ABSTRACT

Older adults are more susceptible to fraud than younger adults offline. This may be true online as well. Older adults are also increasingly using the Internet for various activities, including managing their financial assets. Therefore, there is a need to develop risk communication technologies targeted towards older adults. These technologies should leverage mental models of end users to communicate risk in an accessible manner. Research in cognition suggests that risk communication using videos rather than text leads to improved comprehension and thus, better understanding of risks. We developed narrative-driven risk communication videos that address online fraud. These videos can be used for stand alone security education or as just-in-time decision aids. In this paper we present the design of such videos for phishing and malware. We also report results of a pilot study to measure the effectiveness of these videos. The study had twelve participants.

Categories and Subject Descriptors
H.1.2 [Models and Application]: User/Machine systems—human factors, human information processing

General Terms
Design, Human Factors, Security

Keywords
Older adults, Risk communication, Phishing, Malware, Video

1. 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 \textsuperscript{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 \cite{7}. By \textsuperscript{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 Federal Trade Commission over 20\% of the victims of financial fraud are older adults \cite{3}. 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 \cite{10}. Conversely, older adults are disproportionately inexperienced with information technology. They have less cognitive reserves and plasticity than younger cohorts \cite{32, 37}. 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 \cite{9}.

There is limited research examining older adults’ understanding of the risk generated by their digital data with respect to financial privacy and security \cite{28, 27, 31}. We propose to address this knowledge gap by creating a model of older adults’ understanding of their digital footprint and financial risk. Previous research has investigated providing security education to change existing mental models of online risks \cite{22}. The rationale has been to address attitudes and thereby improve behavior. However, attitudes do not always reflect behavior\cite{1}. Thus, we complement traditional...
approaches in security education with risk communication. Risk communication may facilitate behavioral experience, which can then inform attitudes [12].

Fischhoff [13] outlines an eight stage model for risk communication. The first stage consists of identifying the right information. The second stage consists of communicating that information to the appropriate target. The third stage constitutes explaining what that information means. Thus, merely presenting information about the risk only accounts for the first three stages. This has been the traditional approach in task based risk communication with the ubiquitous pop-up box. However, analogies grounded in physical mental models allow us to go a step further and show that non-experts have rejected similar risks in other domains. Our agenda in design and research is to engage elders as partners in risk communication. We leverage existing mental models to improve the effectiveness of risk communication designs. This approach can also inform existing strategies in security education by separating the notions of comprehension and attitudes from action and behaviors.

Thus, in this study we wanted to address the following research questions:

1. What is the effect on comprehension when using videos as opposed to text?
2. What are the determinants of older adults perception of online risk, specifically for phishing and malware emails?

Older adults generally express lower concerns about information privacy than population at large [36, 23]. 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 disproportionately suffer from increased sensitivity to irrelevant intrusions and are less able to selectively attend to information [17].

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. Section 2 is background and describes the rationale for our approach. Section 3 describes the design of the videos. Section 4 presents the design of the evaluation strategy. Section 5 presents the results of the pilot studies. Section 6 consists of discussion of the findings. Section 7 is conclusion and future work.

2. 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. Until recently, financial exploits occurred either in person or over the phone so assailants could be identified to family members, neighbors, and law enforcement. 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. For example, several studies have investigated the design of phishing education [22, 30, 33]. 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. [15] 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. Typical age related differences in memory include decreased working memory capacity, decrements in encoding and retrieving information, and declines in declarative memory. Episodic memory and semantic memory together form the declarative memory. Episodic memory retains rich sensory information and thus requires more processing and storage capacity. It usually retains personally experienced events as opposed to semantic memory which retains information about the world in a broad sense. Episodic memory deteriorates more quickly than semantic memory [24]. There are advantages to episodic memory. Older adults are more likely to retain content than context [34]. This context is provided by episodic memory. Older adults also suffer dis-

2Working memory refers to the temporary memory that stores information pertinent to immediate activities.
3Episodic memory is associated with contextual knowledge and autobiographical events such as emotions.
4Semantic memory is associated with conceptual and factual information.
proportionally 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 [6]. 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 [18, 29]. 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 [35]. 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 [4], the assumption that videos would provide richer comprehension is largely untested. However, recent studies in cognition have been promising [6].

Another component of risk communication is using the appropriate mental models [26]. Mental models refer to internalized representations of external reality [19]. A mental models approach has been used successfully to communicate risk in other fields such as environmental risks [20]. This has also been explored in security and privacy [8, 11]. Camp [8] 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 [5]. End users find physical/criminal mental models to be the most accessible [16]. Physical mental models can both leverage the affect heuristic as well as providing grounding of abstract online risks in a more tractable context.

Kapadia et al. [21] used the physical mental models of walls to propose a new design for access control. Adams et al. [2] use mental models of color perception, i.e. red—danger and green—safe, to propose a new design for privacy policy controls in electronic medical records. A similar approach has also been taken by Web of Trust. Web of Trust is a Mozilla plugin that informs the user whether a website is categorized as “safe” or red if it is “unsafe”. The Ambient Cube similarly uses a red/green metaphor [38]. While Adams et al., the Ambient Cube, and Web of Trust give users some indication of the legitimacy of web sites, none of these provide education to increase understanding of risk nor do they provide risk mitigation other than risk avoidance. The design of the Ambient Cube interaction does, however, address age-related cognitive changes. In contrast, our approach towards risk communication in this study, combines cognition and mental models insights to develop video-based narratives grounded in physical analogies. Furthermore, we include risk mitigation and risk avoidance strategies in these video and text communications.

3. 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 malware, 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 [25]. Malware also has significant financial impact. Small and mid-sized companies lost up to $40M in 2009 due to malware in United States6.

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 online and bridge the gap between the offline analogy and the online risk. We also provide statistics to convey the severity of falling victim. Finally, we provide links to more information.

Fisk et al. [15] provide guidelines for designs targeted towards older adults. Our findings were that the following recommendations were pertinent to our research:

1. Do not overload the visual sensory channel.
2. Do not overload both visual and auditory channels at the same time.
3. Avoid irrelevant data including ambient music or sounds effect.
4. Avoid presenting two different sets of information simultaneously.
5. Avoid presenting redundant information through different channels.
6. Present associated information in one place.
7. Present relevant graphics in addition to words.
8. Allow for reflection on the material presented.

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 subtitles provide the same information as the audio, they may be important for older adults who may suffer from impaired hearing.

5 www.mywot.com/ Last Accessed: March 10, 2011
3.1 Phishing

Phishing involves a criminal entity masquerading as a legitimate trustworthy entity to procure an individual’s private information. Criminals usually send out phishing emails to potential victims to get this information. The email usually contains a link that the victims are encouraged to follow. The victims then are asked to reveal sensitive information at the link locale e.g. social security numbers, bank account numbers. In order to design a physical narrative we had to identify the key characteristics of phishing emails. 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 phishing. 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.

3.2 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. Emails are one common vector for social engineering attacks that encourage victims to download malware. The emails usually contain an attachment. This attachment is offered for download as something benign e.g. valentine day cards, holiday music. The emails might also point to a webpage. The victim may be asked to navigate to this link to access potentially desirable products like free music. The webpage itself may have several links to desired content, e.g. music, movies. However, once the victim clicks on a link they receive malware instead of or in addition to the desired content. 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 valentines 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.

4. 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 the study we wanted to address the following research questions:

5The complete video is available here: www.youtube.com/watch?v=4ZQ9pFTCdy4

6The complete video is available here: www.youtube.com/watch?v=6zHjoZqrCB0
1. What is the effect on comprehension when using videos as opposed to text?

2. What are the determinants of older adults perception of online risk, specifically for responding to phishing and malware emails?

We have evaluated in a pilot study if videos impinge on comprehension as opposed to text. Research in cognition suggests videos provide richer comprehension. Conversely, there is evidence to show that older adults may feel overwhelmed by the multiple use 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.

### 4.1 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 [16]. The nine dimensional model was introduced by Fischhoff et al. [14] 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, newness, common-dread, chronic-catastrophic, and severity. Garg et al. found that not all the nine dimensions are equally relevant online [16]. 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. Cullen 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)

---

9Mr. Cullen is the name of the older adult in the video.
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)

4.2 Comprehension: Video vs. Text

Research has shown that videos can lead to richer comprehension over text [18, 29]. 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.
5. Describe the impact of phishing on the people or organizations listed above.

The findings and responses to these questions are discussed in Section 5.

4.3 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.

\textsuperscript{10}In the initial few studies the participants were asked to watch the entire first segment to the point where the older adults does give out his personal information to the attacker pretending to be an agent. This, however, biased the participants as they felt the information had already been given out and so they had already responded.

\textsuperscript{11}This is for the phishing video.
5. 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. [15] 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, post test interviews indicated that such an approach may 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.

5.1 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 nonexistent at best and more risks 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.

5.2 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.

Participants unequivocally suggested not responding to avoid being phished. Family members, person receiving the phishing email, and financial services companies were seen to be 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.

6. 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 understood 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.

### 7. 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 goal of this pilot was to determine if there were any differences between video and textual risk communication for online risks. The pilot study had twelve participants. However, to be able to truly measure the respective advantages of each media requires a much larger sample. The findings from this study have been encouraging and justify a further study with a larger sample.

In the phishing video the older adult is contacted by an ‘IRS’ agent. This is applicable in an American context. However, in other countries revenue services are known by other names, or may not exist in the form that they exist in United States. Similarly in the malware video the older adult receives a singing valentine. However, this may not be understood in cultures where Valentines Day is not celebrated. Thus future research includes exploration of how these videos might be modified to serve in a multi-cultural environment.

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.

---

<table>
<thead>
<tr>
<th>Table 1: Average risk ratings for video group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Responding</td>
</tr>
<tr>
<td>Voluntariness</td>
</tr>
<tr>
<td>Immediacy</td>
</tr>
<tr>
<td>Control</td>
</tr>
<tr>
<td>Chronic-catastrophic</td>
</tr>
<tr>
<td>Severity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Average risk ratings for text group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Responding</td>
</tr>
<tr>
<td>Voluntariness</td>
</tr>
<tr>
<td>Immediacy</td>
</tr>
<tr>
<td>Control</td>
</tr>
<tr>
<td>Chronic-catastrophic</td>
</tr>
<tr>
<td>Severity</td>
</tr>
</tbody>
</table>
Ethics

According to the rules of Indiana University we submitted our study design to the Institutional Review Board (IRB). This study was approved as minimal risk under exempt status by the IRB. Details available upon request.

Acknowledgments

We would like to thank Kelly Caine who provided insight in the development of the survey instrument. We would also like to thank Kurt Weisman, Dave Cooley, Lisa Borrello, Richard Burke and Allen Shyu for helping us shoot the videos.

8. REFERENCES


