factors that can lower the sufficiency threshold for message recipients. *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, reduce their suspicions, and eventually mislead them to give away sensitive information or perform actions that would be deemed atypical or otherwise in violation of company policies (Mitnick and Simon, 2002). Pretexting comes in many forms. A common prerequisite for pretexting success is research into people and events within a victim's organization. For example, a perpetrator might read a newspaper story about a hacking attack at a hospital in which patient data was compromised. The story might include a quote from a company executive that the XYZ consulting firm has been hired to investigate the cause and improve data security. The perpetrator might then craft a message that appears to be from an employee of XYZ consulting firm, access the hospital's web site to extract employee email addresses, and target those employees with a false request to change their passwords. In terms of the HSM, we hypothesize that pretexting lowers the sufficiency threshold of message recipients, and hence:

H5. Phishing attacks coupled with pretexting are more likely to victimize message recipients.

We also believe that phishing messages targeting less damage will lead the message recipients to care less about the message validity and more likely to act as instructed by the message. As research in ecommerce and information privacy has long suggested, people's online behavior is influenced by their perception of how risky that behavior will be (Dinev and Hart, 2006). When people perceive a high risk of losing control of their information, they are more likely to guard the information (Malhotra et al., 2004). Conversely, when they do not feel that they have much to lose, they are more likely to oblige and disclose information (Li et al., 2011). Moreover, an individual's assessment of potential damage is situational, rooted in the circumstance under which the decision is made (Li et al., 2011). With less damage (e.g., asking for a small

amount of donation or less sensitive information), phishing attackers may avoid raising the sufficiency threshold or even lower it, reducing the probability that message recipients will engage in systematic processing. Thus,

H6. Phishing attacks targeting less damage are more likely to victimize message recipients.

5. Research method

5.1. Overview

Students in a graduate information assurance class were asked to develop, launch, and analyze the results of a phishing attack

A

UNM 2011 Budget Cuts Survey

UNM Surveys [unmsurveys@gmail.com]

Sent: Thursday, December 02, 2010 11:55 AM
To: ASM-Staff-DU

Dear faculty and staff,

Here at the University of New Mexico we take great pleasure in making sure your opinion is taken into account. As you all know, the University of New Mexico expects to slash its budget by more than 5 percent next year due to the reduced state funding and the expiration of federal stimulus money. Critics have claimed the across-the-board cuts disproportionately affected academics while not making enough from University administration and athletics.

We are asking all faculty and staff to participate in a short survey that will help the university determine if the budget cuts are jeopardizing the academic mission of the University. We take great pride in our academics and want to make sure the budget cuts will not hamper our student's experience. We feel that with the faculty and staff's support, we can persuade the University to take more cuts from the administration and athletic departments rather than the academic departments.

This short survey will take no longer than 5 minutes to complete and we are asking that only faculty and staff participate. Please CLICK HERE to participate in the survey. You will be asked to enter your UNM Net ID and password to make sure only UNM faculty and staff are participants in the survey.

Thank you for your time and we value your opinion!

Office of the President
President's Strategic Advisory Team (PSAT)

B

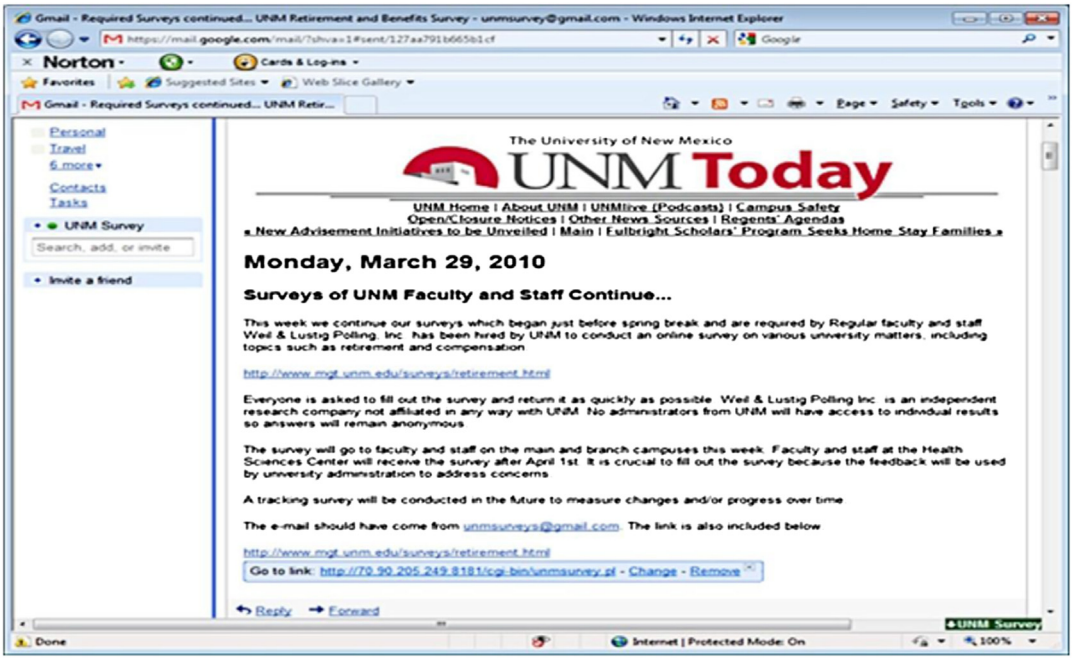


Fig. 3 – A. Phishing email message; B. Phishing survey.

against 105 faculty and staff members at the School of Management in a public university located in southwest US. A faculty member supervised each step but the students themselves were responsible for all aspects of the attack. Beyond the educational objectives for the students, the exercise was intended to gauge faculty and staff susceptibility and the effectiveness of spear phishing. Spear phishing targets specific victims and high net worth individuals, often with intimate knowledge of the target organization and/or individuals.

Phishing emails arrive at the school email server on a daily basis though almost all are caught by email filters. Of those messages that do escape filtering, many have significant flaws in their design such as grammatical errors or strange source email addresses. This exercise was intended to test user susceptibility to a sophisticated spear phishing attack.

The team's approach in this exercise was a two-phase operation. The first phase entailed crafting a message that achieved two goals:

- Incorporate multiple techniques to promote incorrect or biased heuristic processing and suppress systematic processing
- Survive at least minimal systematic processing if the first goal wasn't achieved

The second phase was to include a hyperlink within the email for the victim to complete a survey on current events at the institution. The goal was to phish staff and faculty for their login and password credentials just like a cyber-criminal would.

5.2. *Anatomy of the attack*

Students were instructed to employ several techniques to boost attack effectiveness:

- Mimic the structure and content of existing university communications (genre conformity)
- Choose a subject area of timely interest to many intended victims (pretexting)
- Create a sense of urgency (time criticality or time pressure)

Instead of 'spoofing' an email to look like it came from a valid email address in the organization the team created one they felt would appear genuine, UNMsurveys@gmail.com, with the from field 'UNM Surveys'. In order to pique the interest of the intended victims the team needed to find a current topic of interest at the institution and request input and comments. Looming budget cuts to academics and administration during a volatile time and related rumors about possible cuts to retirement and other benefits provided an ideal basis for pretexting. In addition, publicly reported delays in budget talks coupled with a general lack of

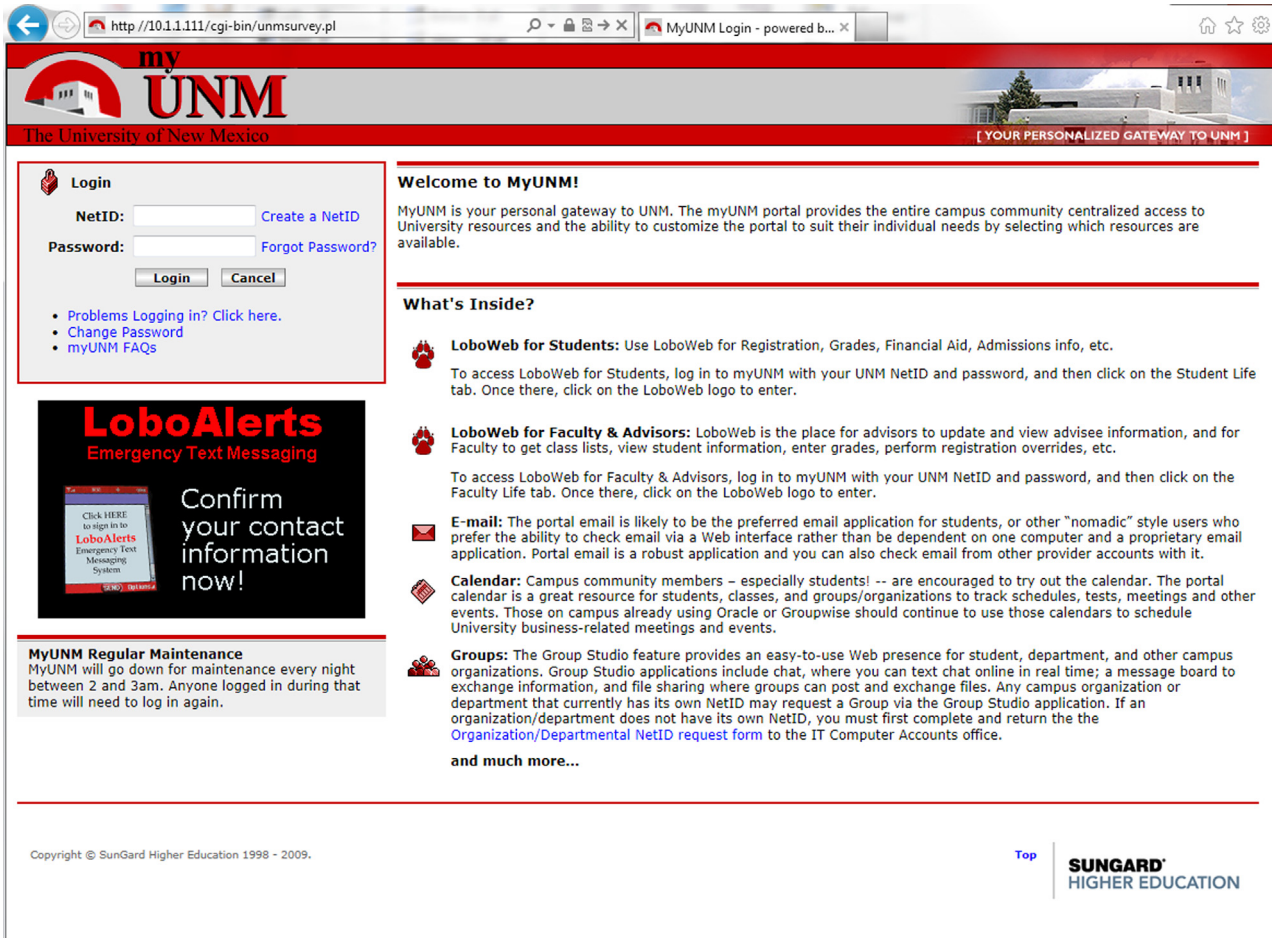


Fig. 4 – Masqueraded login page.

transparency by university administrators had now placed the target population in a vulnerable position – anxious to get an update on the situation and eager to provide feedback. In addition, the university had used the services of an outside company a few months earlier for an unrelated faculty survey. With the delivery method in place and the carrier message crafted the team continued to phase 2.

The team mimiced the UNM CAS (Central Authentication Service) login template since as it was universally familiar around campus. It was a simple process of copying over the source code and saving it to a new file on our server. Additionally they recycled a small script used in previous classes which records the victim's IP address, Net ID and password, and stores them in a file. In order to ensure the personal security and integrity of the victim's information they also built a script to remove the first five characters of the Net ID and password before being stored. In order to bypass the email filtering services the team registered a valid domain name to embed in the email that would host the survey and authentication web site, http://login.unmsurveys.org.

The email shown in Fig. 3A was sent to all school faculty and staff members at the university email addresses. Many parts of the message incorporate heuristic cues from similar legitimate email messages including the banner, links at the top of the page, fonts, and general layout. Students searched publicly-accessible archives of older email messages via the university web site in order to find samples to emulate. The university had conducted multiple surveys on a variety of topics in the preceding months including healthcare insurance, commuting habits, and evaluations of senior administrators. Thus, the arrival of yet another survey request should not have raised many suspicions by itself among intended victims. An example is shown in Fig. 3B, where elements of the message mimic those of common communications between a university and its faculty and staff using heuristic cues such as colors, logos, and the standard layout of an internal newsletter.

If the hyperlink in the blue box was clicked, the intended victim's Web browser was directed to a page on a server managed by the students (see Fig. 4). The displayed page mimics the real login page for the university faculty/staff portal in minute detail (see Fig. 5). If the intended victim entered a username and password then he or she was redirected to a two-page retirement survey (Fig. 6 shows the first page). Usernames, passwords, and survey responses were not stored or further analyzed.

5.3. *Results and findings*

There were 105 people listed in the school's staff and faculty distribution lists. Within a 22 min period the spear phishing attack was able to bait 38 people to click the embedded link and log 16 sets of credentials (see Table 1). At that point, the

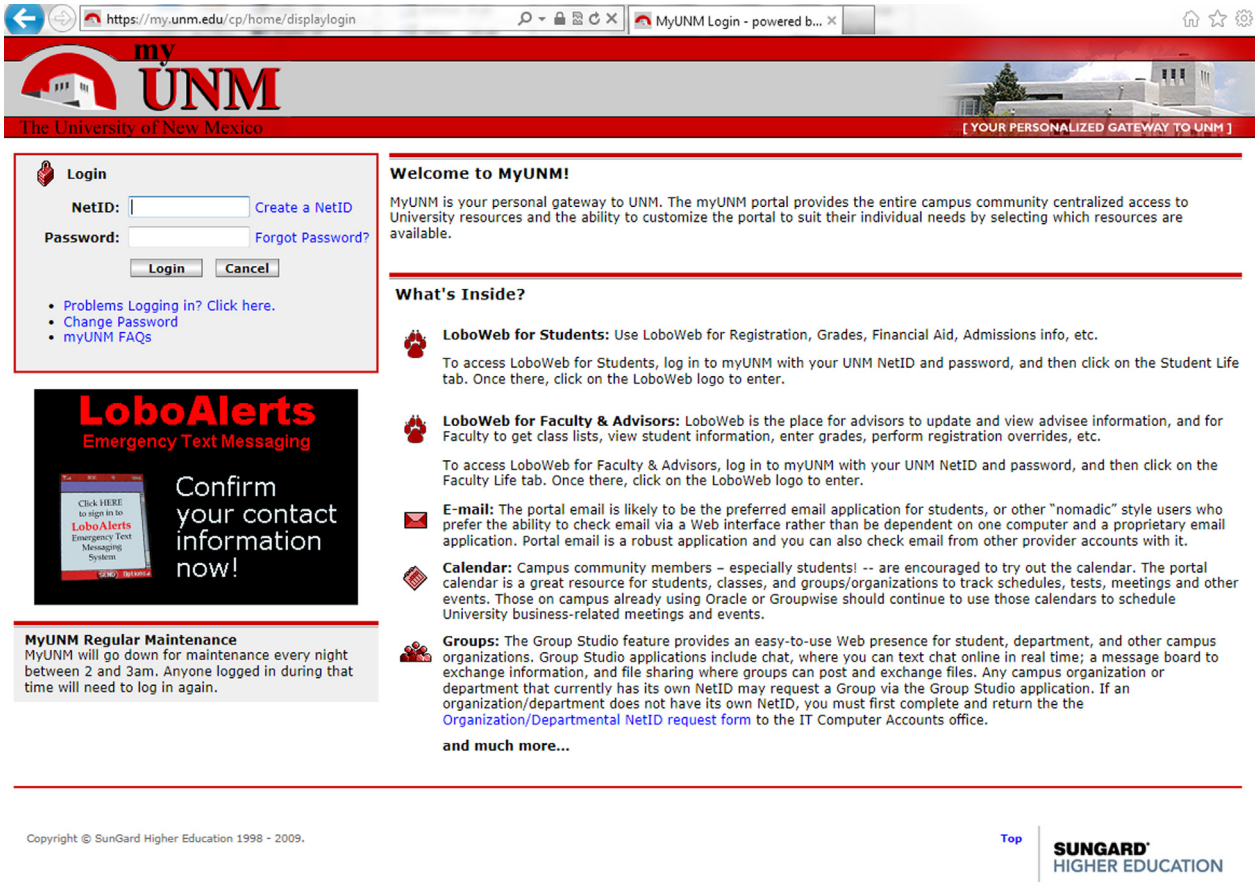
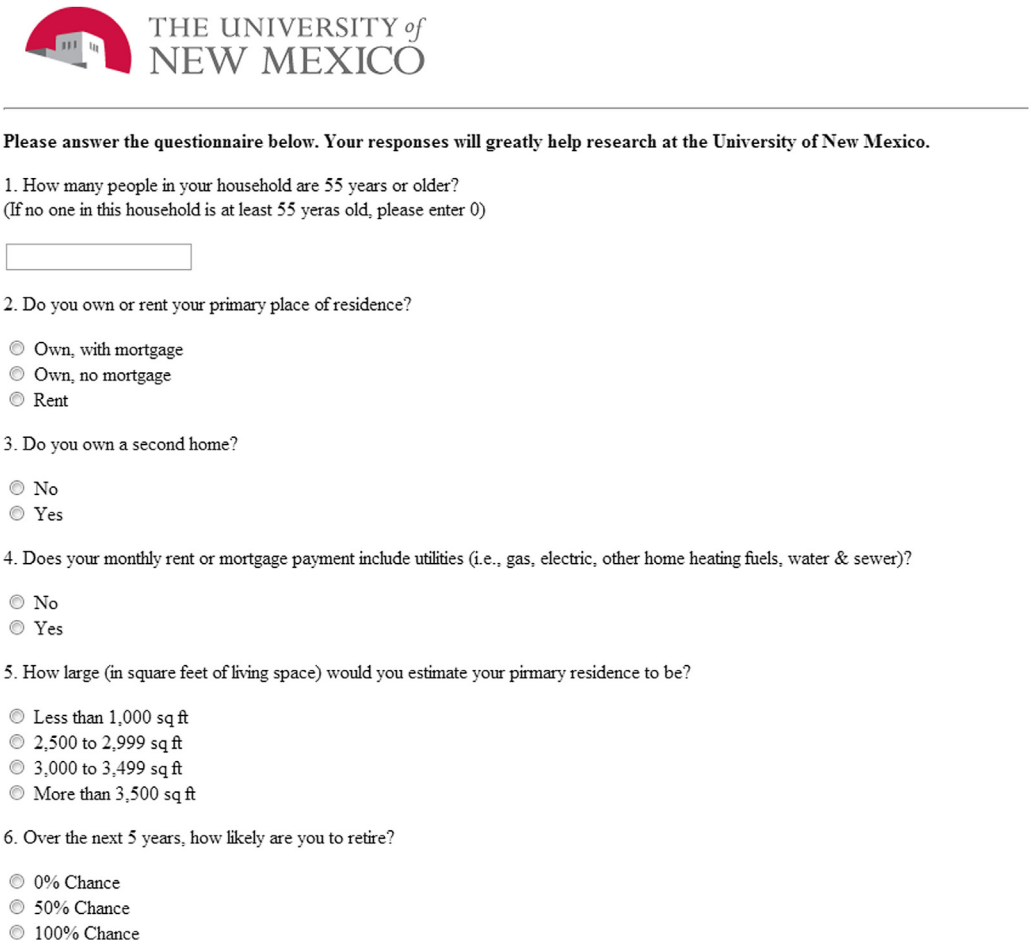


Fig. 5 – Actual university login page.


THE UNIVERSITY of NEW MEXICO

Please answer the questionnaire below. Your responses will greatly help research at the University of New Mexico.

1. How many people in your household are 55 years or older?
(If no one in this household is at least 55 yeras old, please enter 0)

2. Do you own or rent your primary place of residence?

- Own, with mortgage
- Own, no mortgage
- Rent

3. Do you own a second home?

- No
- Yes

4. Does your monthly rent or mortgage payment include utilities (i.e., gas, electric, other home heating fuels, water & sewer)?

- No
- Yes

5. How large (in square feet of living space) would you estimate your pirmary residence to be?

- Less than 1,000 sq ft
- 2,500 to 2,999 sq ft
- 3,000 to 3,499 sq ft
- More than 3,500 sq ft

6. Over the next 5 years, how likely are you to retire?

- 0% Chance
- 50% Chance
- 100% Chance

Fig. 6 – Retirement survey first page.

attackers could have compromised their computer systems and any digital resources for which they had sufficient privileges. A real phishing scam might have also embedded a worm or virus into the page and infected the victim's computer.

The experiment could have victimized more users were it not for an unfortunate detail—a detail that made the phishing email seem authentic but also led its discovery as a fraud. The message used a name very similar to the name of an employee from the Office of the President. The similarity made the message appear to come from an appropriate and credible source but it also meant that this person could be directly contacted for confirmation. The Associate Dean at the School of Management quickly contacted this person to ask if the email he received was from her, to which she responded no. He then sent a message to all faculty and staff alerting them that the email was not real and warning them to not click the link.

Table 1 – Phishing results.

	Clicked the link	Submitted credentials (net ID/password)
Number	38	16
Percentage	**36.19%**	15.24%

6. Discussion & limitations

Table 2 summarizes the correspondence between testable hypotheses in our research model and salient features of the explorative study. Though the study was neither a controlled experiment nor an exhaustive test of the hypotheses, its design and results do support the plausibility of applying HSM to studying phishing since all of the results are consistent with the hypotheses we were able to test.

The successful launch of the spear phishing attack can help scientifically explain the influences of the independent variables on the dependent variable in an interpretive manner. In terms of scientific research validation, a narrowly targeted spear phishing attack has inherent advantages and limitations. Spear phishing messages appear to originate from a trusted source (i.e., a person in a position of authority of the victim's own organization), so it's likely that the research model carries exceedingly satisfactory explanatory power of the independent variables on the dependent variable (i.e., victimization). Yet employing spear phishing to test the proposed research model risks loss of generalizability due to the narrow focus of the targeted victims. The masqueraded email has high-quality grammar and punctuation as well as convincing and properly formatted content—in other words, high argument quality. The surprisingly short time frame

Table 2 – Correspondence among testable model hypotheses and results of the study.

Hypothesis	Explorative study
H1. Message recipients will be more likely to be victimized by phishing messages with high argument quality.	Message was well-crafted with proper grammar, punctuation, and style, and lacking obvious content or format errors – hypothesis is consistent with study results
H2.1. Message recipients will be more likely to be victimized by phishing messages pretending to be from a source with higher level of source credibility.	Fraudulent message source was purportedly a high-ranking official within the intended victims' organization – hypothesis is consistent with study results
H2.2. Message recipients will be more likely to be victimized by phishing messages with higher level of genre conformity.	Message mimicked legitimate organizational messages with attributes such as layout, font, and images – hypothesis is consistent with results
H3.1 Message recipients with higher need for cognition is less likely to be victimized.	Faculty and staff tend to have high education levels and strong attention to detail indicative of need for cognition though actual levels and differences in levels between victims and non-victims weren't measured – consistency of hypotheses with study results is uncertain
H3.2 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.	
H3.3 Effect of genre conformity on victimization will be less for message recipients with higher need for cognition.	
H4.1 Phishing messages that impose more time pressure decrease the effect of argument quality.	Time pressure was only weakly present in the study – hypothesis is not fully tested
H4.2 Phishing messages that impose more time pressure increase the effect of source credibility.	
H4.3 Phishing messages that impose more time pressure increase the effect of genre conformity.	
H5. Phishing attacks coupled with pretexting are more likely to victimize message recipients.	Message incorporated strong pretexting – hypothesis is consistent with study results
H6. Phishing attacks targeting less damage are more likely to victimize message recipients.	Message didn't incorporate any elements with obvious damage potential – hypothesis is consistent with study results

required to capture 16 valid login credentials is consistent with H1. In other words, high argument quality appears to lead to successful victimization.

The phishing email spoofed an authoritative university official's identify, thus generating source credibility. Until the email was personally verified by a potential victim, the fraudulent source credibility was unchallenged. Has the results of the Associate Dean's systematic processing not been quickly communicated to others, the population of victims might have been larger. Thus, H2.1 appears to be consistent with the attack's success.

Furthermore, H2.2 also seems consistent with the results because the victims surmised that the email communication was a legitimate organizational communication due to its strong genre conformity. The student team went to great lengths to ensure genre conformity by examining similar publicly-accessible messages and mimicking as many of their features as possible.

Due to the fact that the current data analytical method is insufficient to catch the moderating effect given the absent measure levels of *need for cognition* and *time pressure*, H3.* and H4.* are in store for future empirical validation. We however conjecture that phishing messages which carry less need for cognition and time pressure could further justify the success of this spear phishing attack given the fact that email communication frequently occurs between the university and its employees.

The message exhibited a degree of genre conformity through timing and content. By incorporating a "hot topic" for the intended victims (i.e., retirement plan and benefits), the phishing attack effectively legitimized the interactions between the student team and the victims. Also, the low potential for damage plays a significant role in convincing the victims to divulge their confidential information in a short time. As such, H5 and H6 appear consistent with the attack results.

The proposed research model serves as an overarching model for future studies. This study shows that HSM has the potential to be a solid theoretical foundation for studying phishing. It provides a theoretical framework for future research in which both qualitative and quantitative data will be collected to more thoroughly examine and gauge the research model and hypotheses. Qualitative data collected through field observations and interviews will allow researchers to gain more first-hand insights into the phishing attacks and the messages they use, and provide the opportunity to verify theoretical reasoning and refine it. In addition, quantitative data collected through scenario-based surveys, on the other hand, will allow investigators to test the hypotheses in a positivist way. It is hoped that the proposed moderating effects on hypotheses H3.2, H3.3, H4.2, and H4.3 shall be examined in a quantitative approach (i.e., using Structural Equation Modeling technique). Through triangulating the findings from both methodological approaches, future researchers can gain more confidence in the validity of the findings toward scientifically rigorous outcomes in the near future.

Despite the fact that the explorative study strives to validate the proposed framework in a qualitative way, this study inevitably suffers from several limitations. First, the constructs and hypotheses need to be further operationalized to enhance their rigor and appropriateness for further parsimonious investigations. Second, although a detailed understanding of the determinants of phishing victimization is an interesting goal in itself, many researchers, system/network

administrators, and users are more interested in how to prevent phishing victimization. One possible application of the results of controlled experiments of the above hypotheses will be to determine which are proven and to what extent each contributes to victimization. Knowing which model components are most significant will provide direction to further research specifically targeted to reducing victimization and will ultimately enable more precise targeting of anti-phishing efforts. For example, if source credibility were the most significant determinant, anti-phishing technology researchers and vendors might achieve greater success by concentrating their efforts on sender identification technologies and system administrators might add them to email and other messaging systems. In addition, user training efforts might place greater emphasis on identifying bogus and valid senders and teach specifically-targeted techniques, skills, and exercises to do so.

7. Conclusions

In this article we propose a study of victimization by phishing based on HSM. Through this qualitative explorative study, we hope to offer instrumental insights to the often neglected human aspects of information systems security management and to theoretically advance behavioral information security research. Applying HSM to victimization by phishing, we strive to test the theoretical underpinning in a new research context, and potentially advance this popular theory as well as this line of research. We believe that the surprising yet intriguing results derived from this study can pragmatically inform business decision-makers of how employees can deal with phishing attacks and social policy-makers of how public can recognize and circumvent phishing attacks.

Acknowledgement

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

REFERENCES

Aaker JL, Maheswaran D. The effect of cultural orientation on persuasion. Journal of Consumer Research;24:315–28.

Bose I, Leung ACM. Assessing anti-phishing preparedness: a study of online banks in Hong Kong. Decision Support Systems 2008;45:897–912.

Cacioppo JT, Petty RE. The need for cognition. Journal of Personality and Social Psychology 1982;42(1):116–31.

Chen S, Chaiken S. The heuristic–systematic model in its broader context. In: Chaiken S, Trope Y, editors. Dual process theories in social psychology. Guilford Press; 1999.

Chen X, Bose I, Leung ACM, Guo C. Assessing the severity of phishing attacks: a hybrid data mining approach. Decision Support Systems 2011;50:662–72.

Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. Information Systems Research 2006; 17(1):61–80.

Eagly AH, Chaiken S. The psychology of attitudes. Orlando, FL: Harcourt, Brace, & Janovich; 1993.

Fabrigar LR, Priester JR, Petty RE, Wegener DT. The impact of attitude accessibility on cognitive elaboration of persuasive messages. Personality and Social Psychology Bulletin 1998;24: 339–52.

Fishbein M, Middlestadt S. Noncognitive effects on attitude formation and change: fact or artifact? Journal of Consumer Psychology;2:181–202.

Frías DM, Rodríguez MA, Castañeda JA. Internet vs. travel agencies on pre-visit destination image formation: an information processing view. Tourism Management 2008;29: 163–79.

Hilligoss B, Rieh SY. Developing a unifying framework of credibility assessment: construct, heuristics, and interaction in context. Information Processing and Management 2007. http://dx.doi.org/10.1016/j.ipm.2007.10.001.

Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Communications of the ACM October 2007;50(10).

Li H, Sarathy R, Xu H. The role of affect and cognition on online consumers' willingness to disclose personal information. Decision Support Systems 2011;51(3):434–45.

Maheswaran D, Chaiken S. Promoting systematic processing in low-motivation settings: effect of incongruent information on processing and judgment. Journal of Personality and Social Psychology 1991;61:13–25.

Maheswaran D, Mackie DM, Chaiken S. Brand name as a heuristic cue: the effects of task importance and expectancy confirmation on consumer judgments. Journal of Consumer Psychology 1992;1:317–36.

Malhotra NK, Sung SK, Agarwal J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 2004;15(4):336–55.

Metzger M. Making sense of credibility on the web: models for evaluating online information and recommendations for future research. Journal of The American Society for Information Science and Technology 2007;58(13):2078–91.

Mitnick KD, Simon WL. The art of deception: controlling the human element of security. Indianapolis, Ind.: Wiley Publishing, Inc.; 2002.

Newell A, Simon HA. Human problem solving. Prentice-Hall; 1972.

Orlikowski WJ, Yates J. Genre repertoire: the structuring of communicative practices in organizations. Administrative Science Quarterly 1994;39:541–74.

Patrick A, Marsh S, Briggs P. Designing systems that people will trust. In: Security and usability: designing secure systems that people can use. National Research Council Canada; January 2005.

Petty RE, Cacioppo JT. Communication and persuasion. New York: Springer-Verlag; 1986.

Petty RE, Wegener DT. The elaboration likelihood model: current status and controversies. In: Chaiken S, Trope Y, editors. Dual process theories in social psychology. Guilford Press; 1999.

PhiskTank. Phishing statistics for July 2012 [downloaded on 04.10.12], http://www.phishtank.com/stats/2012/07.

Rothman A, Hardin CD. Differential use of the availability heuristic in social judgment. Personality and Social Psychology Bulletin 1997;23:123–38.

Sloman SA. The empirical case for two systems of reasoning. Psychological Bulletin;119:3–22.

Sundar SS. The MAIN model: a heuristic approach to understanding technology effects on credibility. Digital media, youth, and credibility. In: Metzger Miriam J, Flanagin Andrew J, editors. The John D. and Catherine T. MacArthur Foundation series on digital media and learning. Cambridge, MA: The MIT Press; 2008. p. 73–100. http://dx.doi.org/10.1162/dmal.9780262562324.073.

Sussman SW, Siegal WS. Informational influence in organizations: an integrated approach to knowledge adoption. Information Systems Research 2003;14(1):47–65.

USLegal.com. Phishing definition. http://definitions.uslegal.com/p/phishing [downloaded on 14.06.11].
Vishwanath A, Herath T, Chen R, Wang J, Rao HR. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems 2011;51:576–86.
Wirth W, Böcking T, Karnowski V, von Paper T. Heuristic and systematic use of search engines. Journal of Computer-Mediated Communication 2007;12:778–800.
Workman M. 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 2008;59(4):662–74.
Wright RT, Marett K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. Journal of Management Information Systems 2010;27(1):273–303.
Yates J, Orlikowski WJ, Okamura K. Explicit and implicit structuring of genres in electronic communication: reinforcement and change of social interaction. Organization Science 1999;10(1):83–117.
Zhang W, Watts S. Knowledge adoption in online communities of practice. Seattle: ICIS; 2003.
Zhang W, Watts S. Capitalizing on content: information adoption in two online communities. Journal of Association of Information Systems 2008;9(2):73–94.

Dr. Xin (Robert) Luo is an Associate Professor of Management Information Systems and Information Assurance in the Anderson School of Management at the University of New Mexico, USA. He earned his Ph.D. in Information Systems from Mississippi State University. His research interests include information assurance, e-commerce/m-commerce, and cross-cultural management. His research has been published in journals including *Journal of the Association for Information Systems, European Journal of Information Systems, Communications of the ACM, Decision Support Systems, Journal of Strategic Information Systems, Communication of the Association for Information Systems, and Journal of Organizational and End User Computing, etc.*

Dr. Wei Zhang is an Associate Professor of Management Information at the University of Massachusetts Boston. His research interests include Knowledge Management, Information Systems in Nonprofits, and Information Systems Education. Dr. Zhang has published in journals such as *Journal of Association for Information Systems, Social Work, Communications of the Association for Information Systems,* and *Journal of Information Systems Education*. He earned his bachelor's degree from University of Science and Technology of China, his master's degree from Renmin University of China, and his doctorate in management information systems from Boston University.

Dr. Stephen Burd is an Associate Professor of Management in the Anderson School of Management at the University of New Mexico. He earned his Ph.D. from Purdue University in 1983. His teaching and research interests include computer and software architecture, system and network administration, healthcare technology and cost-effectiveness, and database management. He is Associate Director for UNM's Center for Information Assurance Research and Education and is Secretary and Treasurer of the New Mexico Telehealth Alliance. He is a Certified Public Accountant licensed in Maryland.

Professor Alessandro Seazzu is the director of UNM's Center for Information Assurance Research and Education (CIARE). Through CIARE, UNM has been designated by the NSA and DHS as a Center of Academic Excellence in Information Assurance and was recently selected as the host site for one of the FBI's Regional Computer Forensics Laboratory. He has been a faculty member with the Anderson School since 1995. His areas of research and study have been in virtual environments in security and human behavior in security.