Risk communication design for older adults

Vaibhav Garg [1]*, Lesa Lorenzen-Huber [2], L. Jean Camp [1], and Kay Connelly [1]

[1] School of Informatics and Computing, Indiana University, USA
[2] School of Health, Physical Education, and Recreation, Indiana University, USA
** Corresponding author (gargv@indiana.edu)*

Purpose Older adults are more susceptible to fraud offline than younger adults. As they increasingly use the internet for activities including managing financial assets, this susceptibility is transferred online. Thus, there is an imminent need to communicate the risks inherent in these new technologies, especially that of data disclosure, to older adults. These risks might best be communicated by using appropriate mental models and grounding analogies in more familiar risks, e.g. physical risks. Using videos rather than text may improve comprehension as well as address other concerns of aging, e.g. attention and memory. While videos can lead to richer comprehension, multi-media communications can challenge cognitive reserves. We present the design of narrative-driven risk communication videos that leverage physical analogies to answer the following questions: (i) What are the determinants of older adults perception of online risk, specifically for responding to phishing and malware e-mails?; and (ii) What is the effect on comprehension when using videos as opposed to text? **Method** To investigate the determinants of older adults' perceptions of online risk, Garg and Camp investigated a nine-dimensional model of risk perception that is based on an expressed preferences. They found that not all the nine dimensions are equally relevant online. They proposed a five-dimensional model for online risks consisting of voluntariness, immediacy, control, chronic-catastrophic, and severity. These dimensions were adapted to create a survey to assess elders' determinants of risk. For example, voluntariness is redefined as, "To what extent does an older adult have a choice in being exposed to this risk? (1=Voluntary, 5= Involuntary)". Our second question, whether video is more effective than text in communicating risk, was evaluated by participant comprehension: participants' ability to identify the risk, the attack vector, the impact of risk if exploited, and strategies to avoid or mitigate the risk. We conducted pilot studies with a convenience sample of 12 older adults (8 female and 4 male). Six participants watched the videos, the other six read the textual description of the risks, and each filled out associated surveys. **Results & Discussion** All 12 participants rated the risk of responding to be higher than that of not responding, but not all items on the five dimensions were rated higher for responding. This indicates that not all dimensions have equal weights in the construction of perceived risk. Participants in the video group were more likely to verbalize the risk of responding or not responding, suggesting videos might be better at explaining online risks to older adults.

***Keywords**: communication and governance, security, older adults, risk communication*

INTRODUCTION

As the baby boomers approach the age of retirement, older adults have become the fastest growing demographic in United States. Currently people over 65 form 13% of the population. This is expected to increase to 20.7% by 2050. Financial assets owned by older adults are consequently proportionally increasing. One-tenth of all publicly held bonds are held by people over 65 years of age[5]. By 2020 older adults will own one-third of all publicly held stocks in America. Older adults are, however, highly susceptible to scams and financial fraud. According to the Federal Trade Commission, over 20% of the victims of financial fraud are older adults[1]. This susceptibility to victimization is likely to be transferred online.

Older adults are increasingly using the Internet to manage their financial assets. However, they have traditionally been underserved by the designers of technology. The current design of technologies assumes a high level of computer literacy and agile cognitive abilities[8]. Conversely, older adults are disproportionately inexperienced with information technology. They have less cognitive reserve and plasticity than younger cohorts[20]. As such they may be unaware of the many risks they face when they go online. Thus a combination of misperception of risk, poor understanding of technology, and age related cognitive changes might either prove a deterrent to adoption or expose older adults to undesirable risks[7].

There is limited research examining older adults' understanding of the risk generated by their digital data with respect to financial privacy and security[17]. We propose to address this knowledge gap by creating a model of older adults' understanding of their digital footprint and financial risk.

Thus, in this study we wanted to address two research questions. First, what is the effect on comprehension when using videos as opposed to text? Second, what are the determinants of older adults' perception of online risk, specifically for responding to phishing and malware emails?

Older adults generally express lower concerns about information privacy than the population at large[19]. In many cases, their perceived risk is less than their actual risk. To address this gap, there is a need to

identify determinants of risk perceptions for older adults. These determinants can then inform the design of risk communication technologies targeted towards older adults. Our goal is to enable older adults to identify, mitigate, and avoid risks to their financial assets and personal identity. Identifying determinants of risk perception would allow designers to ensure that the information contained in risk communication is pertinent, aligned with the elder's mental model, and informs decision- making. This is particularly important for older adults as they disproportionally suffer from increased sensitivity to irrelevant intrusions and are less able to selectively attend to information[12].

In this paper we present the design of narrative-driven risk communication videos that leverage physical mental models to inform older adults about online risks. The two risks we target are phishing and malware. The next section provides the background and describes the rationale for our approach.

BACKGROUND

Misperception of risk, limited understanding of information technology, and age-related cognitive changes leave older adults vulnerable to a host of financial crimes. Financial loss can be more distressing for elders than their younger counterparts, as elders have limited time and ability to recover financially. With the ubiquity of the Internet, financial exploits can now be conducted by unidentifiable electronic assailants from distant jurisdictions. As recovery becomes more difficult, prevention is increasingly crucial.

Individual resilience to social engineering attacks has been addressed by providing security education to non-experts, e.g. phishing education[16]. The participants in these studies, however, are usually younger adults who may differ from older adults in their ability to assimilate new information. We propose to build upon these works by addressing a demographic group that differs in its cognitive plasticity and technological experience. Furthermore, our approach addresses risk communication as a complement to security education. Education may be a longer-term effort that requires a higher cognitive commitment. It can be argued that the primary goal is to change behavioral reaction to risk rather than to explain the underlying mechanism. The latter might be particularly difficult for online risks that are novel and abstract. This becomes even more problematic for older adults who may be less experienced with technology and thus less aware of the risks. Here risk communication can mediate education by facilitating behavior change. Therefore, there is a need to design risk communication technologies geared towards near term behavioral change in older adults.

If risk communication is to be effective its design must address the target demographic. There has been limited research in designs targeted specifically towards older adults. Designing for older adults is not the same designing for a generic end user. Aging has an effect on memory, cognition, and attention, including the older adults' ability to process information. Older adults, for example, can be overwhelmed by the information they are exposed to, if both the visual and the audio channel are simultaneously being used to communicate different information. Fisk et al.[10] recommend design guidelines for instructional technologies targeted towards older adults. They advocate against overload of sensory channels and avoidance of irrelevant data, while advocating for allowing time to reflect and internalize the material presented.

The underlying rational for these recommendations is to meet the needs of older adults who experience age related cognitive changes. In general, episodic memory deteriorates more quickly than semantic memory[2]. However, there are advantages to episodic memory. Older adults are more likely to retain content than context. This context is provided by episodic memory. Older adults also suffer disproportionally from irrelevant intrusions, i.e. when faced with a decision they are less able to determine the pertinent information that should occupy the working memory than when they were younger. This retrieval of pertinent information is better in episodic memory than semantic memory[4]. Thus, there are several advantages to using techniques that trigger episodic memory. These advantages consist of richer comprehension and contextualization as well as efficient and pertinent information retrieval.

Videos, rich in multi-sensory information, trigger episodic memory. Video-based narratives can provide richer comprehension than text[13]. Videos are coded in the episodic memory as compared to text, which is coded in the semantic memory. Episodic memory, though richer, requires more memory blocks[2,4]. Thus while retention periods may be smaller, videos can provide better understanding, for example of how security and privacy risks are realized online. Since episodic memory in older adults deteriorates more quickly than semantic memory[2], the assumption that videos would provide richer comprehension is largely untested. However, recent studies in cognition have been promising[4].

Another component of risk communication is using the appropriate mental models[6]. Mental models refer to internalized representations of external reality[6]. Camp[6] states that security experts predominantly use five mental models: physical, criminal, medical, warfare and market. Mental models of end users are not always aligned with security experts[3]. End users find physical/criminal mental models to be the most accessible[3]. Physical mental models can both lever-

age the affect heuristic as well as providing grounding of abstract online risks in a more tractable context.

Thus, our approach towards risk communication in this study combines insights from studies on cognition and mental models to develop video-based narratives grounded in physical analogies. Furthermore, we include risk mitigation and risk avoidance strategies in these video and text communications.

VIDEO DESIGN

In this section we give a description of the video design. We sought to design videos that leveraged physical/criminal mental models. Thus, we developed narratives that use analogies from the physical world to convey virtual risks. The two risks we targeted were phishing emails and mal- ware, in particular key loggers. These risks were chosen due to their strong financial impact. Research shows that the annual loss due to phishing, and possible gain to phishers, is $178.1M a year[14]. Malware also has significant financial impact. Small and mid-sized companies lost up to $40M in 2009 due to malware in United States.

The videos were designed to be a narrative with three parts:

1. Risk awareness: We show how someone might fall victim to a risk like a phishing or malware email.
2. Risk avoidance/Risk mitigation: We show how the victim can avoid or mitigate the risk by demonstrating alternatives to accepting the risk.
3. Risk in context: In (1) and (2) we used narratives based in physical analogues. In the third part we demonstrate how a similar scenario might play out on- line and bridge the gap between the offline analogy and the online risk. We also provide statistics to con- vey the severity of falling victim. Finally, we provide links to more information.

Fisk et al.[14] provide guidelines for designs targeted towards older adults. Some of our design decisions were contrary to the recommended guidelines. We found that providing both visual and audio stimuli at the same time would be preferable in a narration-based setting. Subtitles can be used and indeed add to the ease of comprehending the video. Though sub- titles provide the same information as the audio, they may be important for older adults who may suffer from impaired hearing.

Phishing

Phishing involves a criminal entity masquerading as a legitimate trustworthy entity to procure an individual's private information. So we took an example phishing email and presented it in two versions, text and video:

Text Version:

We used an example email:

Dear Mr. Cullen, We are from the IRS and we are writing regarding your retirement funds and bank accounts. It has come to your attention that their might be some discrepancies with respect to some of the transactions made from your accounts. We are conducting an investigation into this. We would like to get some information from you. Please click on the link at the bottom of the email and answer a few questions. Please make sure that you have your bank account number, password, and your social security number as you may be asked about them.

www.IRS.com

Regards IRS

From this email we can identify the key characteristics of a phishing email: (1) phishing emails appear legitimate; (2) they try to scare the victim. In this example the victim is supposedly being investigated by IRS for financial discrepancies; (3) they inquire about the victim's financial information like Social Security Number (SSN).

Video Version: Based on these characteristics we designed the physical narrative for the phishing video. We had an older adult pose as a target of the scam. We had an attacker who was dressed in a suit pretending to be an IRS agent. The agent carried credentials that appeared authentic. The agent came to the house of the older adult and informed him that he was under investigation due to financial discrepancies. The agent then asked for the older adult's financial information. In the first scenario the older adult, wanting to comply with the investigation, provided the information and thus was phished. In the second scenario the older adult refused to provide information until he could confirm the existence of the financial discrepancies. The older adult then called his bank to inquire about the said discrepancies and whether he was being investigated. Thus he discovers that the agent was a fraud. Finally we establish the connection between the physical analogy and the online risk, as shown in Fig. 1.

Fig. 1. Phishing websites, like the fake agent in our video, appear to be legitimate.

Malware

Malware is malicious software. It is hard to detect once installed and can potentially log critical authenticating information and send it to the attacker. Similar to the phishing emails, we had to identify the key characteristics of emails that encourage users to download malware.

Text Version:

We used an example email:

Dear Mr. Cullen, You have a secret valentine. Your secret love has sent you a singing telegram. To listen to the message and find out who your secret love is click on the link below.

secretvalentine.exe

Regards Your secret crush!

From this email we can identify the key characteristics of a malware email: (1) these emails appear to be from a friend or an acquaintance; (2) they may not reveal the identity of the sender; (3) They play on curiosity of the receiver; (4) They ask the receiver to download an attachment.

Video Version: Based on these characteristics we designed the physical narrative for the malware video. We had an older adult pose as the intended target. The attackers were two people pretending to deliver Valentine's Day messages. In the first scenario the older adult would let them in the house. One of the attackers then bugs the older adult's phone so that they can listen in on the older adult's conversation. In the second scenario the older adults does not let them in the house thereby thwarting the attack. In the last segment, we again draw the parallel between the physical analogy and the online risk, as shown in Fig. 2.

Fig. 2. Just like the bug, malware once installed captures sends it to the attacker.

STUDY DESIGN

While several efforts have been made to design risk communication technologies for risk education, they are usually evaluated experimentally with college students. This research specifically targets older adults. Older adults tend to have a different understanding of technology than younger adults. In particular they tend to be more cautious about technology. Recall, in this study we address two research questions. First, what is the effect on comprehension when using videos as opposed to text? Second, what are the determinants of older adults perception of online risk, specifically for responding to phishing and malware emails?

Research in cognition suggests videos provide richer comprehension. Conversely, there is evidence to show that older adults may feel overwhelmed by the use multiple of media in videos (visual, audio, text). There is also the question of assessing whether the physical analogies are accessible to older adults and if they understand how a similar attack might play out online. Older adults in general may be technology averse. Thus, we need to ensure that the design of the videos should not make them unduly anxious about technology or online financial management. Our design and research goal is that the videos result in avoidance of threat by older adults. A key goal of our study design was to determine if the videos or text better enabled older adults to clearly identify risk avoidance strategies.

In addition to answering these questions we sought to discover the determinants of risk. What are the characteristics of threats that are perceived as most risky? There is little research that explains the underlying determinants of online risk perception of older adults. In particular we seek to understand why or when older adults might disclose their financial information online or download an attachment. We also seek a better understanding of their mental models of online financial risk. Such an understanding would allow us to identify and address the key determinants in new designs for risk communication of this most vulnerable population.

In the next section, we describe the canonical nine dimensional model that we incorporated in the survey to measure risk perception. Further, we detail the design of questions that evaluate comprehension.

Determinants of Risk Perception

Identifying why and to what extent online threats may or may not be perceived as risky is necessary to design effective risk communication. Research in risk perception online has, however, been limited. Garg et al. investigated the applicability of a canonical nine dimensional model of risk perception based on expressed preferences[11].

The nine dimensional model was introduced by Fischhoff et al.[9] to study risk perception in the offline world. These nine dimensions were grounded in the psychometric paradigm and consisted of voluntariness, immediacy, knowledge to the exposed, knowledge to science, control, newness, common-dread, chronic-catastrophic, and severity. Garg et al.

found that not all the nine dimensions are equally relevant online[11] Specifically knowledge to the exposed, knowledge to science, newness, and common-dread were not found applicable. They proposed a five dimensional model consists of voluntariness, immediacy, control, chronic-catastrophic, and severity for online risks. These dimensions have been adapted for the current work as follows:

1. Voluntariness: To what extent does Mr. Cullen9 have a choice in being exposed to this risk? (1=Voluntary, 5= Involuntary)
2. Immediacy: Is the risk from the threat immediate or does it occur at a later time? (1=Immediate, 5=Delayed)
3. Control: To what extent can Mr. Cullen control (or mitigate) the risk? (1=Uncontrollable, 5=Controllable)
4. Chronic-catastrophic: Does this risk effect only Mr. Cullen or does it effect many people? (1=Mr. Cullen/Chronic, 5=Many People/Catastrophic)
5. Severity: In the worst possible outcome, how severe would the consequences be? (1=Not Severe, 5=Severe)

Comprehension: Video vs. Text

Research has shown that videos can lead to richer comprehension over text[13]. We measure comprehension of the videos by participants as follows: (1) they should be able to identify the risk; (2) they should be able to identify the attack vector; (3) they should be able to identify the potential consequences of the risk; (4) they should be able to suggest strategies to avoid or mitigate the risk.

In our beta test of the study design, we asked the participants close ended multiple choice questions, e.g. 'Why do you think the older adult was suspicious of the agent?' This sometimes biased the participants. For example, a participant may not feel that the older adult was suspicious of the agent. Once the question is asked, however, the participant might nevertheless think of justifications. Thus for the pilot our questions were open ended. Participants were asked the following questions: (1) what is phishing?; (2) how does phishing work?; (3) how can you avoid phishing?; (4) list everyone that suffers if a phishing attack is successful; and (5) describe the impact of phishing on the people or organizations listed above. The findings and responses to these questions are discussed later in the results section.

Procedure

The participants were asked to watch part of the first segment of the video, to the point where the fake agent asks the older adults to divulge the information. Participants were then asked to identify which they considered more risky: responding or not responding. Further, they rated both the risk of responding and not responding on the five dimensions of risk perceptions described previously. The rating was based on a five point semantic scale.

The participants were then shown the remaining section of the video. The participants were then asked to answer the comprehension questions. The participants were asked to think of themselves as the older adult in the video and the risk to them as that older adult.

RESULTS

Some iterative beta testing was conducted with ten older adults for both the phishing video and the evaluation survey during the design phase. Many of the older adults had trouble hearing the audio. In the second iteration we added subtitles to the video. While this was counter to the guidelines proposed by Fisk et al.[14] we found that in this particular case, older adults preferred having both the subtitles and the audio. Initially, the comprehension questions were close-ended and multiple choice. However, posttest interviews indicated that such an approach might prime the participants. Thus, the second iteration included only open-ended questions.

The following results were from the pilot studies with a convenience sample of older adults. The participants were randomly assigned to either the video or the text group. The pilot studies were conducted only for the phishing video. We had twelve participants in the pilot study. There were eight females and four males. Participants ranged in age from 70 through 85. Ninety-percent have adult children, with almost half having children living nearby. About 25% were married; the rest lived alone. All were mobile, healthy, and cognitively high functioning. Ninety-eight percent had attended college and six had graduate degrees. All were residents of a local, affluent retirement facility; most lived independently in cottage-style housing or apartments, but could take advantage of the central dining facilities and social activities.

A preliminary anonymous survey was administered to the group. Most participants were familiar with at least some form of information technology (computers, cell phones, etc.). A small minority used a medical alert bracelet or other personal safety-monitoring device; only a few had experience with any other monitoring or other home-based technologies. Six of the participants watched the videos and filled out the survey instrument based on the video. The other six read the textual description of the risks and filled out the survey instruments based on text. In the video group five of the participants were female and there was one male. In the text group there were three males and three females.

Video based survey

All six participants rated the risk of responding to be higher than that of not responding. The risk of responding consisted of: (1) IRS agent might use the information against the older adult; (2) The older adult did not have enough information to verify the authenticity of the IRS agent; (3) The older adult might become the victim of theft.

While the risk of responding was rated higher, not all items on the five dimensions are rated higher for responding. This indicates that not all dimensions have equal weights in the construction of perceived risk. While the sample size in this study is too small to allow statistical analysis to identify those weights, it does encourage further investigation.

The risks of not responding to the IRS agent were seen to be none at best and more visits from IRS at the worst. The characteristics of phishing were: (1) criminal act; (2) stealing private information or identity; and (3) impersonation of legitimate entities for financial gain. Participants had more difficulty explaining how they would identify phishing. Only two participants could make tangible proposals: companies would not ask for private information online and before providing information call the company and verify the requesting agent. Participants had an easier time explaining how to avoid phishing. Most participants recommended not giving out private or financial information online and not trusting emails. Participants identified themselves, their family, their bank, bank accounts, and businesses as entities that would suffer if they get phished. Financial loss was the most frequently identified consequence of being phished. Other outcomes were loss of privacy, trust, and decreased credit ratings.

Responding	Yes	No	Rating Scale
Voluntariness	2.5	3	1=Voluntary, 5=Involuntary
Immediacy	1.5	3.25	1=Immediate, 5=Delayed
Control	3	4	1=Uncontrollable, 5=Controllable
Chronic-catastrophic	3.75	3.25	1=Chronic, 5=Catastrophic
Severity	5	4.5	1=Not Severe, 5=Severe

Table 1. Average risk ratings for video group

Text based survey

All six participants rated the risk of responding higher than the risk of not responding. The risk of responding consisted of: (1) giving out too much information; (2) invasion of privacy.

None of the participants articulated the risk of not responding. Phishing was described as: (1) misleadingly or apparently legitimate, (2) email scam, and (3) procuring valuable personal or private information. Participants had more difficulty describing how they would identify phishing emails: (1) email can be identified as phishing based on the information requested, e.g. SSN; (2) strangers prying into private information; (3) sometimes it is difficult because it seems authentic, but no legitimate business would ask for personal information unsolicited; (4) the request includes information one should not share; (5) the proposal is often unrealistic and tries to offer a reward to the receiver for providing information or financial help that will hurt the receiver legally or financially.

Responding	Yes	No	Rating Scale
Voluntariness	1.8	2	1=Voluntary, 5=Involuntary
Immediacy	1.8	2.5	1=Immediate, 5=Delayed
Control	1.8	4	1=Uncontrollable, 5=Controllable
Chronic-catastrophic	3	2.75	1=Chronic, 5=Catastrophic
Severity	5	2.5	1=Not Severe, 5=Severe

Table 2. Average risk ratings for text group

Participants unequivocally suggested not responding to avoid being phished. Family members, person receiving the phishing email, and financial services companies were impacted due to successful phishing. Loss or money, dignity and privacy were seen as major outcomes of being phished. One of the respondents stated spouse gets mad as an outcome.

DISCUSSION

Participants in the video group were more likely to articulate the risk of responding or not responding than the text group. In the video group four participants provided a textual description of the risk of responding and three participants described the risk of not responding. In comparison, for the text group, only two participants enumerated the risk of responding and none indicated a risk of not responding. The risks of responding were also more concretely defined by the video group participants. For example participants in the video group stated theft as a risk of responding, which is much more tangible than the abstract loss of privacy offered as a risk by the text group. This suggests that participants in the video group had better comprehension of the risk than the text group.

All the participants in both the groups rated the risk of responding to be higher than the risk of not responding. In the video group, participants rated the risk of responding to be more voluntary, more immediate, less controllable, more catastrophic and more severe, as compared to the risk of not responding. In the text group, the risk of responding was seen as

less voluntary, more immediate, less controllable, more catastrophic, and more severe. Thus clearly participants in the video group felt that the victim had a choice in responding or not responding. The text group felt that they could not avoid the risk of their own volition.

Both the groups provided similar definitions of phishing. Both the groups had more difficulty explaining how to identify phishing than they had defining phishing. While both the groups recommended not responding to such emails to avoid getting phished there were subtle differences. Participants in the video group talked about the issue of trust and how there is no inherent trust in emails. This is important as it indicates that participants in the video group under- stood the underlying principle of phishing and similar email based scams as opposed to those in the text group.

Video group participants associated the risk of phishing more with personal loss. Two participants in the text group did not list themselves as entities that would be impinged if phishing were successful. One of the participants listed family first and themselves second. The participants in the video group were seen to use phrases like my bank, my social security number etc. They also more accurately described the financial risks. Instead of listing a generic financial service that would be effected, they gave specific examples, e.g. bank account numbers that would be compromised.

CONCLUSION AND FUTURE WORK

In this paper we presented the design of narrative driven risk communication videos targeted towards older adults. These videos targeted online financial risks of phishing and malware. We presented the design of these videos and an evaluation strategy. The results are promising in terms of communicating the risks of phishing attacks. The results are illustrative rather than conclusive and do not claim to provide a quantitative assessment. A larger study is in progress due to this successful pilot.

Participants who watched the video saw themselves and their assets as being more at risk when compared to those who read the text. Video participants were also able to articulate both the description of the risk and the implications of responding vs. not-responding in more concrete terms than the text group. This indicates that videos might be better at explaining online risks to older adults despite previous work arguing the converse.

The contribution of this work is not in the use of videos for training purposes. Rather this work presents guidelines for the development of narrative-driven videos that leverage physical mental models for risk mitigation online targeted towards older adults. We build upon previous work by presenting risk not as is, but by abstracting it to mental models that are more accessible to non-experts. Finally, we evaluate our design with older adults who differ from younger adults in their cognitive capacity. This demographic has been under served by previous studies, which have primarily concentrated on younger adults.

References

1. Anderson, K., “Consumer fraud in the United States: An FTC survey”, *Federal Trade Commission*, 2004.
2. Anderson, N. and Craik, F., “Memory in the aging brain”, *The Oxford handbook of memory*, pp. 411–425, 2000.
3. Asgharpour, F., Liu, D., and Camp, L. J., “Mental models of security risks”, *in: Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, pp. 367–377, 2007.
4. Aslan, A., Bauml, K., and Pastotter, B., “No inhibitory deficit in older adults’ episodic memory”, *Psychological Science*, Vol. 18(1), pp. 72, 2007.
5. Bertoni, D., “Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, But Vulnerabilities Remain: Congressional Testimony”, *DIANE Publishing*, 2009.
6. Camp, L.J., “Mental models of privacy and security”, *IEEE Technology and Society Magazine,* Vol. 28(3), pp. 37–46, 2009.
7. Camp, L.J. and Connelly K., “Beyond consent: privacy in ubiquitous computing”, *Digital Privacy: Theory, Technologies, and Practices*, pp. 327–343, 2008.
8. Connelly, K., Lorenzen-Huber, L., Shankar, K., and Camp, L.J., “ETHOS: Ethical Technologies in the Homes of Seniors”, *Submitted to special issue, Personal and Ubiquitous Computing*, 2009.
9. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B., “How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits”, *Policy Sciences*, Vol. 9(2), pp. 127–152, 1978.
10. Fisk, A., Rogers, W., Charness, N., Czaja, S. and Sharit, J., “Designing for older adults: Principles and creative human factors approaches”, *CRC*, 2009.
11. Garg, V. and Camp, L.J., “How safe is safe enough: Online”, *Workshop on Security and Human Behavior*, 2010.
12. Hasher, L., Stoltzfus, E., Zacks, R., and Rypma, B., “Age and inhibition”, *Journal of experimental psychology: Learning, Memory, and Cognition*, Vol. 17(1), pp. 163–169, 1991.
13. Herron, C., York, H., Corrie, C., and Cole, S., “A comparison study of the effects of a story-based video instructional package versus a text-based instructional package in the intermediate-level foreign language classroom”, *CALICO Journal*, Vol. 23(2), pp. 281, 2006.

14. Moore, T. and Clayton, R., “An empirical analysis of the current state of phishing attack and defense”, *in: Workshop on the Economics of Information Security*, 2007.
15. Morris, M., “Social networks as health feedback displays”, *IEEE Internet Computing*, pp. 29–37, 2005.
16. Robila, S. and Ragucci, J., “Don’t be a phish: steps in user education”, *ACM SIGCSE Bulletin*, Vol. 38(3), pp. 237–241, 2006.
17. Rowan, J. and Mynatt, E., “Digital family portrait field trial: Support for aging in place”, *in: Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 02–07, 2005.
18. Sharit, J., Hernandez, M., Czaja, S., and Pirolli, P., “Investigating the roles of knowledge and cognitive abilities in older adult information seeking on the web”, *ACM Transactions on Computer-Human Interaction (TOCHI)*, Vol. 15(1), pp. 1–25, 2008.
19. Wild, K., Boise, L., Lundell, J., and Foucek, A., “Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults”, *Journal of Applied Gerontology*, Vol. 27(2), pp. 181, 2008.
20. Willis, S., Schaie, K., and Martin, M., “Cognitive plasticity”, *Handbook of theories of aging*, pp. 295–322, 2009.