Assessment of Cybersecurity Knowledge and Behavior: An Anti-phishing Scenario

Ping An Wang
Department of Cybersecurity and Information Assurance, Graduate School
University of Maryland University College
Adelphi, Maryland, USA
Email: pwang2050@yahoo.com

***Abstract* – This paper focuses on the cybersecurity risk of online phishing and anti-phishing solutions to study user knowledge of phishing risks and intention to use anti-phishing solutions. Online phishing has become a major avenue for cyberattacks and a common cause for identity theft and financial losses. The availability of online security and anti-phishing solutions has been on the rise. However, there has been little research focus and consensus on assessing the effect of users' knowledge of cybersecurity risks and technology solutions on their acceptance and adoptions of cybersecurity solutions. This study proposes a novel model of assessment of users' cybersecurity knowledge and acceptance, which consists of both direct objective assessment and indirect self-assessment. The research model is designed to evaluate the relationship between online users' technical knowledge and competence in cybersecurity risks (i.e., online phishing risks) and their behavioral intention to use cybersecurity (i.e., anti-phishing) technology solutions. This study employs a survey method that measures end users' knowledge and competence of anti-phishing techniques and their intention to adopt and use anti-phishing solutions. Statistical analysis of the data collected suggests a positive correlation between users' technical knowledge of online phishing risks and solutions and their intention to adopt and use anti-phishing solutions. A positive correlation also appears between the direct assessment answers and self-assessment responses.**

Keywords-cybersecurity; phishing; knowledge; assessment

I. INTRODUCTION

Cybersecurity risks such as online phishing, have become an increasingly significant issue for information technology (IT) end users. Online phishing is a common cybersecurity attack targeting unsuspecting users and victims who are lured into clicking a spoofed universal resource locator (URL) or fraudulent email attachments or links pointing to a rogue Web page to give away their sensitive personal and financial information. The latest Phishing Activity Trends Report released by Anti-phishing Working Group (APWG) shows that attacks targeting consumers have remained at high levels with hundreds of phishing websites established online every day to lure online users to trouble and loss [1]. A recent report from security firm Trend Micro also confirms that 91 percent of cyberattacks now start with spear phishing, a special type of phishing targeting specific individuals [2].

There have been considerable efforts from cybersecurity industry and experts to make countermeasures and technology solutions available to detect, prevent, and minimize losses from cybersecurity attacks. Anti-phishing technology solutions do exist, which include anti-phishing features built in web browsers and protection against phishing in commercial software from cybersecurity vendors, such as Symantec. However, the latest CSI Computer Crime and Security Survey report indicates a consistently small investment and effort in end user cybersecurity awareness training for several years [3]. Meanwhile, users' adoption and actual use of cybersecurity solutions have been relatively low and not commensurate with the severity level of their perceptions and concerns about cybersecurity risks [4, 5]. Thus, it is vital to assess end users' knowledge of cybersecurity risks and the key factors in users' decision on adopting and using cybersecurity solutions.

Human capital and cybersecurity knowledge are the essential factors for achieving technical competence in the general cybersecurity competency model [6]. Knowledge is the contextual and high-value form of information and experience ready to apply to decisions and actions [7]. Research findings have indicated IT users' lack of knowledge and clear understanding of cybersecurity solutions, including protections against phishing, unwanted tracking of their online activities, and potential leak of sensitive personal information [8, 9, 10]. However, there has been little research on user acceptance of cybersecurity solutions from the knowledge perspective. Most of the prior studies on technology acceptance focused on new technologies in general and the constructs of user perceptions of usefulness and ease of use as determinants of user attitude and behavioral intention toward technology adoption. These studies were primarily based on the technology acceptance model (TAM) and the theory of planned behavior (TPB). The research model proposed in this study focuses on the relationship between the assessment of user knowledge of cybersecurity and user attitude and intention toward adopting and using cybersecurity solutions.

Empirically, this study uses a behavioral survey method to assess users' knowledge and attitude and intention regarding cybersecurity (i.e., anti-phishing) technology solutions. The findings suggest that user knowledge is positively associated with user acceptance of and intention to use in the domain of cybersecurity (i.e., anti-phishing) technology.

There are six sections in this paper. Section I introduces the paper and the motivation for the study. Section II explains the research goals and discusses relevant theoretical background. Section III presents the research model. Section IV explains the survey-based methodology used for this study. Section V presents the results and data analysis. Section VI concludes the paper with findings, implications, and possible follow-up research.

II. RESEARCH GOALS AND BACKGROUND

The goal of this research is to use the anti-phishing scenario to assess end user knowledge of cybersecurity risks and solutions and uncover the relationship between user knowledge and user acceptance of cybersecurity solutions. Knowledge includes contextual information, awareness, and personal experience ready to be used for decisions and actions. Knowledge consists of both explicit knowledge or communicable information and tacit knowledge, which is personal and intuitive insights and know-how originated from individual experiences and values [11]. One’s attitude is a determining factor of one’s behavioral intention that predicts one’s actual behavior [12]. User knowledge of online security risks and protective and preventive solutions was found to be an important factor affecting user attitude and trust in online vendors in the e-commerce domain [13, 14]. Thus, users’ knowledge of cybersecurity may be a predictor of their attitude and intention that are essential to their acceptance of security solutions. This research study primarily explores the relationship between user knowledge of cybersecurity and user acceptance of cybersecurity solutions. In addition, this study attempts to address the question of how to properly assess user knowledge of cybersecurity risks and technology.

A. Attitudinal Theories on Cybersecurity Knowledge

A large amount of prior research on cybersecurity knowledge was based on attitudinal theories involving users’ perceptions of online risks and behavioral intentions. The conceptual assumption of such models was based on the theory of reasoned action (TRA). In TRA, behavioral intentions are antecedents to individual behavior, and intention is determined by attitudes and perceptions [12]. Accordingly, one’s perception and attitudes regarding online risks will have an influence on attitudes toward online transactions and in turn, affect his or her behavioral intentions to conduct online transactions.

Several studies used attitudinal theories to study how risk perceptions affect a dependent variable such as trust, purchase intention, and etc. These studies include Bhatnagar et al. [15], Miyazaki and Fernandez [16], Salisbury et al. [17], Pavlou [18], Milne et al. [19], Dinev and Hu [20], Jiang et al. [14], and Tsai et al. [21]. Knowledge in these studies generally refers to experience, maturity of subject, user awareness in a general sense, and familiarity with a task or risks in the online purchase environment.

The primary interest of these attitudinal studies was in user perceptions of online risks and intention to purchase online. Their common assumption is that people’s decisions under risks are driven by inconsistent perceptions, beliefs, and emotions. Such an assumption does lend support for the suggestion that users’ self-assessment of knowledge may have an impact on their behavior and decision making. However, the attitudinal studies have two major limitations: a) no focus on the assessment of user knowledge of cybersecurity risks and solutions; b) no focus on the relationship between cybersecurity knowledge assessment and intention to adopt cybersecurity technology solutions. This research attempts to address these limitations.

B. Psychometric Theories on Cybersecurity Knowledge

The psychometric paradigm is an important approach to the knowledge dimension of risk studies even though such research on online security risks has been limited. The psychometric paradigm uses multivariate techniques to recover cognitive maps of decision makers’ risk perceptions and attitudes so as to understand the dimensions of risk and the cognitive schema [22]. Fischhoff et al. studied technological risks and benefits using the psychometric paradigm with some inclusion of knowledge of risks, but the study did not address the relationship between risks and technology acceptance [23]. Slovic, Fischhoff, and Lichtenstein found that risk acceptability is affected by risk attributes, such as familiarity with the level of risk [22]. They equated the concept of knowledge of risk to people’s familiarity with the level of risk. However, the study did not address the assessment of cybersecurity knowledge or user acceptance of online security technology solutions.

Slovic further elaborated the psychometric approach to the study of risk perceptions and suggested that the level of knowledge attribute seems to influence the relationship between perceived risk, perceived benefit, and risk acceptance [24]. However, he did not clearly define the concept of knowledge and did not include cybersecurity knowledge and technology acceptance in the study.

Nyshadham and Ugbaja used the techniques of the psychometric paradigm to study how B2C e-commerce consumers organize novel online risks in memory. The study called for further analysis to define the risk dimensions [25]. Using the psychometric paradigm, Gabriel and Nyshadham studied perceptions of online risks that affect online purchase intentions [26]. The study contributed a valuable taxonomy of online risks and a cognitive map of online consumers’ risk perceptions and attitudes. This is a positive step toward recognizing the knowledge dimension in user perceptions of online risks in general. However, there was no focus on cybersecurity risks and technology acceptance in the study.

C. Knowledge and Technology Acceptance

Prior literature on user knowledge and acceptance of cybersecurity solutions was primarily based on TPB and TAM. TPB considers user attitude, perceived social norm, and perceived behavioral control to be the factors determining user behavioral intention that predicts actual user behavior of adopting technology solutions [27]. TPB was the theoretical basis for the anti-spyware adoption model [4]. However, the model did not address the user knowledge factor. Another study on user attitude toward spyware and anti-spyware technologies was based on TPB and TAM [28]. In addition to the three TPB constructs, the TAM constructs of perceived usefulness and perceived ease of use were included as predictors of user attitude and behavior toward anti-spyware solutions. The study did include computer knowledge and awareness of spyware as predictors of user action. However, neither the construct of knowledge nor its role in the TPB model was clearly defined or assessed. Also, these two studies on spyware focused on anti-spyware technology, without addressing phishing risks and anti-phishing solutions.

A later study on protective information technologies based on an extended model of TPB attempted to address user behavioral intention toward cybersecurity technology in general [20]. The extended TPB model dropped the perceived usefulness and perceived ease of use factors and emphasized user awareness as a key determinant of user intention toward adopting protective information technologies. However, as acknowledged by the study itself, the awareness construct was not specific. The survey approach used by the study was also limited to questions on spyware and anti-spyware solutions.

A different theoretical approach to user acceptance of cybersecurity solutions was based on the Protection Motivation Theory (PMT) [29]. The PMT model argues that one’s fear appeals affect the motivation to protect oneself from potential harm. The study concluded that perceived vulnerability, perceived severity, response efficacy, and response cost influence individual behavioral intention to adopt anti-spyware protective technology. However, the PMT model did not address the user knowledge factor or assessment of user knowledge of cybersecurity. Subsequent studies by Wang [30] and Wang and Nyshadham [31] contributed more in-depth definitions of the user knowledge constructs regarding online risks, but their studies focused on the effect on online purchase intentions and decisions with little emphasis on intentions to adopt online security technology solutions.

III. RESEARCH MODEL

Based on the review of the existing research above, this study proposes a new model of technology acceptance to address user acceptance of cybersecurity solutions from the knowledge assessment perspective. This model, shown in Fig. 1, extends the traditional TAM theory to include and focus on the knowledge assessment factor in determining user attitude and intention in the specific anti-phishing cybersecurity context. Knowledge management theory defines knowledge as the contextual and high-value form of information and experience that positively affect decisions and actions [32]. User knowledge in this study includes explicit contextual information and awareness as well as tacit personal experience and technical know-how. In terms of basic knowledge of anti-phishing solutions, users should be aware of and look for the https secure protocol in the URL for a secure website as shown in a sample secure URL in the browser window in Fig. 2. As an indicator of more in-depth knowledge of anti-phishing technology, users should look for a valid security certificate for a secure website as shown in Fig. 3.

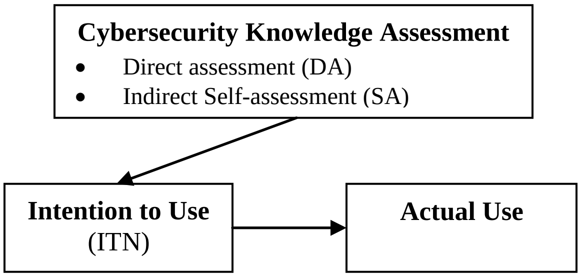

Cybersecurity Knowledge Assessment
• Direct assessment (DA)
• Indirect Self-assessment (SA)
Intention to Use
(ITN)
Actual Use

Figure 1. Research Model

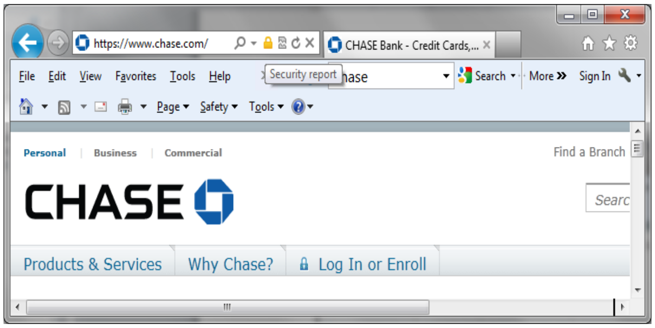
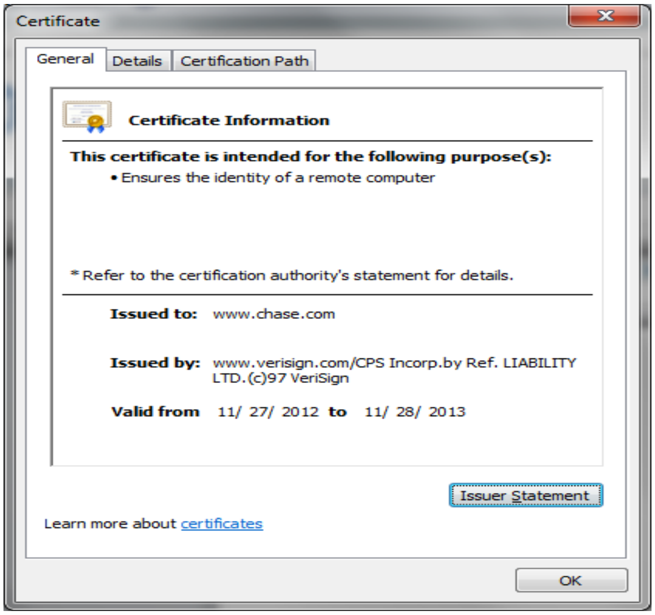


Figure 2. Secure non-phishing URL with https protocol

Assessment of knowledge is a process of measuring and comparing learning expectations and actual learning outcomes [33]. Knowledge assessment in information technology areas can include both direct assessment, such as objective tests and projects, and indirect assessment, such as perceptions and self-assessment (or self-evaluation), and in evaluating the outcomes of technical knowledge and skills both direct and self-assessment methods can work together with positive correlation in results [34]. Accordingly, in assessing user knowledge of phishing risks and anti-phishing technology solutions, objective test questions on technical indicators for secure websites can be used as direct assessment, along with indirect self-assessment questions for users to present their perceptions and self-evaluations of their anti-phishing knowledge and skills.



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.chase.com

Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Valid from 11/ 27/ 2012 to 11/ 28/ 2013

Figure 3. Valid certificate for a non-phishing website

User acceptance refers to user's positive attitude and intention toward using the cybersecurity solutions they know. One's attitude, according to TRA and TAM, determines one's behavioral intention which in turn predicts one's actual behavior. Therefore, the research model proposes that user knowledge of cybersecurity risks and solutions is positively related to user attitude and intention toward using cybersecurity solutions.

TAM has been a traditional model for studying computer usage behavior and acceptance of information technology in general. However, to focus on the knowledge variable, the research model in this study does not include the TAM constructs of perceived usefulness (PU) and perceived ease of use (POEU). The awareness (a component of knowledge) of the consequences of not using cybersecurity technologies is more significant than PU and POEU in affecting user attitude and intention [20]. The constructs of intention to use and actual use are defined according to TAM constructs [35]. Intention to use measures the strength of one's decision to perform the action or behavior of using the cybersecurity technology. Actual use refers to the actual action or behavior of using the cybersecurity technology.

IV. METHODOLOGY

To test the research model, an anonymous questionnaire-based survey was conducted among 210 randomly selected undergraduate students of various majors at a college in the northeast of the United States. The assumption for such randomization is that students of certain technical majors may have more cybersecurity background than those of non-technical majors. Self-report survey question format has been an effective method for eliciting attitudinal responses [36]. The survey for this study utilized a seven-point Likert scale of responses ranging from 7=Strongly Agree to 1=Strongly Disagree.

There are eight content questions related to user knowledge of phishing risks and anti-phishing technology solutions. The content of the questions is based on some common phishing risks and solutions for online activities and transactions. The first four questions in the survey are direct assessment questions expecting factual answers from the subjects to measure their knowledge of phishing risks and essential anti-phishing technology. Questions 5 through 7 are indirect self-assessment questions to elicit the respondents' self-evaluation of their knowledge of phishing risks and anti-phishing solutions. Question 8 was designed to be the dependent variable that measures the subjects' acceptance of and intention to use anti-phishing technology. Additional questions on demographics, such as gender, and age group, years of using computers, average Internet usage, were included in the survey. The eight questions for the survey are as follows:

1. I am aware that online phishing may lead to personal identity theft and financial losses.
2. I am aware of at least one solution to protect against online phishing.
3. https is an important protocol to look for in a secure web address.
4. Before giving my credit card number to an online vendor, I will look for a valid certificate to certify that the vendor web site is secure.
5. I will not likely accept email invitations from an unfamiliar source to give out my personal account information.
6. I am well informed about online phishing risks.
7. I am well informed about anti-phishing technology.
8. I intend to use effective protection technology against online phishing on a regular basis.

The questionnaire was pilot-tested among 15 students. Minor changes in wording were made prior to the formal distribution and administration of the final survey. The survey was distributed to a total of 210 students. The student participation in the survey was declared anonymous and voluntary, and a total of 186 responses were received. 14 responses were eliminated for missing data. A final total of 172 responses were used for data analysis. The next section presents the findings and discussions.

V. FINDINGS AND DISCUSSIONS

Demographic data collected from the subjects included gender, age group, years of using computers, and average Internet usage. The data show that all subjects had at least two years of experience of using computers. Over 85% of the subjects use the Internet between 1 and 6 hours per day;

and over 78% of the subjects have used the Internet for four or more years. The age of the subjects falls between 18 and 56, including 55.7% in age 18-21, 32.4% in age 22-30, 8.9% in age 31-40, 2.3% in age 41-50, and 0.7% above the age of 50. 55% of the subjects were female while 46% were male. The data are close to the general demographics of the student population at the surveyed institution.

SPSS version 18.0 for Windows was used for statistical analysis of the data collected. The reliability analysis of the survey instrument and the Pearson correlations among the eight variables are presented in Table 1 and Table 2 below. The seven independent variables include four Direct Assessment questions (coded as DA1, DA2, DA3, and DA4 represented by questions 1-4 in the survey) and three Indirect Self-assessment questions (coded as SA1, SA2, and SA3 represented by questions 5-7 in the survey). ITN stands for the Intention to Use, which is the dependent variable represented by question 8 in the survey. The valid responses collected were entered into SPSS for reliability and correlations analysis. The analysis reports are presented in TABLE 1 and TABLE 2. The Cronbach's Alpha coefficient is an effective measure of internal consistency reliability, and coefficient values over 0.80 indicate good internal consistency reliability [37]. The Cronbach Alpha values for the four construct items in this study, as shown in Table 1, are all above 0.80 among the eight variables. Therefore, the measures used in this study are considered to have good internal consistency reliability. Discriminant validity of measures is achieved if correlations between any pair of latent constructs are significantly less than 1.00 [38]. The Pearson correlations among the variables shown in Table 2 are significantly less than 1.00. Thus, the measures in this study have demonstrated considerable discriminant validity. In addition, the pilot test of the survey instrument and necessary revisions made in the wording of the survey questions were also helpful in improving the content validity of the questionnaire.

TABLE 1: RELIABILITY STATISTICS

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.803	.803	8

TABLE 2: PEARSON CORRELATIONS

	DA1	DA2	DA3	DA4	SA1	SA2	SA3	ITN
DA1	1	.167*	.337**	.274**	.220*	.277**	.312**	.343*
DA2	.167*	1	.319**	.394**	.372**	.208**	.293**	.349**
DA3	.337**	.319**	1	.552**	.325**	.349**	.420**	.544**
DA4	.274**	.394**	.552**	1	.262*	.310**	.305**	.354**
SA1	.220*	.372**	.325**	.262*	1	.312**	.332**	.260*
SA2	.277**	.208**	.349**	.310**	.312**	1	.263*	.292**
SA3	.312**	.293**	.420**	.305**	.332**	.263*	1	.554**
ITN	.343*	.349**	.544**	.354**	.260*	.292**	.554**	1

*. Correlation is significant at the 0.05 level (two-tailed).
**. Correlation is significant at the 0.01 level (two-tailed).

The Pearson correlation results shown in Table 2 indicate support for the research model of this study. The Pearson correlation coefficient is appropriate for interval-scaled measures [37]. The results in the correlations matrix in Table 2 indicate a significant positive relationship between end users' cybersecurity knowledge (via direct assessment and indirect self-assessment) and their intention to use cybersecurity technology solutions. The results also show significant and positive correlations between the Direct Assessment variables and the Indirect Self-assessment variables, which indicates support for the cybersecurity knowledge assessment construct in the research model proposed in this study.

VI. CONCLUSION

This study focuses on the relationship between assessment of users' knowledge of cybersecurity risks and solutions (i.e., phishing risks and anti-phishing solutions) and their attitude and intention toward adoption and use of cybersecurity solutions. Based on the anti-phishing scenario, a novel and simplified technology acceptance model was proposed and tested using a survey study including independent variables of both direct assessment and indirect self-assessment of cybersecurity knowledge. The findings indicate support for the proposition that users' cybersecurity (i.e., phishing) knowledge is positively related to their attitude and intention toward adopting and using cybersecurity (anti-phishing) solutions. The research data also indicate a positive correlation between the direct assessment method and the indirect self-assessment method in evaluating users' cybersecurity knowledge. This correlation may point to the valid practice of including both direct and indirect assessment methods in cybersecurity knowledge training.

User acceptance and adoptions of cybersecurity technology solutions is an emerging and significant area for researchers and the business community. This study contributes a new model of cybersecurity knowledge assessment and user acceptance of cybersecurity solutions. The study also adds valuable data to the study of online phishing risks and user acceptance of anti-phishing solutions. This study has some important practical implications as well. Cybersecurity technology solution vendors need to heed user knowledge level in marketing their products and services. Improving user training and knowledge level may lead to higher levels of acceptance and adoptions of cybersecurity solutions. It is also an opportunity and social responsibility for educational institutions to provide more effective cybersecurity (i.e., anti-phishing) programs and courses to improve user knowledge of cybersecurity risks and cybersecurity technology solutions. In terms of assessing cybersecurity knowledge, the study suggests that direct and objective assessment method can be as equally effective as indirect self-assessment method. Therefore, cybersecurity training programs may consider using both direct assessment and indirect assessment questions in evaluating users' knowledge and competency.

There are promising follow-up research opportunities to pursue this study further. This study focused on the effect of the direct and indirect cybersecurity knowledge variables on user intention to use cybersecurity solutions using samples of general users. Further studies can be conducted among users of different levels of cybersecurity experience and include additional variables, such as specific variables on user experience in online security risks and resolutions as well as effectiveness in communication of cybersecurity risks and solutions. This study is based on the specific area of phishing risks and anti-phishing solutions. Future studies can be done on other cybersecurity topics, such as malware risks and anti-malware solutions, botnets, or the emerging cloud security risks and solutions. In addition, using a larger sample size and a more comprehensive assessment process than those used in this study may produce more informative and conclusive data.

REFERENCES

[1] Phishing Activity Trends Report (2nd Qtr 2012), Published by Anti-phishing Working Group (APWG) at http://www.apwg.org, retrieved: April, 2013.

[2] A. Savvas, "Spear phishing the main email attachment threat," from https://www.networkworld.com/news/2012/112912-39spear-phishing39-the-main-email-264621.html, retrieved: April, 2013.

[3] 2010/2011 Computer Crime and Security Survey, Published by Computer Security Insitute (CSI).

[4] Y. Lee and K. A. Kozar, "An empirical investigation of anti-spyware software adoption: A multi-theoretical perspective," Information & Management, vol. 48, 2008, pp. 109-119.

[5] Q. Yeh and A. J. Chang, "Threats and countermeasures for information system security: A cross-industry study," Information & Management, vol. 44, 2007, pp. 480-491.

[6] Cybersecurity Human Capital (November 2011). Published by United States Government Accountability Office (GAO) at http://www.gao.gov/products/GAO-12-8, retrieved: April, 2013.

[7] T. H. Davenport, D. De Long, and M. Beers, "Successful knowledge management," Sloan Management Review, vol. 39, 1998, pp. 43-57.

[8] S. M. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal Internet users," Computers & Security, vol. 26, 2007, pp. 410-417.

[9] L. F. Cranor, "Can users control online behavioral advertising effectively?", IEEE Security & Privacy, vol. 10, no. 2, March/April 2012, pp. 93-96.

[10] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," CHI 2013, February 2013, pp. 1-11.

[11] K.Desouza,"Facilitating tacit knowledge exchange," Communications of the ACM, vol. 46, June 2003, pp. 85-89.

[12] M. Fishbein and I. Ajzen, Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley, 1975.

[13] B. Suh and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," International Journal of Electronic Commerce, vol. 7, Spring 2003, pp. 135-161.

[14] J. Jiang, C. Chen, and C. Wang, "Knowledge and trust in e-consumers' online shopping behavior," International Symposium on Electronic Commerce and Security, 2008, pp. 652-656, doi: 10.1109/ISECS.2008.117.

[15] A. Bhatnagar, S. Misra, and H.R. Rao, "On risk, convenience, and internet shopping behavior," Communications of the ACM, vol. 43, no. 11, 2000, pp. 98-105.

[16] A. D. Miyazaki and A. Fernandez, "Consumer perceptions of privacy and security risks for online shopping," The Journal of Consumer Affairs, vol. 35, no. 1, 2001, pp. 27-44.

[17] W. D. Salisbury, R. A. Pearson, A. W. Pearson, and D. W. Miller, "Perceived security and World Wide Web purchase intention," Industrial Management & Data Systems, vol. 101, no.4, pp. 165-176.

[18] P. A. Pavlou, "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model," International Journal of Electronic Commerce, vol. 7, no. 3, 2003, pp. 69-103.

[19] G. R. Milne, A. J. Rohm, and S. Bahl, "Consumers' protection of online privacy and identity," The Journal of Consumer Affairs, vol. 38, no.2, pp. 217-232.

[20] T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," Journal of the Association for Information Systems, vol. 8, July 2007, pp. 386-408.

[21] J. Tsai, L. Cranor, S. Egelman, and A. Acqusiti, "The effect of online privacy information on purchasing behavior: An experimental study," Proceedings of the Twenty Eighth International Conference on Information Systems, Montreal, Canada, 2007, pp. 1-17.

[22] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Why study risk perception?" Risk Analysis, vol. 2, no. 2, 1982, pp. 83-93.

[23] B. Fischhoff, P. Slovic, and S. Lichtenstein, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," Policy Sciences, vol. 9, no. 2, 1978, pp. 127-152.

[24] P. Slovic, "Perception of risk," *Science*, no. 236, 1987, pp. 280-285.

[25] E. A. Nyshadham and M. Ugbaja, "A study of ecommerce risk perceptions among b2c consumers: A two country study," Proceedings of the 19th Bled eConference, Bled, Slovenia, 2006.

[26] I. J. Gabriel and E. Nyshadham, "A cognitive map of people's online risk perceptions and attitudes: An empirical study," Proceedings of the 41st Annual Hawaii International Conference on Systems Sciences, January 2008, pp. 274-283.

[27] I. Ajzen, Attitudes, Personality, and Behavior, Chicago, IL: The Dorsey Press, 1988.

[28] Q. Hu and T. Dinev, "Is spyware an Internet nuisance or public menace?" Communications of the ACM, vol. 48, August 2005, pp. 61-66.

[29] T. Chenoweth, R. Minch, and T. Gattiker, "Application of protection motivation theory to adoption of protective technologies," Proceedings of the 42nd Hawaii International Conference on System Sciences, January 2009, pp. 1-10.

[30] P. Wang, "Information security knowledge and behavior: An adapted model of technology acceptance," 2nd International Conference on Educational Technology and Computer (ICETC), June 2010, pp. 364-367. DOI: 10.1109/ICETC.2010.5529366.

[31] P. Wang and E. A. Nyshadham, "Knowledge of online security risks and consumer decision making: An experimental study," Proceedings of the 44th Hawaii International Conference on System Sciences, January 2010, pp. 1-10.

[32] T. H. Davenport and L. Prusak, Working Knowledge: How Organizations Manage What They Know. Cambridge, MA: Harvard Business School Press, 1998.

[33] L. Suskie, Assessing Student Learning: A Common Sense Guide (2nd ed.). Hoboken, NJ: Wiley, John & Sons, Inc., 2009.

[34] P. Anderson, J. W. Merhout, J. Bernamati, and T. M. Rajkumar, "Are student self-assessments a valid proxy for direct assessments in information systems programs?" Proceedings of the Sixteenth Americas Conference on Information Systems, August 2010, pp. 1-8.

[35] F. D. Davis Jr., A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results. Ph.D. dissertation, Massachusetts Institute of Technology, Sloan School of Management, 1986.

[36] S. Grenier, A. Barrette, and R. Ladouceur, “Intolerance of uncertainty and intolerance of ambiguity: Similarities and differences,” Personality and Individual Differences, vol. 39, 2005, pp. 593-600.

[37] U. Sekaran, Research Methods For Business: A Skill Building Approach, 4th ed. Hoboken, NJ: John Wiley & Sons, Inc., 2003.

[38] M. Boudreau, D. Gefen, and D.W. Straub, “Validation in IS research: A state-of-the-art assessment” MIS Quarterly, vol. 25, 2001, pp. 1-16.