2012 45th Hawaii International Conference on System Sciences

How Could I Fall for That?
Exploring Phishing Victimization with the Heuristic-Systematic Model

Wei Zhang
University of Massachusetts Boston
Wei.Zhang@umb.edu

Xin Luo
University of New Mexico
luo@mgt.unm.edu

Stephen D. Burd
University of New Mexico
burd@mgt.unm.edu

Alessandro F. Seazzu
University of New Mexico
alex@mgt.unm.edu

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 propose a study on 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, and present a preliminary 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." [26]

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 14,586 unique phishing attacks during April, 2011 [21]. 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 informal and 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 minutes 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 victim-specific information from social networking sources. [11]

Phishing 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, but little research has attempted to identify, describe, and analyze them systematically. This paper endeavors to bridge the gap.

Prior studies have attempted to investigate phishing through a variety of theory-driven and methodological means, such as the influence of experiential and dispositional cues [30], individual differences in phishing susceptibility [27], information carelessness [29], hybrid data mining on the severity of the phishing attack [5], and pragmatic preparedness of practitioners [2]. No study, to our best knowledge, has been able to further gauge the psychological mechanism underlying the effectiveness of phishing attacks.

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.302

IEEE computer society

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

Drawing on a dual-process theory of information processing, we propose an empirical study that investigates the human factors and psychological mechanisms associated with phishing attacks based on Heuristic-Systematic Model. We begin with introducing the model and explaining why it can be applied to study victimization by phishing. We then develop a preliminary research model, followed by a brief discussion on research method. A short discussion on potential contributions that the model might provide concludes the paper.

2. Heuristic-Systematic Model

The Heuristic-Systematic Model (HSM) is a model of information processing [4] that originated from persuasion research in social psychology. Persuasion research studies how received messages can change people's attitudes. The gist of the HSM model 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 [20] 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 analyzes the message's information content and may also conduct follow-on research 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 unless motivated to do so. Among the factors that may motivate people to invest or not invest cognitive resources are:

- Perceived importance of the decision outcome
- Perceived risks
- Time and other pressures
- Skill level
- Presence/absence of heuristic cues

In a similar fashion to Simon and Newell's description of satisficing [16], the HSM recognizes that not all decisions are worthy of the exhaustive effort required to generate high reliability or accuracy. People adjust 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.

HSM is unique among dual-process information processing models due to its inclusion of a concept called the *sufficiency threshold*—the "desired judgmental confidence" that people wish to reach when making decisions under a given circumstance [6]. 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. Thus, 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 requires more effort

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 [7], [12], [22], and [23]. Further support and application is found in the marketing-related literature including [13], [1], [9], and [8].

Researchers in various computer- and information-related subfields have also supported and applied the HSM model to user evaluation of trust and credibility in online scenarios such as [18], [28], [24], and [10]. 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." [28]. Researchers that analyzed digital media credibility evaluations by young people concluded "A heuristic thus invoked can either directly lead to a snap judgment as in heuristic processing … or serve to

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

frame, bias, or otherwise guide more systematic processing of ..." [24]

In an article summarizing the skills that users need to assess the credibility of online information, the author proposed a model of Web site credibility assessment shown in Figure 1 [14]. Note that the model explicitly incorporates aspects of the HSM including motivation, ability (skill), and both heuristic and systematic processing.

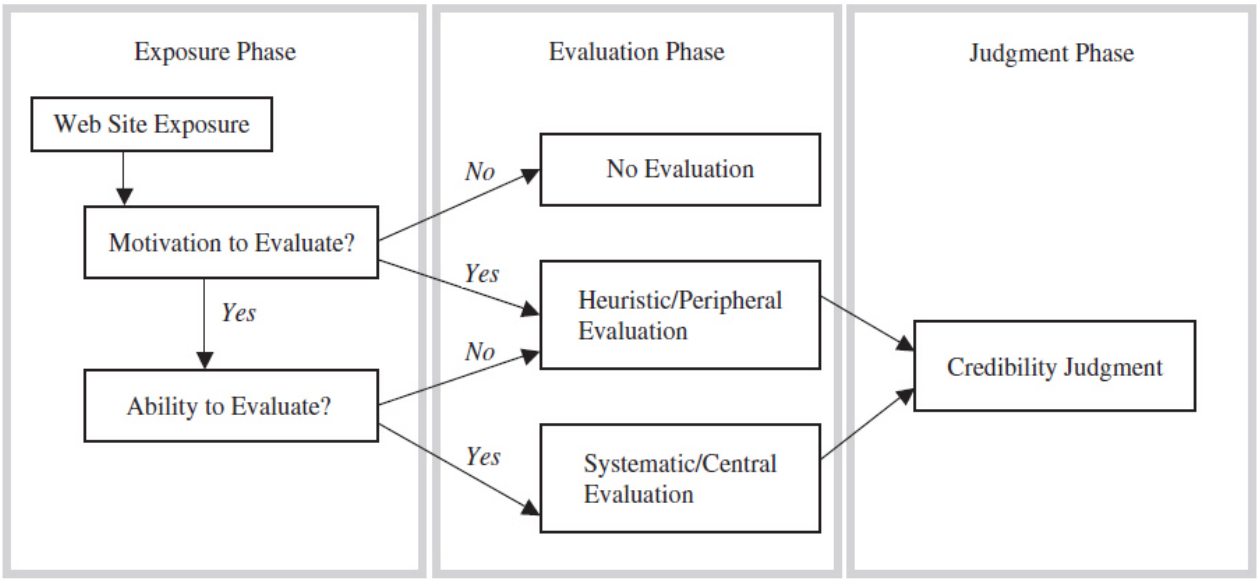

Figure 1. Dual-processing model of Web site credibility assessment. [14]

4. Phishing and the HSM Model

Application of the HSM to phishing is a straightforward extension of the applications of search engine and web site credibility noted above. The nature of phishing attacks is to mislead message recipients into making a quick but incorrect heuristic assessment of the validity of false messages, thus avoiding or biasing systematic processing. Thus from HSM's perspective, the success of a phishing attack depends on whether the attacker can achieve the following objectives individually or in combination:

1) Promote heuristic processing
2) Suppressing systematic processing
3) Reduce the sufficiency threshold
4) Provide a message that can stand systematic processing

In this sense, HSM provides an ideal theoretical framework to understand victimization by phishing.

To illustrate how HSM can be employed to investigate how phishing leads to victimization, we present a preliminary research model (Figure 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" [6] – 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. High level of argument quality that can stand message recipients' systematic processing will increase the likelihood that they be victimized. Therefore, we hypothesize:

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

Heuristic processing depends on the ready availability of heuristic cues. One heuristic cue that has been extensively studied [25] [33] and that phishing offenders particularly like to take advantage of is *source credibility*: Most phishing messages assume a false source identity and pretend to be from 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.*

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

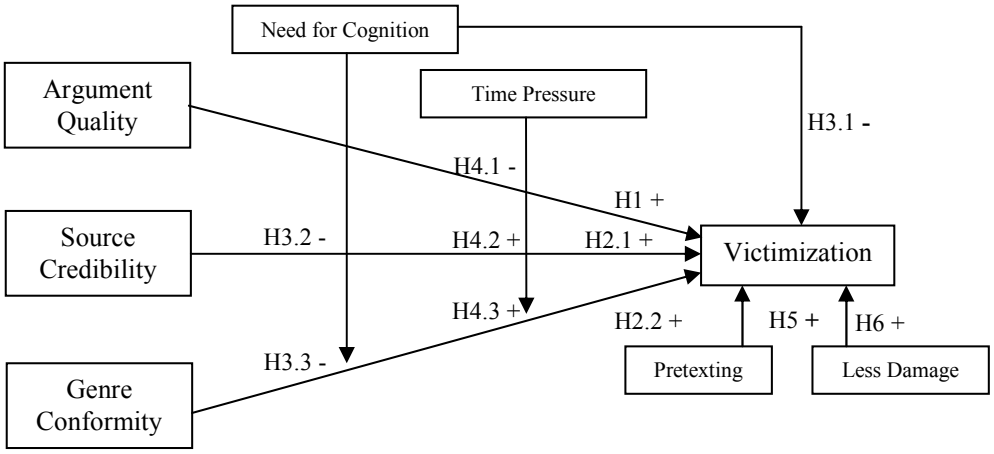

Figure 2. Proposed research model

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" [17]. Serving as templates for communications, they represent the association between communication formats and communication purposes [31], and help to improve communication efficiency and effectiveness.

For example, as businesses communicate with their customers electronically over time they develop certain communication genres for certain communication purposes. Especially, the email and/or message templates frequently used by businesses when sending mass communications to customers further reinforce the development and use of such genres. Phishing offenders can abuse these genres by forging their messages to resemble legitimate messages and bias the recipients into believing the validity of the messages [32]. An example is shown in Figure 3, 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. This figure shows the email message used in one the studies described in the paper introduction.

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., [25] [33]). 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 dispositions to engage in effortful cognitive activities [3] [[19]. Previous research suggested that people with 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 fallacy of phishing messages, 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.

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

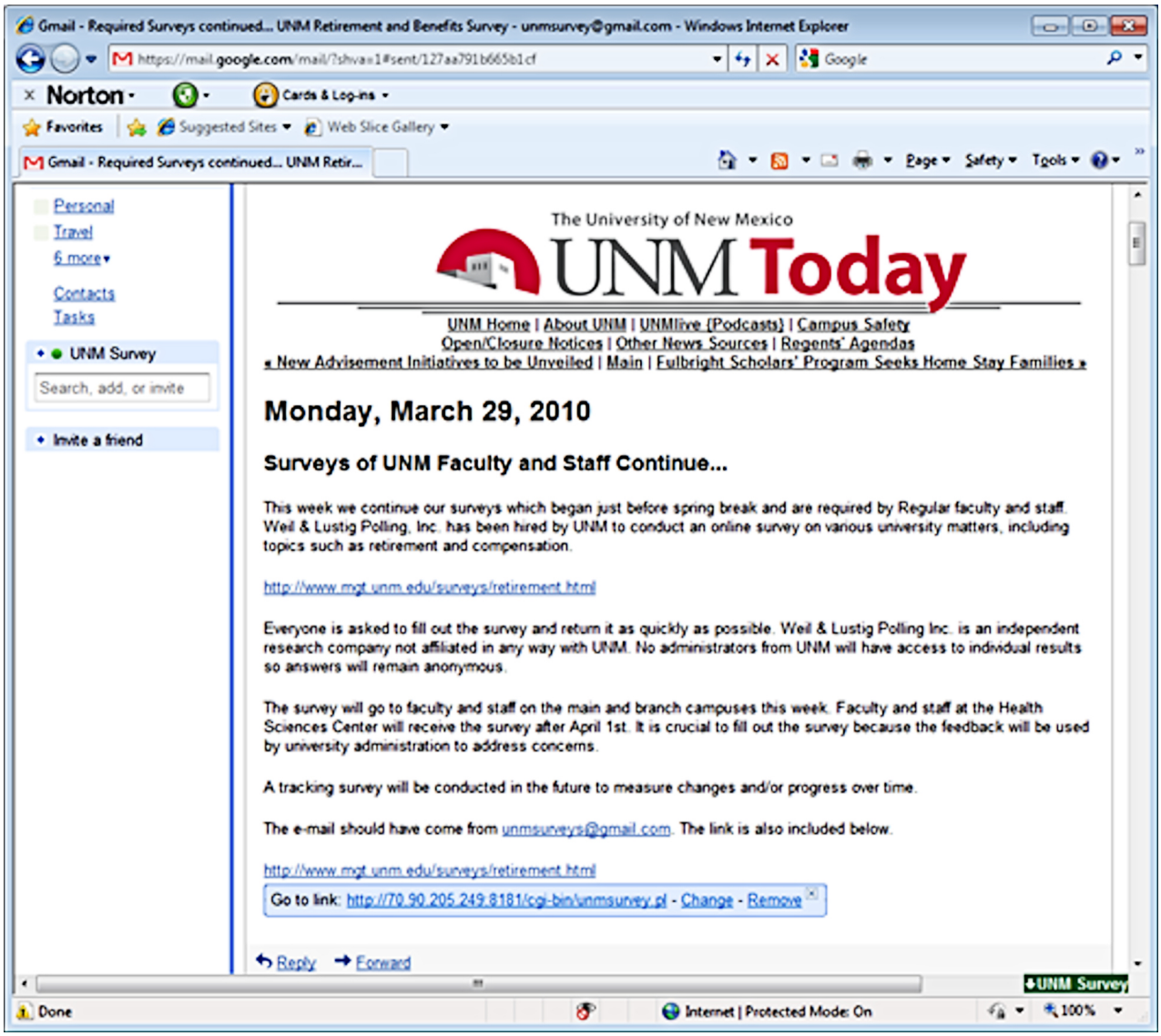

Figure 3. A phishing message demonstrating genre conformity

Systematic processing demands time and cognitive resources. If message recipients are distracted, or are pressed for time, systematic processing will be suppressed. Some phishing attacks attempt to exaggerate the urgency of the situation and press the message recipients into actions 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

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

atypical or in violation of company policies otherwise [15].

In the context of phishing, pretexting may be difficult to design, but it may simply be the result of coincidences: a company may have experienced an email system failure just before their employees received phishing messages asking for their email account information. Either way, we argue that pretexting can lower 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:

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

5. Research Method and Applications

The research model presented in Figure 2, of course, is preliminary. The constructs and hypotheses, therefore, need to be further developed, refined, and operationalized to enhance their rigor and appropriateness for further parsimonious investigations. Both qualitative and quantitative data will be collected to test the final research model and hypotheses. Qualitative data collected through field observations and interviews will allow us to gain more first-hand insights into the phishing attacks and the messages they use, and provide us with the opportunity to verify our theoretical reasoning and refine it.

Quantitative data collected through scenario-based surveys, on the other hand, will allow us to test the hypotheses in a positivist way. Through triangulating the findings from both studies, we can gain more confidence in the validity of the findings and hope to present scientifically rigorous outcomes in the near future.

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.

6. Conclusions

In this article we propose a study of victimization by phishing based on HSM. Through this 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 hope to test it in a new research context, and potentially advance this popular theory. We are also optimistic that the results 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.

7. References

[1] J.L. Aaker and D. Maheswaran, The effect of cultural orientation on persuasion. journal of Consumer Research, 24, 315-328.

[2] I. Bose and A.C.M. Leung, “Assessing Anti-phishing Preparedness: A Study of Online Banks in Hong Kong,” Decision Support Systems, 45 (2008), pp. 897-912.

[3] J.T. Cacioppo and R.E. Petty, "The Need for Cognition," Journal of Personality and Social Psychology, volume 42:1(1982), pp. 116-131.

[4] S. Chen and S. Chaiken, The Heruistic-Systematic Model in Its Broader Context, in Dual Process Theories in Social Psychology, Eds. S. Chaiken and Y. Trope, Guilford Press, 1999.

[5] X. Chen, I. Bose, A.C.M. Leung, and C. Guo, “Assessing the Severity of Phishing Attacks: A Hybrid Data Mining Approach,” Decision Support Systems, 50 (2011), pp. 662-672.

[6] A.H. Eagly and S. Chaiken, The Psychology of Attitudes. Orlando, FL: Harcourt, Brace, & Janovich, 1993.

[7] L.R. Fabrigar, J.R. Priester, R.E. Petty, and D.T. Wegener (1998), The impact of attitude accessibility on cognitive elaboration of persuasive messages. Personality and Social Psychology Bulletin, 24, 339-352.

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.

[8] M. Fishbein and S. Middlestadt, Noncognitive effects on attitude formation and change: Fact or artifact? Journal of Consumer Psychology, 2, 181-202.

[9] D.M. Frías, M.A. Rodríguez, and J.A. Castañeda, Internet vs. travel agencies on pre-visit destination image formation: An information processing view, Tourism Management, vol. 29 (2008), pp. 163-179.

[10] B. Hilligoss and S.Y. Rieh, Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context, Information Processing and Management (2007), doi:10.1016/j.ipm.2007.10.001.

[11] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer, Social Phishing, Communications of the ACM, volume 50:10 (October, 2007).

[12] D. Maheswaran and S. Chaiken (1991), Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. journal of Personality and Social Psychology, 61, 13-25.

[13] D. Maheswaran, D.M. Mackie, and S. Chaiken (1992), Brand name as a heuristic cue: The effects of task importance and expectancy confirmation on consumer judgments. Journal of Consumer Psychology, 1, 317-336.

[14] M. Metzger, 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, volume 58:13 (2007), pp. 2078–2091.

[15] K.D. Mitnick and W.L. Simon, The Art of Deception: Controlling the Human Element of Security. Indianapolis, Ind.: Wiley Publishing, Inc., 2002.

[16] A. Newell and H.A. Simon, Human Problem Solving, Prentice-Hall, 1972.

[17] W.J. Orlikowski and J. Yates, "Genre Repertoire: The Structuring of Communicative Practices in Organizations," Administrative Science Quarterly, volume 39(1994), pp. 541-574.

[18] A. Patrick, S. Marsh, and P. Briggs, Designing Systems That People Will Trust, in Security and Usability: Designing Secure Systems That People Can Use, National Research Council Canada, January, 2005.

[19] R.E. Petty and J.T. Cacioppo, J.T., Communication and Persuasion. New York: Springer-Verlag, 1986.

[20] R.E. Petty and D.T. Wegener, The Elaboration Likelihood Model: Current Status and Controversies, in Dual Process Theories in Social Psychology, Eds. S. Chaiken and Y. Trope, Guilford Press, 1999.

[21] PhiskTank, Phishing statistics for April 2011, http://www.phishtank.com/stats/2011/04, downloaded on June 14, 2011.

[22] A. Rothman and C.D. Hardin (1997), Differential use of the availability heuristic in social judgment. Personality and Social Psychology Bulletin, 23, 123-138.

[23] S.A. Sloman, The empirical case for two systems of reasoning. Psychological Bulletin, 119, 3-22.

[24] S.S. Sundar, The MAIN Model: A Heuristic Approach to Understanding Technology Effects on Credibility. Digital Media, Youth, and Credibility. Edited by Miriam J. Metzger and Andrew J. Flanagin. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, 2008. 73–100. doi: 10.1162/dmal.9780262562324.073.

[25] S.W. Sussman and W.S. Siegal, "Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption," Information Systems Research vol. 14:1 (2003), pp. 47-65.

[26] USLegal.com, Phishing definition, http://definitions.uslegal.com/p/phishing, downloaded on June 14, 2011.

[27] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," Decision Support Systems, volume 51 (2011), pp. 576-586.

[28] W. Wirth, T. Böcking, V. Karnowski, and T. von Paper, Heuristic and Systematic Use of Search Engines, Journal of Computer-Mediated Communication, vol. 12 (2007), pp. 778-800.

[29] M. Workman, "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, volume 59:4, (2008), pp. 662-647.

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

[31] J. Yates, W.J. Orlikowski, and K. Okamura, "Explicit and Implicit Structuring of Genres in Electronic Communication: Reinforcement and Change of Social Interaction," Organization Science, volume 10:1(1999), pp. 83-117.

[32] W. Zhang and S. Watts, "Knowledge Adoption in Online Communities of Practice," ICIS 2003, Seattle.

[33] W. Zhang and S. Watts, Capitalizing on Content: Information Adoption in Two Online Communities," Journal of Association of Information Systems volume 9:2 (2008), pp. 73-94.

Authorized licensed use limited to: California Polytechnic State University San Luis Obispo. Downloaded on April 27,2022 at 02:51:04 UTC from IEEE Xplore. Restrictions apply.