An Integrated Model of Individual Web Security Behavior

Journal:	*16th Americas Conference on Information Systems*
Manuscript ID:	AMCIS-0911-2010.R1
Submission Type:	Paper
Mini-Track:	Trust in Information Systems < HCI Studies in Information Systems (SIGHCI)

An Integrated Model of Individual Web Security Behavior

Li-Chiou Chen
Pace University
lchen@pace.edu

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

ABSTRACT

Most users find security-informed decisions hard to make while utilizing web sites for social networking, online banking, or shopping. In order to solve security problems, it is critical that we understand how human factors influence users' trust on web sites and users' decisions involving computer security related risk. We propose an integrative model of human factors on decisions involving online security risk. The model will provide a comprehensive view of the impact of the situation and personal factors on trust, perceived security risk and web site functionality from both internal and external perspectives. The proposed model will extend existing theories by studying the human factors in terms of internal intrinsic traits such as personality, culture, risk beliefs and extrinsic factors such as experience and familiarity. Similarly it will study internal situation factors such as website performance and utility, and external situation factors such as context.

Keywords

Perceived security risk, web security, individual decision making, trust, human factor.

INTRODUCTION

Human factors are often the weakest links of computer security but they are among the most important factors to consider in security design and security policy (Bresz 2004, Cranor 2008, Lineberry 2007). Security usability has been focused on designing security technologies that users can easily adopt (Cranor and Garnkel 2005, Whitten and Tygar 1999). However, most users still find security-informed decisions hard to make while utilizing web sites for social networking, online banking, or shopping. Therefore, in order to solve security problems, it is critical that we understand how human factors influence users' decisions involving computer security related risk.

This paper developed an integrative model of human factors on decisions involving online security risk. Using this model, we plan to study how do personal dispositions and user web experiences impact one's trusting beliefs, perceived security, and perceived utility, which then influence one's security decisions on the web. The model hypothesizes how human factors such as personality, culture, and web experiences directly impact end users' perceived security, trust and utility which may in turn influence their decision making online. End users' perceived online security risk often deviates from the actual risk. This deviation often leads users to misplace trust on untrustworthy websites and sources. The gap between their perceived risk and actual risk often results in inappropriate decisions for managing online risk. For example, a user who downloads free software from an arbitrary source on the web may not be aware of the spyware embedded in this free software. In this case, the user misplaces his/her trust on untrustworthy source by perceiving a lower security risk than the actual security risk of downloading the software.

It is important to build such an integrative model to enhance our understanding of individual web security behavior. While users are interacting with a web site, they often need to make various decisions regarding web security. For example, in the case of the spyware, users can decide not to download and install the free software. However, if the users decide to do so in spite of the warning from the spyware detection software on their machines, they are risking security in exchange of utility. An integrated model will be useful for understanding such tradeoff and the factors that may have the most impact on the users' security decision making. We are also expecting this integrated model will provide implications for developing web security countermeasures that address the human factors.

By reviewing literature, the next section will provide reasons why an integrated model of individual web security behavior is needed. Section 3 will describe our model and each of the constructs in the model. Section 4 will discuss implications and future empirical studies followed by conclusions.

THE NEED FOR A MODEL OF WEB SECURITY BEHAVIOR

Understanding the security decision making process -- the interplay between computer systems and end users: While interacting with a computer system, such as a web site, individuals often need to make various implicit or explicit decisions in order to utilize the functionality provided by the system. While making these decisions, users are often not aware of or ignore security implications. For example, in order to read morning news from a news web site, users are often asked to accept web cookies which may reveal their browsing history to a third party that the users are not aware of. Although web browsers can provide users some control over web cookies, users may have little understanding regarding the impact of their decisions or the tradeoff that they have just made. Our integrative model is set to understand how the users make the security decision tradeoff involving utility and security, while they are interacting with web sites. Utility is the measure of usefulness (e.g., information contents) and performance benefits (e.g., navigational ease) that a user derives from a website. The trade off involves decision between perceived security and perceived utility. Users may forgo perceived security for perceived utility, or vice versa. It is important to study perceived security, since it is one's perception which motivates one to transact with the website.

Aligning end users' trust with trustworthy systems: With the understanding of end user security decision making, the paper aims at discovering human factors that may influence the users' decisions. Based on the discovery, we will be able to design training that influence users' security behavior through these human aspects. For example, trusting belief has long been regarded as a driving factor in adopting e-commerce, designing a secure e-business portal that users will trust requires a technology not only securing the system but also informing users to make secure decisions and aligning their trust with actual system security. Our integrative model aims at developing a theoretical foundation that considers user awareness and training in realigning their trust belief through examining the technological cues.

Providing an integrated perspective of individual security decision making: Although previous studies have provided some empirical evidence on the determinants of user security behavior, it is necessary to develop a research model that incorporates users' perceptions and decision making process (Aytes and Connolly 2004, Lee et al. 2004). Our integrated model will take a further step that integrates various human factors, such as personality, culture, individual web experiences, and individual concerns/beliefs, into a proposed model of individual web security behavior which consider the impact of these factors on perceived security, trusting beliefs, perceived utility and secure decision making. Within an organizational context, Stanton et. Al (2005) has proposed a taxonomy of end user security behavior categorized by intention and expertise. This taxonomy is created based upon interview results of 110 information technology professionals and self-reports of password-related behaviors of 1167 end users. Based on Health Belief Model (Rosenstoick 1974), Ng and Xu have shown that perceived susceptibility (a user's perceived likelihood of a security incident taking place), perceived benefits (a user's belief in the perceived effectiveness of practicing computer security) and self-efficacy (a user's self-confidence in her/his ability of practicing computer security) are determinants of email related security behavior (Ng et al. 2009). Based on a study in password security within an organization, research has found two factors that lead to insecure behavior. These factors are users' lack of security awareness and security departments' lack of knowledge about users (Adams and Sasse 1999). Mental model approach has also been used to understand how users perceive computer security risk (Asgharpour et al. 2007).

AN INTEGRATED MODEL OF INDIVIDUAL WEB SECURITY BEHAVIOR

We propose an integrated model of individual web security behavior, depicted as in Figure 1. A "+" sign on an arrow refers to a hypothesized positive relationship between the two constructs while a "-" sign on the arrow refers to a hypothesized negative relationship. We propose that the actual web user behavior, such as purchasing a product, sending out personal information or downloading software, is positively influenced by the user's intention of transacting with a web site. The intention is influenced by three constructs: the user's perceived security risk (negative impact), trusting belief (positive impact) and perceived utility (positive impact). Individual concern and personal dispositions will have an indirect impact on the user's web security behavior through these three constructs. We also propose that end user security efficacy such as security skill and awareness will have a positive impact on their perceived security risk. Web context is a construct that will be used as a control variable manipulated in empirical studies. As it has been shown that user's behaviors are impacted by the underlying context. For example, users are less forthcoming in more sensitive contexts, and vice versa (Bansal et al. 2008b).

Perceived security risk: This construct refers to an individual's judgment of how risky a certain event is. We will measure this construct based on the individual's perceived probability of risk, perceived consequences and perceived control (security countermeasures). Understanding how humans perceive the exposure and the effects of risk is considered an important part of analyzing and managing technology-induced risk (Morgan 1981). However, risk perception of computer security has yet to be fully studied although the general perception of risk has been found to greatly impact individual computer decisions (Hardee et al. 2006). Research has empirically verified that higher perceived security control is positively related to trust in e-commerce web site (Chellappa and Pavlou 2002, Chen and Barnes 2007, Suh and Han 2003), users' intention of purchasing

(Bhatnagar et al. 2000, Ranganathan and Ganapathy 2002, Salisbury et al. 2001, Suh and Han 2003) and in online banking (Liao and Cheung 2002).

Perceived utility: In our model, perceived utility is defined as being comprised of the usefulness and performance of a web site as perceived by the users. Technology Acceptance Model (Davis 1989) and its application on e-commerce (e.g., Gefen et al. 2003a; 2003b) have provided empirical evidence that perceived usefulness has contributed positively to users' adoption of e-commerce. Basing our definition of usefulness and performance in terms of information quality and systems quality respectively (DeLone and McLean 1992, McKinney et al. 2002) we define usefulness in terms of information quality such as information content, discount offered, deals, etc. Performance on the other hand is defined in terms of performance in delivering information such as fast and easy navigation.

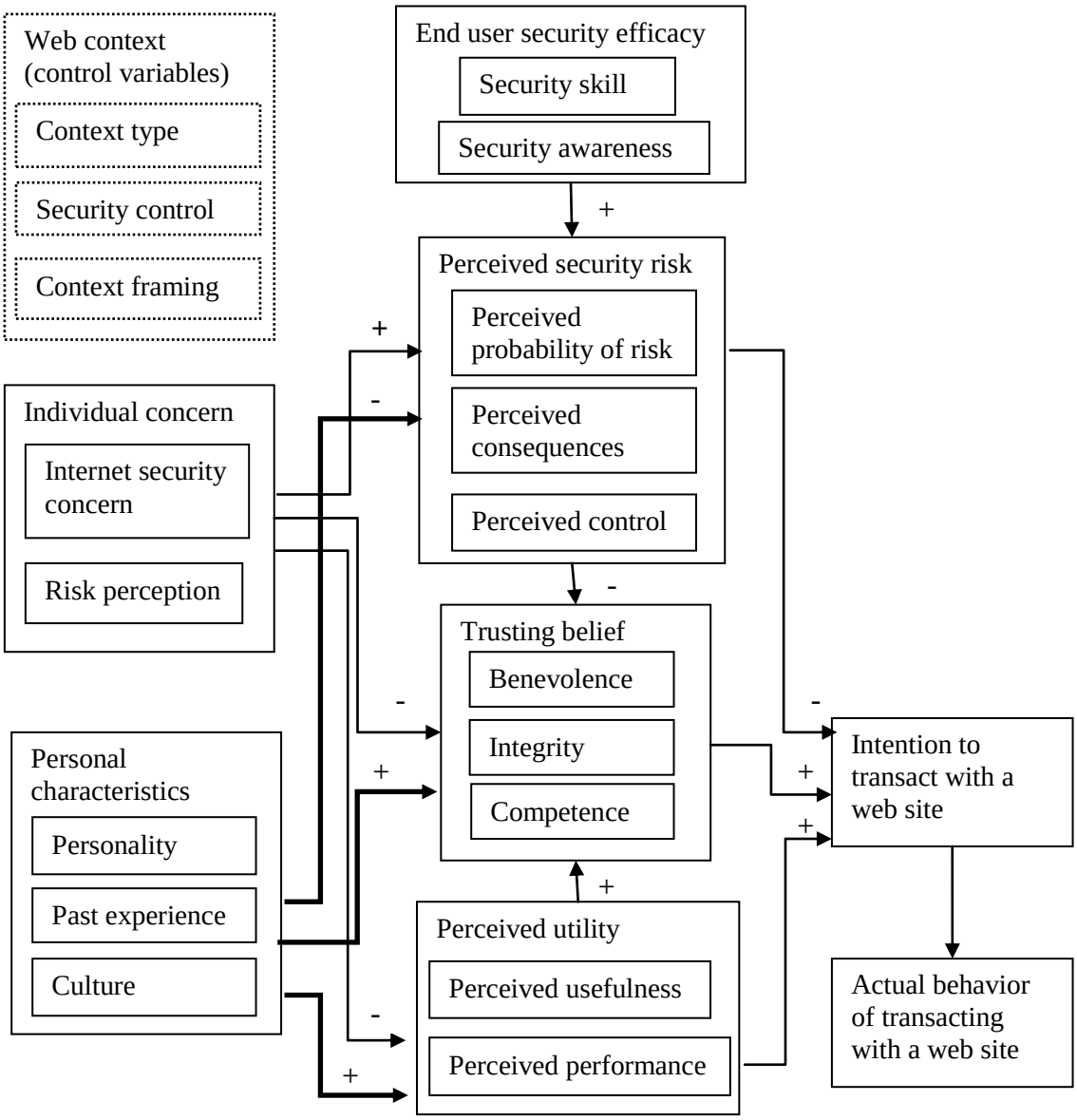

Figure 1: An Integrated Model of Individual Web Security Behavior

Trusting belief: The definition of trusting belief varies in different disciplines. We will adopt the definition from McKnight et al. (McKnight et al. 2002) since it describes users' initial trust on web sites. Trusting belief means the truster' (the end user) perceives that the trustee (e.g. a specific web site) has attributes that are beneficial to the truster. Three trusting beliefs will be investigated, including competence (ability of the web site to do what the end user needs), benevolence (the web site

caring about and being motivated to act in the end user's interests), and integrity (honesty and promise keeping by the web site). Research on online trust has focused on examining the antecedents of online trust and understanding how trust impacts one's intention to transact with a website (Ba and Pavlou 2002, Gefen 2002). Users' trust in the businesses, people or entities (such as seals) is often transferred to trust in their web sites (Fogg et al. 2003, Friedman et al. 2000). However, the cues for trust do not necessary indicate the security of the web sites and, as a result, the perceived security risk of the web sites is often not aligned with the actual security technology deployed if the perceived security risk is positively impacted by the trusting beliefs. When the trusting belief is not backed by secured technology, a web site can become a security risk once spoofed.

Intention to transact with a web site: This construct depicts user's decisions or preferences to transact with a web site. Such decisions or preferences sometimes involve risk choices, such as downloading spyware or accepting cookies, or trading off between a perceived secured site and perceived utility. We will investigate how these choices are made based upon theories from individual decision making. Prospect theory (Kahneman and Tversky 1979) has been the most cited theory in this field which explains that people tend to overweigh outcomes that are considered certain in comparison to outcomes that are merely probable (Tversky and Kahneman 1981). Prospect theory has been proposed to explain how individuals make decisions when facing security tradeoffs (West 2008) but only limited empirical studies have been done at this point (Chen and Farkas 2009a; 2009b). It is unclear if people behave the same way in computer security risk tradeoffs compared to economic tradeoffs. In the context of computer security, this theory implies that people will prefer smaller security gains over a chance of a larger reward and will prefer the chance of larger security loss over a small loss. For example, users might choose to risk the possibility of virus infection rather than spend $200 on anti-virus software.

Actual behavior of transacting with a web site: This construct will measure users' actual behavior in transacting with web sites. . Actual behavior is determined by individuals' behavior intention (Ajzen 1991, Ajzen and Fishbein 1980) which is influenced by individuals' attitude and subjective norms. Research has found some evidence that users behave differently than they think they would (Douglas and Wind 1971). To observe users' actual behavior, experimental designs in additional to user surveys are usually needed.

End user security efficacy: This construct is defined as users' ability to examine security cues on web sites (security skill) and their awareness of security information/cues on the site's vulnerabilities (security awareness). Such security cues may include specific site security information and security indicators such as SSL padlocks. Research had shown that, within an organizational context, users' awareness of security policy, SETA programs and computer monitoring significantly increases their perceived severity of information systems misuse and therefore reduces information systems misuse intention (D'Arcy et al. 2009). While security education in general might not increase users' perceived security risk, specific web security information might reduce users' risk of becoming involved in phishing (Downs et al. 2007). In addition, experts might also perceive security differently from users since they have more technical security knowledge (Turner et al. 2001). In terms of training methods, Campeau and Higgins (1995) compared two training models: (a) behavior and (b) traditional lecture to examine computer self-efficacy, outcome expectations, and performance. The behavior model was more effective than the traditional lecture for training the spreadsheet application.

Web context: Web context changes the underlying security risk since both the functionalities and the types of information provided on the site vary. Mayer et al. (1995) asserted the role of context as: "the antecedents of trust (ability, benevolence, and integrity) are affected by the context". Bansal et al. (2008b) show that context impacts the relationships amongst privacy concern, trust and intention to disclose information on a website. Bansal et al. (2008b) had shown the importance of web context on privacy decisions.

Individual concern: This construct depicts users' concerns on Internet security and risk perception in general. Internet security concerns have been acknowledged as significant factors in the adoption of e-commerce (Kim 2008). Risk perception in general has also been found to be correlated with computer security risk perception (Chen and Farkas 2009a, 2009b). Research has found that privacy concern lowers trust in a web site (Eastlick et al. 2006, Kim 2008, Malhotra et al. 2004, Van Dyke et al. 2007), but it is not clear how Internet security concern and risk belief will influence trust. Thus it could be argued that individual beliefs and concerns play a significant role in impacting security related decisions and behavior online.

Personal characteristics: This construct depicts individual traits, such as personalities, past experience and culture, which may have an impact on their web security behavior.

- Personality: Based on the Utility theory (Luce 1959, Mcfadden 1986; 2001), Bansal et al. (2010) argued that the utility one derives from a web site is a function of utility enhancers (e.g., trust) and utility reducers (e.g., security and privacy concern), and that the perceived valuation of these utility enhancers and reducers is a function of one's own individual traits. It is known that personality traits influence the perceived information sensitivity, and through it

privacy concern and trust (Bansal et al. 2010). Similarly, Korzaan and Baswell (2008) and Junglas et al. (2008) have also found that personality impacts privacy concern. Thus it could be argued that individual traits such as personality, culture, and past experiences could also shape one's security concern, and security related behavior online.

- Culture: Culture is the social programming of the mind. Culture impacts privacy concern and hence information sensitivity. For instance, it has been argued that collectivists are less concerned about privacy than individualists (Milberg et al. 1995). Culture also has an impact on individual risk attitude and risk perception (Weber and Hsee 1998). In addition, Aldiri et al. (2008) showed that initial trust differed across two cultural settings. Cyr et al. (2005) suggested that culture influences the perception of trust. Gefen et al. (2005) showed that culture impacts the relationship between trust and perceived usefulness. Srite and Karahanna (2006) showed that the relationship between perceived usefulness (utility) and intention is moderated by culture.
- Past experience: User experience with a web site or similar web activities may have an impact on their current behavior in terms of security decisions (Gefen et al. 2003a, Song and Zahedi 2007). Such experience could be positive, such as purchasing a product successfully from a site without any complications, or negative, such as falling into a phishing scam.

DISCUSSION AND IMPLICATIONS

The central implication of this paper is its support of the need to develop and study a comprehensive model of user online security behavior. Although recent studies shed light on design features, little effort has been made to examine the comprehensive model which studies both the situation and person specific factors simultaneously. The proposed model will extend existing theories by studying the human factors in terms of internal intrinsic traits such as personality, culture, risk beliefs and extrinsic factors such as experience and familiarity. Similarly it will study internal situation factors such as website performance and utility, and external situation factors such as context. Thus the model provides the comprehensive view of situation and personal factors from both internal and external perspective.

The work would also contribute by identifying the processes by which the users make security-related decisions online. The study would have practical implications as well. The findings would enhance our understanding about the relative importance of these internal and external, situation and person specific factors, which would then lead to the better design of the systems, as well as development of the appropriate educational and training material. The study would inform the website managers of the relative role of perceived usefulness and performance as well as other factors which impact the users' security decisions online. The findings would thus assist them in investing their resources accordingly. The website managers would understand the relative role of user experiences, website characteristics - such as performance vs. content, user security awareness among other things, thus assisting them in prioritizing their efforts as they try to make their websites safe and appear safe as well.

Various empirical studies can be designed upon this model to verify the hypotheses. First, by asking subjects to observe and utilize web sites in various contexts, an empirical study can be designed to identify the impact of individual concern and belief, and personal characteristics (independent variables) on perceived security risk, perceived utility, trusting belief, and intention/behavior to transact with a web site (dependent variables). Second, we can explore the impact of both security skill and security awareness on their perceived security risk and web security behavior by giving the subjects security efficacy training, such as recognizing security cues on web sites or reading through privacy/security policies of the sites. Last but not least, to validate the impact of culture, the previous two empirical studies can be implemented by collecting responses from subjects with different culture background. While designing the empirical studies, we will define the operationalization of the constructs carefully and follow the previous literature as possible.

CONCLUSIONS

We proposed an integrative model of human factors on decisions involving online security risk based upon previous literature. Our proposed model investigates a research area that has not been previously fully understood: the impact of human factors, such as personality, culture, web experiences, risk perception, and privacy concern on online security decision making. It provides a research foundation that is cross-disciplinary, including computer science, psychology, information systems, and management. It will allow us to extend our understanding of human dimension as it relates to online security. Future research will be conducted to validate the hypotheses in this model.

ACKNOWLEDGMENTS

Dr. Li-Chiou Chen is supported by a grant from the Thinkfinity Initiative of the Verizon Foundation for conducting this work. She would like to acknowledge the support of the Verizon Foundation in partnership with Pace University.

REFERENCES

1. Adams A., M. A. Sasse. 1999. Users are not the enemy. Communications of the ACM 42(12) 40-46.
2. Ajzen, I. 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50(2), 179-211.
3. Ajzen, I., M. Fishbein. 1980. Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ.
4. Aldiri, K, Hobbs, D., R. Qahwaji. 2008. The human face of e-business: engendering consumer initial trust through the use of images of sales personnel on e-commerce web sites. International Journal of E-Business Research 4(4) 58-78.
5. Asgharpour, F., Liu, D., L. J. Camp. 2007. Mental models of computer security risks, in Workshop on the Economics of Information Security, Pittsburgh, PA.
6. Aytes, K., T. Connolly. 2004. Computer security and risky computing practices: A rational choice perspective. Journal of Organizational and End User Computing 16(3) 22-40.
7. Ba, S., P. Pavlou. 2002. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. MIS Quarterly 26(3) 243-268.
8. Bansal, G., Zahedi F.M., D. Gefen. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, forthcoming
9. Bansal, G., Zahedi, F.M., D. Gefen. 2008a. Efficacy of privacy assurance mechanisms in the context of disclosing health information online, in Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Toronto, Canada.
10. Bansal, G., Zahedi, F.M., D. Gefen. 2008b. The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation, in the proceedings of the International Conference on Information Systems (ICIS), Paris.
11. Bhatnagar, A., Misra, S., H. R. Rao. 2000. On risk convenience, and internet shopping behavior. Communications of the ACM 43(11) 98-105.
12. Bresz, F. P. 2004. People - often the weakest link in security, but one of the best places to start. Journal of Health Care Compliance 57-60.
13. Chellappa, R., P.A. Pavlou. 2002. Perceived information security, financial liability, and consumer trust in electronic commerce transactions. Journal of Logistics Information Management, Special Issue on 'Information Security' 11(5) 358-368.
14. Chen, Y. H., S. Barnes. 2007. Initial trust and online buyer behavior. Industrial Management and Data Systems 107 21-36.
15. Chen, L.-C., D. Farkas. 2009a. An investigation of decision-making and the tradeoffs involving computer security risk," in the Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California.
16. Chen, L.-C., Farkas, D. 2009b. Individual risk perception and attitude towards computer security risks, in the Proceedings of the Third International Conferences on Internet Technologies and Applications, Wrexham, North Wales, UK.
17. Cranor, L., S. Garnkel, S. 2005. Security and usability: designing systems that people can use. O'Reilly Media, edited collection edition.
18. Cranor, L. 2008. A framework for reasoning about the human in the loop, in USENIX usability, psychology, and security (UPSEC).
19. Cyr, D., Bonanni, C., Bowes, J., J. Ilsever. 2005. Beyond trust: website design preferences across cultures. Journal of Global Information Management 13(4) 24-52.

20. D'Arcy, J., Hovav, A., and Galletta, D.F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research (20:1), p. 79-98.
21. Davis, F. D. 1989. Perceived usefulness, perceived ease of use and user acceptance of information technology. MIS Quarterly 13(3) 319-340.
22. DeLone, W. H., E. R. McLean. 1992. Information systems success: the quest for the dependent variable. Information Systems Research 3(1) 60-95.
23. Downs, J. S., Holbrook, M., L. F. Cranor. 2007. Behavioral response to phishing risk, in APWG eCrime Researchers Summit, Pittsburgh, PA.
24. Eastlick, M. A., Lotz, S. L., P. Warrington, P. 2006. Understanding online b-to-c relationships: an integrated model of privacy concerns, trust, and commitment. Journal of Business Research 59 877-886.
25. Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., E. R. Tauber. 2003. How do users evaluate the credibility of web sites?, in Proceedings of the 2003 conference on Designing for user experiences, San Francisco, California.
26. Friedman, B., Kahn, P.H., D. C. Howe, D.C. 2000. Trust online. Communications of the ACM 43(12) 34-40.
27. Gefen, D. 2002. Reflections on the dimensions of trust and trustworthiness among online consumers. ACM SIGMIS Database 33(3) 38-53.
28. Gefen, D., Karahanna, E., D. W. Straub. 2003a. Inexperience and experience with online stores: the importance of TAM and trust. IEEE Transactions on Engineering Management 50(3) 307-321.
29. Gefen, D., Karahanna, E., D. W. Straub. 2003b. Trust and TAM in online shopping: an integrated model. MIS Quarterly 27(1) 51-90.
30. Gefen, D., Rose, G.M., Warkentin, M., P. A. Pavlou. 2005. Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa. Journal of Global Information Management 13(1) 54-79
31. Hardee, J. B., West, R., C. B. Mayhorn. 2006. To download or not to download: an examination of computer security decision making. ACM Interactions 32-27.
32. Junglas, I. A., Johnson, N. A., C. Spitzmuller. 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. European Journal of Information Systems 17 387-402.
33. Kahneman, D., A. Tversky, A. 1979. Prospect theory: an analysis of decision under risk. Econometrica 47(2) 263-291.
34. Kim, D. J. 2008. Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. Journal of Management Information Systems 24(4) 13-45.
35. Korzaan, M. L., K. T. Boswell. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. The Journal of Computer Information Systems 48(4) 15-24.
36. Liao, Z., M. T. Cheung. 2002. Internet-based e-banking and consumer attitudes: an empirical study. Information & Management (39) 283-295.
37. Lee, S. M., Lee, S. G., S. Yoo. 2004. An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41(6) 707-718.
38. Lineberry, S. 2007. "The human element: the weakest link in information security. Journal of Accountancy 44-49.
39. Luce, R.D. 1959. Individual Choice Behavior: A Theoretical Analysis. New York: Wiley.
40. Malhotra, N. K., Kim, S. S., J. Agarwal. 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 15(4) 336-355.
41. Mayer, R. C., Davis, J. H., F. D. Schoorman. 1995. An integration model of organizational trust. Academy of Management Review 20(3) 709-735.
42. McFadden, D. L. 2001. Economic choices. American Economic Review 91(3) 351-378.
43. McFadden, D. L. 1986. The choice theory approach to market research. Marketing Science 5(4) 275-297.

44. McKinney, V., Yoon, K., F. Zahedi. 2002. The measurement of web-customer satisfaction: an expectation and disconfirmation approach. Information Systems Research 13(3) 296-315.
45. McKnight, D. H., Chervany, N.L. C. Kacmar. 2002. Developing and validating trust measures for e-commerce. Information Systems Research 13(3) 344-59.
46. Milberg, S. J., Burke, S. J., Smith, H. J., E. A. Kallman. 1995. Values, personal information privacy, and regulatory approaches. Communications of the ACM 38(12) 65-74.
47. Morgan, M. G. 1981. Probing the question of technology-induced risk. IEEE Spectrum 18(11) 58-64.
48. Ng, B.-Y., Kankanhalli, A., Y. Xu. 2009. Studying users' computer security behavior: A health belief perspective. Decision Support Systems 46 815-825.
49. Ranganathan, C., S. Ganapathy. 2002. Key dimensions of business-to-consumer web sites. Information and Management 39(6) 457-465.
50. M. Rosenstoick, 1974. The Historical Origins of the Health Belief Model. Health Education Monograph. 2 (4).
51. Salisbury, W., Pearson, P., Pearson, A., D. Miller. 2001. Perceived security and world wide web purchase intention. Industrial Management & Data Systems 101 165 -176.
52. Song, J., F. Zahedi. 2007. Trust in health infomediaries. Decision Support Systems 43 390-407.
53. Srite, M., E. Karahanna. 2006. The role of espoused national culture values in technology acceptance. MIS Quarterly 30(3) 679-704.
54. Stanton, J. M., Stam, K. R., Mastrangelo, P., J. Jolton. 2005. An analysis of end user security behaviors. Computers & Security 24 124-133.
55. Suh, B., I. Han. 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce 7(3)135-161.
56. Turner, C. W., Zavod, M., W. Yurcik. 2001. Factors that affect the perception of security and privacy of e-commerce web sites, In B. Gavish (Ed.), in the Proceedings of the Fourth International Conference on Electronic Commerce Research 628-636.
57. Tversky, A., D. Kahneman. 1981. The framing of decisions and the psychology of choice. Science 211(4481) 453-458.
58. Van Dyke, T. P., Midha, V., H. Nemati. 2007. The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. Electronic Markets 17(1) 68-81.
59. Weber, E.U., C. Hsee. 1998. Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk. Management Science 44(9) 1205-1217.
60. West, R. 2008. The psychology of security. Communications of ACM 51(4) 34-40.
61. Whitten, A., J. D. Tygar. Why Johnny can't encrypt: A usability case study of PGP 5.0, in Proceedings of the 8th USENIX Security Symposium, Washington D. C., 1999 169-184.