Winter 12-15-2012

An Exploration of Security and Privacy Behavior of Elders on the Internet and comparison with Younger Adults

Rajarshi Chakraborthy
University at Buffalo, rc53@buffalo.edu

Sharmistha Bagchi-Sen
University at Buffalo

Raghav H. Rao
University at Buffalo, mgmtrao@buffalo.edu

Shambhu Upadhyaya
University at Buffalo

An Exploration of Security and Privacy Behavior of Elders on the Internet and comparison with Younger Adults

Rajarshi Chakraborty[1]
School of Management, University at Buffalo,
Amherst, NY

Sharmistha Bagchi-Sen
Dept. of Geography, University at Buffalo,
Amherst, NY

H. Raghav Rao
School of Management, University at Buffalo, Amherst, NY
Sogang University, Seoul, South Korea

Shambhu Upadhyaya
Computer Science & Engg, University at Buffalo,
Amherst, NY

ABSTRACT

One of the fastest growing demographics to utilize the Web as part of their everyday life is the group of older adults who are aged 55 and above. The rising adoption of the Internet by older adults has resulted in both security and privacy problems for them. In this paper we develop a model to focus on the behavioral side of the security and privacy discussion among elders. For comparative purposes we also test the model with student subjects. We find considerable differences in the results between the elders and young adults and suggest potential issues that can be tested for understanding the differences.

Keywords: Older Adults, Information Privacy, Information Security, Security Behavior, Privacy Behavior, Privacy Attitude

[1] Corresponding author. rc53@buffalo.edu

INTRODUCTION

One of the fastest growing demographics to utilize the Web as part of their everyday life is the group of older adults who are aged 55 and above (Brockman 2010). In spite of this increased adoption of the Web, people aged 55 and above remain the most vulnerable in terms of online information security and privacy. A recent report (2012) based on complaints received at FTC show that "scam artists are targeting older Americans more than ever before". Wall Street Journal (2011) reported that 2011 was the record year for investment scams for people aged over 50. Much of these scams and other reported frauds highlight both security and privacy problems for older adults. It has been established (Yao 2011) that privacy issues on the Internet involve a lot more self-protective strategies compared to protecting privacy in the physical world. The rest of the paper lays out the theoretical underpinnings for a research model followed by a presentation of the data collected, the method applied for analysis and the results obtained. For comparative purposes we also test the model with student subjects.

THEORY AND RESEARCH MODEL

The objective of this study is to investigate the factors that are responsible for the actions that older adults take on the Internet to maintain their security and privacy. One of the commonly used theoretical frameworks for studying human behavior in context of computer security is the variance model of the Technology Threat Avoidance Theory (TTAT) (Liang and Xue 2009) which describes how IT users deal with technology-borne threats and the mechanisms that result in intentions and actual actions that mitigate those threats. This model is largely based on the Protection Motivation Theory (PMT) (Rippetoe and Rogers 1987). It helps identify that IT users not only perceive threat and appraise its severity but also seek coping mechanisms. These two dynamics along with a certain

awareness level of possible threats are jointly affect the actions that help minimize or mitigate relevant threats. The actions are termed as "avoidance behavior".

While the variance model of TTAT tries to cover sufficient ground by incorporating social influence as well as breaking down threat appraisal and coping appraisal into fundamental constructs, we have adapted select constructs from it for our study. The motivation here is to form a more relevant model as a first step towards understanding older adults' online privacy. One of the differences between scenarios that TTAT is supposed to address and the ones that we are interested in is that the technology itself need not be malicious. TTAT essentially looks human response to malicious IT artifacts and situations. In other words, TTAT assumes that the individual is already aware of the threat (e.g. in Liang and Xue's JAIS paper in 2010 they test the adoption of spyware using TTAT).

In our situation though we are looking at general actions with respect to virtuous IT that an individual depends on every day (e.g. web browsers and email clients). Here perception of severity does not play a significant role until some privacy or security breach has occurred and the user is well aware of it. The actions we are interested in are rather relevant to situations that consist of elements of uncertainty. In particular, the focus of our research is the attitude and the subsequent action of an older adult in the presence of an unsolicited email or in the presence of a new website. These scenarios don't involve malicious activities all the time.

Given the lack of emphasis on privacy and security related behavior by older adults on the Internet in the cyber security literature, we set out to understand behavior by investigating some of the fundamental IT specific factors that generic in nature (are not specific to aging).

Constructs

Online Security and Privacy Behavior (OSPB)

The goal of this paper is to understand behavior in the face of uncertain security and privacy concerns on the Internet. We call this the Online Security and Privacy Behavior (OSPB). OSPB indicates the extent of protective and preventive measures an individual reportedly takes in safeguarding his/her own computer and personal information that is available on that computer. Actions that are intended to safeguard the information constitute privacy protection. We are focusing here on privacy breaches that could be perpetuated by compromising the security of any Internet-connected software. More specifically OPSB is intended to account for various important components of security and privacy like password strength, safe Web navigation and computer safety through anti-viruses. In the past researchers have usually looked at actions related to risk mitigation as the natural extension of intentions to undertake the same. These intentions were studied in the context of several factors that can be grouped into coping and appraisal related attributes about the said risk. This framework of study has been widely applied in several domains, especially in information assurance, under the umbrella of Theory of Planned Behavior and PMT. Most of these studies have been limited to the investigation of intentions (Herath and Rao 2009) while a few measured the actions (Furnell et al. 2007; Liang and Xue 2010; Ng et al. 2009; Woon et al. 2005). We take inspiration from the latter body of work and extend it towards actions that cover a wider range of aspects of information security (Furnell et al. 2007).

Previous works on security actions have measured actions related to very specific IT or security artifacts (e.g., securing personal Wi-Fi network (Woon et al. 2005) and run and update anti-spyware (Liang and Xue 2010)). This study on the other hand examines the following aspects of security and privacy: maintaining strong passwords, keeping the computer safe from viruses and

refrain from engaging with unknown websites. Based on discussions with domain experts, we understand that these cover most of the activities of older adults regarding their common security and privacy protection practices.

Perceived Threat (PT)

Actions taken by an individual to remain safe on the Internet should be influenced directly by the amount of threat he/she perceives. Different individuals can perceive threats to a varying degree if there is an element of uncertainty. For example, if unsolicited emails arrive, two individuals might not interpret the opening of such an email (or even any attachment in it) as a situation of vulnerability to the same extent. Threats are assessed partly by the extent to which one feels vulnerable and partly by how severe the threat is deemed to be. Adapting items for measuring telemarketing fraud (Lee and Geistfeld 1999) into the online communication context, we measure Perceived Threat (PT) based on the opinion an individual forms about senders of unsolicited emails. In this study we focus on the vulnerability aspect of threat assessment only. The severity aspect is left out based on our assumption that the phenomenon studied centers around the every day online activity of senior citizens where average individuals are not expected to assess security and privacy threats all the time.

Privacy Attitude (PA)

The decision to be vigilant while using the Internet for daily activities or fun is based partly on the basis of the value an individual attaches to his/her personal information, especially one that is stored on the computer. Additionally, however, it is not just the value of the information itself but also the attitude about controlling any kind of personal information that plays a role in the online security and privacy behavior decisions (OSPB). There is a rich body of literature that defines information privacy as a control over one's personal information (Clarke 1999; Dinev and Hart 2004; Malhotra et al. 2004; Wang et al. 1998). The desire to control one's information manifests as expectations about

how online properties like websites should allow users to keep that control. We thus borrowed the items that measure an individual's awareness of privacy practices from (Malhotra et al. 2004) measure Privacy Attitude (PA) of older adults. What we are essentially assuming here is that a certain sense of expectations to achieve a certain state of control is a direct indicator of the individual's attitude towards that state itself. Since one needs a certain attitude to engage in a relevant action, we treat PA to be an antecedent of OSPB.

Perceived Self-Efficacy (EFF)

When an individual like an older adult makes a conscious decision like avoiding a suspicious website or discerning the risks in opening an unsolicited email attachments on a computer that is not running anti-virus, he/she is essentially engaging in a planned behavior where the part of the planning process includes assessment of his/her confidence. We argue that this is essentially one's confidence in choosing the appropriate methods and tools to deal with any kind of threat. In addition, the planning should also derive from a confidence in one's ability to simply use computers and the Internet in a way that does not land a user in trouble. For example, a Google search for a certain medical information might give unsafe results and it is the ability to avoid those traps that count as good Web navigation skills. Internet skills on the other hand include email skills as well as discretion exercised in attachment download. Such skills give signs for safe Internet behavior (Adams et al. 2005). Planning to use a security tool or to take the extra precautionary steps while carrying out daily routines on the Internet requires crossing a few psychological barrier and one of those barriers is simply the overall confidence or self-efficacy of using the Internet safely. Based on prior research regarding computer self-efficacy (Kuo and Hsu 2001) we will measure perceived self-efficacy (EFF) indirectly through self-reported efficacy in security (PSE), Internet (PIE) as well as in skills to safely navigate the Web (PEWN).

Perceived Cost of Security and Privacy (PCOSP)

TTAT as well as PMT have both ascribed the net assessment of dealing with fears and threats to the existence of certain costs. Behavior in general can be "impeded" by several factors. We believe one of those factors in our scenario is the price a person has to pay to achieve security and privacy on the Internet. Past research on aging and information systems adoption (Hüsing and Selhofer 2002; Peacock and Künemund 2007; Phang et al. 2006) has focused on the risk and cost aspect by generally pointing to an element of uncertainty as a critical part of the overall experience on the Internet for older adults. We postulate here that adopting safeguards against threats on the Internet is essentially just another step of IT adoption for an individual who has already adopted an artifact known as the Internet. Since measures for perceived cost of adopting the Internet for older adults already exists (Cody et al. 1999), we adapted them to the context of online safety to measure Perceived Cost of Security and Privacy (PCOSP).

Hypotheses

In this section, we build the hypotheses for our research model (figure 1) for the population of older adults. All the hypotheses pertain to actions on a computer. These are founded in the Technology Threat Avoidance Theory (TTAT) and extant literature on gerontology and information assurance. It has been shown in the past that people can be discouraged from using the Internet because of perception of vulnerability to threat that they are not even familiar with(Downs et al. 2006; Lee and Geistfeld 1999). Since perception of threat is an essential component of assessing the threat in order to take the appropriate decision (Liang and Xue 2009; Woon et al. 2005), we propose to test the following hypothesis:

H1: *Higher the perceived threat, the more precautionary is the online security and privacy behavior.*

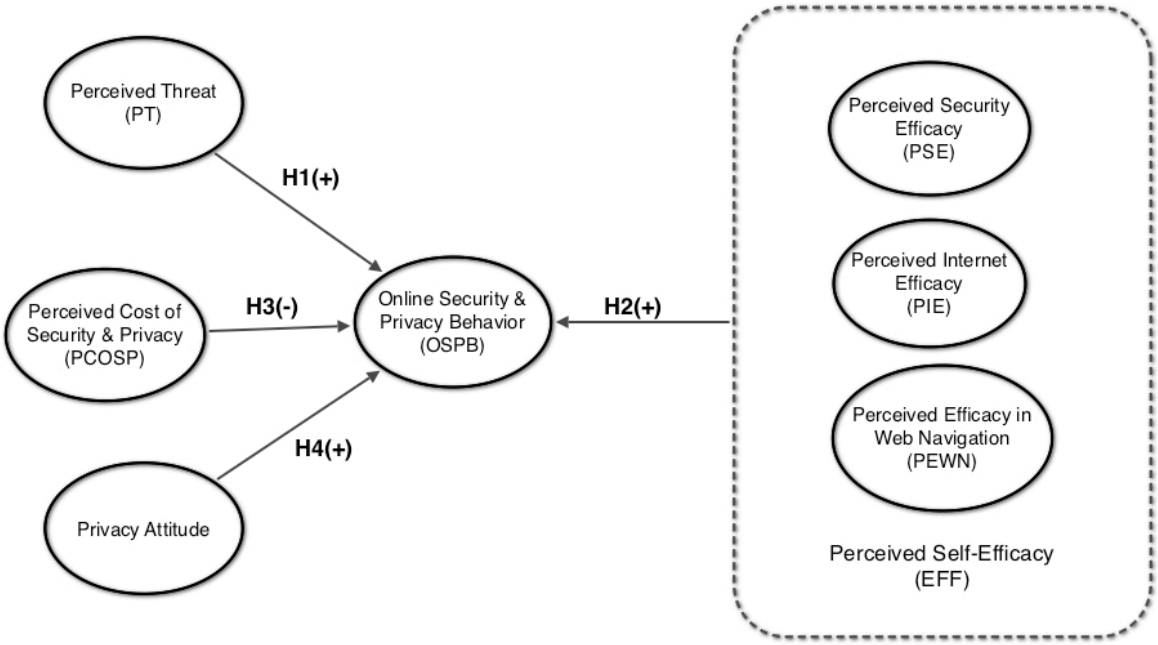

Figure 1. Research Model

While the above pertains to the threat assessment necessary for an adaptive behavior on the Internet, it is also necessary to consider the effect of one's self-efficacy for the same purpose. As discussed before, identifying and assessing a potential threat is one part of the equation while the other part is the equally important task of measuring how one can cope with such a threat. Confidence is one part of that coping assessment process. For example, if a person has to make a decision about visiting only those websites deemed safe enough or if it is about avoiding clicking on ads or download links on an unknown website, the self-efficacy necessary to make the safest choice in this context pertains to one about website navigation primarily. In addition these precautionary actions are to be determined by encouraging belief in general about Internet and security issues as well. We thus test this relationship using the following hypothesis:

H2: *Higher the perceived self-efficacy, the more precautionary is the online security and privacy behavior.*

If self-efficacy helps a person determine the tools and choices to adopt to navigate safely through websites and use Email, those same tools and choices come with a cost. Older adults, especially, are bound to engage in a cost-benefit analysis of before deciding to use such tools and make the appropriate choices. We thus hypothesize the following hypothesis:

H3: *Higher the perceived cost of security and privacy, the less precautionary is the online security and privacy behavior.*

We complete our research model by incorporating the role of attitude towards controlling personal information, also labeled above as privacy attitude. This concept captures the reward aspect of making safe choices on the Internet. In other words, an older adult can consider the ability or the perception of being in control of his/her own information as a benefit of taking extra precautions on the Internet. As manifested in the expectation of online properties giving better privacy controls to the user, this attitude symbolizes a predisposition to act safe on the Internet. This gives us our final hypothesis:

H4: *The more privacy-leaning the privacy attitude, the more precautionary is the online security and privacy behavior.*

Hypotheses H1 and H4 answer our research questions based on security and privacy threat perception, while hypotheses H2 and H3 should help us answer questions about self-efficacy and cost respectively.

DATA, ANALYSIS, AND RESULTS

In order to test our model on older adults, we conducted an online survey for older adults aged above 55. The items used to measure our variables have mostly been based in existing information security and privacy as well as gerontology literature. We measured self-efficacy as a second order construct (Torkzadeh and Van Dyke 2001). We reached out to the older adults through several local

senior center mailing lists as well as local clubs that attracted older adults outside senior centers. After removing responses with missing information, we were left with a sample size of 97 older adults. Majority of the older adults were in the age group of 60-64 (29%) and a majority of them happened to be females as well (72%). These older adults happened to be mostly college educated with a little more 57% reporting to have finished a graduate or a professional degree. Ethnically there was not much variation (90% Caucasian), primarily due to the ethnic distribution of the region. The research model was tested using SmartPLS and bootstrapping for significance testing. The outcome of this analysis was that while most of the measurement model was found to hold true, the structural model did not. In other words, all the hypotheses were rejected.

At this stage, we decided to check if the unfavorable results were an outcome of the instrument itself or if this could be attributed to some hidden social and aging concepts embedded in the phenomenon. To understand this better, we decided to offer the same instrument to an audience of young college students from junior and senior level information systems classes in the School of Management. This resulted in a sample size of 383 and the outcome was that both the structural for the most part and measurement models completely were found significant. In summary, hypothesis H3 (Cost->Behavior) was not supported for the younger adults but the rest were. Table 1 below gives a comparison of the path coefficients for the model with the two data sets. Table 2 gives a deeper insight into the disparity between the models by comparing some validity and reliability metrics for variables where there was a large distinction and especially where the older adult counterpart fell below acceptable threshold values. The R^2 value for OSPB was found to be 0.2151 for the student dataset while it was 0.0428 for the older adults.

Table 1: Comparison of path coefficients

Dataset	H1(+)	H2(+)	H3(-)	H4(+)
Student	0.107*	0.321***	-0.053	0.176*
Older Adults	0.049	-0.084	-0.206	0.034

** p<0.05, *p<0.01, *** p<0.001*

Table 2: Comparison of Reliability and Validity values for some variables

Metric	*Construct*	*Student Sample*	*Older Adult Sample*
AVE	EFF	0.5093	0.3752
Cronbach Alpha	PCOSP	0.6862	0.5877
	PSE	0.7149	0.5697
Communality	EFF	0.5093	0.3752
	OSPB	0.5335	0.5139
	PA	0.7192	0.5262
	PSE	0.6371	0.5331

In particular, the following items did not load significantly on their corresponding constructs for the older adults:

OSPB: "I feel uncomfortable giving away my Social Security Number to anybody on the Internet."

PA: "A good online privacy policy should have a clear and conspicuous disclosure."

PCOSP: "It is expensive to protect myself during my Internet activities like browsing the Web, checking my email or chatting."

These findings have two important implication: (1) The model used for the older adults may have been underspecified and (2) Some of the items used may have been perhaps less relevant to older adults. One way to rectify that could be to include the following constructs in the model/instrument, which have been derived based on careful examination of feedback left by older adults in the previous version of this survey. Possible new concepts based on statements left as feedback in the first phase of survey are given in Table 3.

Table 3: Concepts from user feedback

Concepts	*Statements from survey feedback*
Threat Experience	1. "I used Craig's List to rent a time share week and got involved in a potential scam " 2. "I learned the hard way re: Trojan Viruses which invaded my brand new Lap Top this past Nov."
Awareness of Security and Privacy Issues	1. "Hadn't realized that the hackers could accomplish this, as they didn't actually come from sources I know." 2. "Watch out for helpful Nigerians (and others, those wanting money sent by Western Union and offers that are too good to be true (even if just a little too good)."
Belief in Personal Responsibility	1. "People should use their common sense, as in everything else" 2. "it is important to remain vigilant about changes that occur"

DISCUSSION AND FUTURE WORK

A direct implication from the results above is that there is a disconnect between the behavior and all the supposed antecedents like attitude, perceived threat, cost and efficacy in the older adults. Unlike the results with the student data, this disconnect defies our theoretical foundation adapted from TTAT. While majority (75%) of the student population was between 18 and 25 years old, we got a lot more variety ethnically (39% Caucasians and 35% Asians) and gender-wise (47% males and 53% females). This tells us that the college student population was homogeneous only in age but no in other demographic attributes. On the other hand, as pointed out above, older adults seem more diverse in their age group but not in ethnicity and gender. In other words, we found our model to be satisfied with a younger population that was more homogeneous in age compared to other factors than in an older population that was less homogeneous in age compared to other factors. Additionally, the younger adults (students) were quite homogeneous in terms of technology adoption since 98% owned a computer, 82% did online banking and 95% engaged in online shopping. But this trend was also present in our sample of older adults – every single older adult owned a computer, 72% did online banking and 94% made purchases on the Internet. This comparison shows that there was not a big

different in terms of technology adoption between the two samples. It implies that our fundamental understanding of factors driving older adults' security and privacy behavior need to go beyond what traditional models have captured.

CONCLUSION

Older adults, who are aged 55 years and above, are an unexplored audience in the comprehensive understanding of the behavioral side of information security and privacy. This paper is one of the first steps in that direction and thus started out adapting constructs and theoretical underpinnings from a framework called Technology Threat Avoidance Model (TTAT). However, when compared to a younger generation, the proposed model wasn't supported based on the survey responses returned by the older adults. The model by virtue of surviving the data from the classrooms pushed the discussion towards greater introspection about appropriate application of privacy and security frameworks that simply test actions based on attitude about threats and beliefs in efficacy of those actions. The findings and the subsequent discussion in this paper imply that such frameworks need to incorporate trust, awareness and finally aging-specific variables in context of the population of older adults.

Acknowledgement

We thank the editor and the referees for their invaluable comments and suggestions. This research is supported in part by NSF Grant No. 0916612. The research of the third author was funded in part by Sogang Business School's World Class University Project (R31-20002), funded by Korea Research Foundation and by Sogang university Research Fund. Usual disclaimer applies.

REFERNCES

2011. "Boomers Wearing Bull's-Eyes: Postcrisis, Those over 50 Targeted in Investment Scams; Problem Is 'Rampant'." *The Wall Street Journal*, from http://online.wsj.com/article/SB10001424052970204319004577088170263635052.html

2012. "Scams Targeting Older Adults Are on the Rise." *Huffingtonpost*, from http://www.huffingtonpost.com/2012/03/10/scams-older-adults_n_1317285.html.

Adams, N., Stubbs, D., and Woods, V. 2005. "Psychological Barriers to Internet Usage among Older Adults in the Uk," *Informatics for Health and Social Care* (30:1), pp. 3-17.

Brockman, J. 2010. "Social Networking Surges for Seniors," *Pew Internet & American Life Project,*), August 27, 2010.

Clarke, R. 1999. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), pp. 60-67.

Cody, M., Dunn, D., Hoppin, S., and Wendt, P. 1999. "Silver Surfers: Training and Evaluating Internet Use among Older Adult Learners," *Communication Education* (48:4), pp. 269-286.

Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents-Measurement Validity and a Regression Model," *Behaviour & Information Technology* (23:6), pp. 413-422.

Downs, J., Holbrook, M., and Cranor, L. 2006. "Decision Strategies and Susceptibility to Phishing," ACM New York, NY, USA, pp. 79-90.

Eastman, J.K., and Iyer, R. 2005. "The Impact of Cognitive Age on Internet Use of the Elderly: An Introduction to the Public Policy Implications," *International Journal of Consumer Studies* (29:2), pp. 125-136.

Freese, J., Rivas, S., and Hargittai, E. 2006. "Cognitive Ability and Internet Use among Older Adults," *Poetics* (34:4-5), pp. 236-249.

Furnell, S., Bryant, P., and Phippen, A. 2007. "Assessing the Security Perceptions of Personal Internet Users," *Computers & Security* (26:5), pp. 410-417.

Herath, T., and Rao, H.R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Hüsing, T., and Selhofer, H. 2002. "The Digital Divide Index-a Measure of Social Inequalities in the Adoption of Ict," *Proceedings of ECIS*.

Jobe, J.B., and Mingay, D.J. 1990. "Cognitive Laboratory Approach to Designing Questionnaires for Surveys of the Elderly," *Public Health Reports* (105:5), p. 518.

Kail, R.V., and Cavanaugh, J.C. 2012. *Human Development: A Life-Span View*. Wadsworth Pub Co.

Kuo, F.Y., and Hsu, M.H. 2001. "Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Softlifting," *Journal of Business Ethics* (32:4), pp. 299-315.

Lee, J., and Geistfeld, L. 1999. "Elderly Consumers' Receptiveness to Telemarketing Fraud," *Journal of Public Policy & Marketing* (18:2), pp. 208-217.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *Management Information Systems Quarterly* (33:1), p. 6.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Magaziner, J., Simonsick, E.M., Kashner, T.M., and Hebel, J.R. 1988. "Patient-Proxy Response Comparability on Measures of Patient Health and Functional Status," *Journal of Clinical Epidemiology* (41:11), pp. 1065-1074.

Malhotra, N., Kim, S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns(Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Millward, P. 2003. "The'grey Digital Divide': Perception, Exclusion and Barriers of Access to the Internet for Older People," *First monday* (8:7-7).

Miyazaki, A., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs* (36:1), pp. 28-49.

Ng, B.Y., Kankanhalli, A., and Xu, Y.C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Peacock, S.E., and Künemund, H. 2007. "Senior Citizens and Internet Technology," *European Journal of Ageing* (4:4), pp. 191-200.

Phang, C., Sutanto, J., Kankanhalli, A., Li, Y., Tan, B., and Teo, H. 2006. "Senior Citizens' Acceptance of Information Systems: A Study in the Context of E-Government Services," *IEEE Transactions On Engineering Management* (53:4), p. 555.

Reisenwitz, T., Iyer, R., Kuhlmeier, D., and Eastman, J. 2007. "The Elderly's Internet Usage: An Updated Look," *Journal of Consumer Marketing* (24:7), pp. 406-418.

Rippetoe, P.A., and Rogers, R.W. 1987. "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat," *Journal of personality and social psychology* (52:3), p. 596.

Sutter, M., and Kocher, M.G. 2007. "Trust and Trustworthiness across Different Age Groups," *Games and Economic Behavior* (59:2), pp. 364-382.

Torkzadeh, G., and Van Dyke, T.P. 2001. "Development and Validation of an Internet Self-Efficacy Scale," *Behaviour & Information Technology* (20:4), pp. 275-280.

Wang, H., Lee, M., and Wang, C. 1998. "Consumer Privacy Concerns About Internet Marketing," *Communications of the ACM* (41:3), pp. 63-70.

Willis, G.B., Royston, P., and Bercini, D. 1991. "The Use of Verbal Report Methods in the Development and Testing of Survey Questionnaires," *Applied Cognitive Psychology* (5:3), pp. 251-267.

Woon, I., Tan, G.W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," *ICIS 2005 Proceedings*), p. 31.

Yao, M.Z. 2011. "Self-Protection of Online Privacy: A Behavioral Approach," *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*), p. 111.