Risk Communication Design: Video vs. Text

Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber

Indiana University
{gargv,ljcamp,connelly,lehuber}@indiana.edu

Abstract. There are significant differences between older and younger adults in terms of risk perception and risk behaviors offline. The previously unexplored existence of this dissimilitude online is the motivation for our work. What are the risk perceptions of older adults? How are these correlated with the classic dimensions of risk perception offline? Can we leverage episodic memory, particularly relevant for older adults, to increase the efficacy of risk communication? We conduct a survey based experiment with two groups: video (n=136) and text (113). We find that leveraging episodic memory using video risk communication can improve the ability of elders to avoid phishing attacks and downloading malware. The applicability of the dimensions of risk were different based not only the risk but also the mode of risk communication.

Keywords: Risk, Privacy, Video, Mental Models, Phishing, Malware.

1 Introduction

Emerging digital technologies are typically neither designed by or for older adults, increasing older adults' susceptibility to privacy violations. Older adults tend to be less experienced with technology than younger adults. With certain privacy risks, such as phishing, there is a tangible financial cost to the victims, their families and service providers. Older adults are the fastest growing demographic in United States [13] and they own a disproportional amount of financial assets [10]. They are also more susceptible to financial fraud offline [4], a vulnerability that may transfer online as well. Along with the rest of the population, older adults are being encouraged to use digital technologies to conduct financial transactions - technologies with which they are often unfamiliar. For example, from 2011, the United States Internal Revenue Services (IRS) will no longer mail tax forms to every household, encouraging online filing instead. For those who wish to file their taxes with paper forms, the forms would be available at local post offices. However older adults often have less mobility than young adults, and may not find the post office accessible. In addition, tax returns filed online are processed faster, further encouraging taxpayers to do so. However, online forms are unfamiliar to many, especially older adults. Thus, when an older adult receives a phishing email claiming to be from the IRS that requests them to click on a link to resolve discrepancies with their tax filing, they are likely to believe there has been a legitimate problem and will follow the link. Much has been said

S. Fischer-Hübner and M. Wright (Eds.): PETS 2012, LNCS 7384, pp. 279–298, 2012.

about younger adults, their use of social media, and their disregard for privacy. But older adults may (or may not) be very different in their privacy preferences [31] and in fact may be more likely to engage in risky behavior [51].

There have been two approaches to inform privacy decisions in end users: education [42] and risk communication [2]. Education is a long-term effort that targets risk comprehension and therefore attitudes. Older adults, however, have limited cognitive plasticity, affecting their ability and desire to understand the mechanics of privacy risks such as phishing. Since the goal is to inform behaviors, risk communication might be more pertinent. Thus, we examine the construction of perceived risk online for older adults. Research in risk communication for privacy risks is typically conducted with college undergraduates. Designing for older adults may have additional constraints [23] that arise from limitations on information retention and retrieval [46].

We compare textual and video risk communication. Both media types are built using physical mental models, based on previous research [6,25]. We begin the description of our work by placing it in the historical context of risk perception, and classic developments in risk communication in Section 2. Building on that context, we detail our methodology in Section 3. We present the results in Section 4. After discussing the results in Section 5, we conclude in Section 6.

2 Background and Related Work

The post World War II school of thought, regarding privacy was that of confidentiality, engendered from the privacy needs of the Cold War [39]. Thus, privacy was treated as an extension of security and privacy solutions were mostly technical, e.g. encryption. Information sharing can, however, be beneficial when it, for example, improves market inefficiencies [40]. That individuals share information does not imply a lack of concern for privacy. It merely emphasizes the limitations of privacy as confidentiality [28].

Privacy then becomes not just the ability to hide information, but also the ability to **control** information sharing. To that end there have been both technical solutions like Tor, as well as policy solutions like Do Not Track. Unfortunately, privacy solutions are often limited by their usability [50]. For example, deploying a Tor client requires a certain level of technical competence [18], which may hinder adoption [20]. This might be particularly critical for older adults who are less technically versed. At the same time, usability evaluations are usually done with younger adults, typically college undergraduates.

Previous risk studies have focused on the usability of privacy-enhancing technologies [14,45,19]. Here we focus of purposeful and accidental information-sharing, using phishing and malware respectively. Specifically we examine downloaded malware instead of drive-by malware because downloading requires user action. The goal is not to educate users so that they understand the underlying technical risks but rather to give them the skill set necessary to avoid the risk.

Privacy solutions, even when usable, are frequently not adopted [3]. Even privacy protections that require no technological expertise are not adopted. A recent example of this is the Do Not Track initiative. In terms of usability, all it requires is a click of a button to indicate that the user does not desire to be tracked. Despite the simplicity of it's design, figures indicate that less than 2% of Firefox users opt in [8]. At the same time, survey reports indicate that users are uncomfortable being tracked online. This disconnect between attitudes and behaviors, termed "the privacy paradox" [37], is also encountered offline and should not be surprising [43]. One explanation is our failure to contextualize privacy solutions appropriately [36]. The risk of information sharing is most salient during survey-based elicitation of attitudes. However, in context it would be the benefits of information sharing that are most easily available.

Bonneau et al. argue that it is rational for online service providers to hide the "privacy control interface and privacy policy to maximize sign-up numbers and encourage data sharing from the pragmatic majority of users" [11]. Thus, it is not a lack of user concern for privacy, rather a lack of clear signals that makes privacy solutions impotent [15]. The paradigm of rationality fails systematically and predictably for both security [41,26] and privacy decisions [3]. Our research seeks to address the deeper problem that privacy solutions are limited due to the designers' assumptions about a rational end-user by providing guidance on the systematic, potentially predictable, patterns of irrationality. How does rationality fail? And how can such failures be predicted by building on the foundations built by researchers focusing on offline risks? Ideally, privacy risks would be evaluated as the product of probability of occurrence and the magnitude of implications [9]. However, privacy risk decisions are often acted upon by external factors, e.g. control [12]. Brandimarte et al. noted that participants were more willing to share information when they had control over the publication of information, even though they had no control over access to that information or third party use. Thus, perceived control alleviates aversion to risk. Privacy decisions are then subjective, with end-users balancing perceived risk with perceived benefit. Fischhoff et al. [22] developed the canonical nine-dimensional model of perceived risk. This model has been used extensively to study perceived risk offline for a diverse set of risks, e.g. health risks [32] and environmental risks [24]. It has been used online to examine insider threats [21] as well as security risks [25]. The nine dimensions consist of voluntary, immediacy, knowledge to exposed, knowledge to expert, control, newness, common-dread, chronic-catastrophic, and severity. These have the potential to impact privacy decisions as well. Information sharing on social networks is done voluntarily, implying control and alleviating perceived risk. However, behavioral advertising raises privacy concerns as information is being involuntarily revealed [38]. The benefits of information sharing are immediate, while the consequences of privacy violations may appear delayed [1]. Thus, regrets about privacy risks might appear later [49]. Privacy risks are often not known to the end-user. Even when they are known, end-users may put too much value in expert opinion. Increased trust in expert systems can increase risky behavior. For example, drivers with ABS-enabled cars drive closer to other vehicles [33]. Similarly, perceptions of control can increase risky behavior [12]. Online privacy risks are newer than those offline. For example, information aggregation reveals information about end-users that would not be as easily accessible by individual bits of data. Humans understand averages better than aggregates [48]. When an end-user shares a single piece of information on Facebook, Google Plus, and Linked In, they evaluate it as one piece of information being shared on average, rather than as three pieces of information being shared. It would be even more difficult for end-users to account for a fourth piece of information being revealed as a result of the first three pieces being combined.

Common risks are dreaded less than rarely encountered risks. For example, terrorism appears more threatening than E. coli, despite the far higher death rates for the latter. Likewise, privacy risks are commonly encountered and thus may appear less threatening. Perceived risk is also directly proportional to the number of people at risk. Severity of risk consequences is also directly correlated with perceptions. Thus, decisions concerning risk are not strictly rational.

Risk decisions can be improved by a soft paternalistic nudge [2]. Nudging must impinge both the intuitive as well as the rational decision processes [44]. The effectiveness of intuitive systems is based on the decision system's ability to recognize risk [34]. Individuals respond irrationally to online risks in a manner analogous to offline risks. Ability to identify risk online is driven by the mental models that are used for representation [16]. Accessible mental models would make it easier for end-users to associate online risk with offline risks that they would be more familiar. When encountering an unfamiliar risk, individuals will be guided by their perceptions, not by the calculus of risk [17].

Previous work argued that security experts use five mental models: physical, criminal, warfare, medical, economic. End-users find physical mental models to be most accessible [6,25]. Thus, grounding risk communication designs in physical mental models would make user intuitions more informed.

Simultaneously, the effectiveness of a rule-based system is driven by its ability to extract the relevant information. The design of risk communication must then address information coding, storage, and retrieval. This is especially relevant for older adults who may have less cognitive plasticity compared to the younger adults [52]. The impact of aging on memory is severe [5], with retrieval becoming more difficult as older adults increasingly experience irrelevant intrusions (i.e. interruptions, unrelated information, or background noise) [29]. One approach to address bounds on cognition is by the use of richer media [30]. Videos, for example, are stored in the episodic memory [47] rather than semantic [35] as coding is based in context rather than content [46]. Previous research indicates that richer media can facilitate cognition [7], targeting episodic memory [47] rather than semantic [35]. Simultaneously, the use of appropriate mental models can make risk information more accessible [16]. Traditional online risk communication, however, uses text. Thus, there is a need explore video-based risk communication designs that privacy risks for older adults.

In this paper we present the design of narrative driven risk communication videos grounded in physical mental models. We present the evaluation of these videos by comparing them to traditional text based risk communication. We have designed these videos for older adults, thus our participant pool consists of adults older than 65 years of age. We examine the differences in perceived risk as experienced through different risk communication media. In the next section we present our methodology.

3 Methodology

We used an expressed preferences methodology to evaluate the difference between text and video based risk communication for phishing and malware risks. We conducted a survey-based experiment with two groups. Group 1, referred to as the video group, saw the risk information as a physical mental models based narrative presented in a video. Group 2, referred to as the text group read the risk information in a text form. Participants were randomly assigned to each group. Participant risk was minimized by following the ethics guidelines, for expedited studies, from Internal Review Board (IRB).

Participant recruitment and survey deployment was conducted by Knowledge Networks. Knowledge Network provides access to a representative sample of the U.S. population. They cover both online and offline populations, listed and unlisted phone numbers, households with or without phones as well as households with only cellular phones. Sampling frame is constructed using address based sampling (ABS) and random digit dialing (RDD). This is similar to methodology used by CDC for national immunization surveys. Participants are chosen at random from the sampling frame. Eligibility criteria is applied, i.e. participants need to be over 65. Over-sampling and under-sampling concerns are addressed by the use of post stratification weights. Despite a rigorous methodology there are always limitations. For example, even with ABS and RDD combined the sampling frame is constructed from 98% of the US population. However, the results can be considered to be reasonably generalizable.

Participants began by providing the consent to participate according to IRB guidelines. Participants provided demographic information: age, frequency of Internet use, frequency of cellphone use, as well as whether the participants lived alone or with other people. Participants were then shown text based or video based risk communication respectively. For each group half the participants rated their attitude towards the risk, i.e. which did they consider higher, the risk of responding or that of not responding. For example, for phishing emails the risk of responding would imply clicking on a link and providing personal information. The other half predicted their behavior in response to being exposed to the risk, i.e. are they more likely to respond (or not)?

Risk Communication Design: Participants were communicated the risk of phishing and malware. These risks were chosen due to their implications for identity theft, which could result in personal financial loss. This loss is more detrimental to older adults, as their ability to replace lost income is limited. The risk information was presented in text form to a subset of the participants, text group, and in video form to the rest, video group. Here we will discuss the design of both the text and video based risk communication. Due to space limitation we will discuss only phishing. A detailed discussion of the design process can be found in [27].

In order to minimize psychological risks, such as anxiety, we created a false persona of an older adult: Mr. Cullen. Participants were told that Mr. Cullen is a retired older adult who had just received an email. Then the participants were presented with a canonical phishing email:

Dear Mr. Cullen,
We are from the IRS and we are writing regarding your retirement funds and bank accounts. It has come to our attention that there 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 e-mail 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

The participants were then informed that Mr. Cullen clicked on the associated link and provided the relevant information.

To present this information in the video form, we first identified the key characteristics of phishing from the above email. First, phishing emails appear legitimate. Secondly, they try to scare the recipient. Finally, they ask for the email recipient's financial information. Based on these characteristics we developed a mental models based narrative grounded in a physical analogy. This narrative was later developed into a video. For consistency, the victim in the video was also an older adult. The attacker had to be a legitimate financial entity. Again for consistency we chose an IRS agent, or rather an attacker pretending to be one. Thus, the agent fashioned credentials that appeared authentic. The agent contacted the older adult at home and informed him that he was under investigation due to financial discrepancies. The agent then asked for the older adult's financial information. The older adult, wanting to comply with the investigation, provided the information and, thus, was phished.

Risk Assessment: Text based risk communication would impinge perceived risk differently from risk videos[1]. Half the participants identified whether they felt the risk of responding to the risk was higher than *not responding.* The remaining participants predicted their behavior, i.e. if they would respond to the risk or *not respond.* Participants rated the perceived benefit of responding to the risk on a seven point Likert scale (1=Not beneficial; 7=Highly beneficial). Participants also rated the perceived risk of responding on seven point Likert scale (1=Not risky; 7=Highly risky).

Risk of responding was also evaluated on a nine dimensions of perceived risk identified by Fischhoff et al. [22]. Since its inception in 1978, this model has been used extensively to study risks in a diversity of domains including health

[1] Phishing Video: `http://www.youtube.com/watch?v=4ZQ9pFTCdy4`
Malware Video: `http://www.youtube.com/watch?v=6zHJoZqrCB0`

and environmental risks. Participants were asked to rate the perceived risk of responding to phishing and malware risks on each of the nine dimensions. The rating was on a five point like scale and the dimensions were defined as:

1. Voluntary: 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. Knowledge to the exposed: How much would a person like Mr. Cullen know about the implications of this risk? (1=Knows a lot; 5=Knows nothing)
4. Knowledge to the expert: How much would an expert know about the implications of this risk? (1=Knows a lot; 5=Knows nothing)
5. Control: To what extent can you control (or mitigate) the risk? (1=Uncontrollable; 5=Controllable)
6. Newness: Is this a new risk resulting from new technologies or is it a new version of an old risk? (1=Old; 5=New)
7. Common-Dread: Is this risk commonplace or rarely encountered? (1=Common; 5=Rare)
8. Chronic-catastrophic: Does this risk affect only Mr. Cullen or does it affect many people? (1=(Mr. Cullen) Individual; 5=(Many People) Global)
9. Severity: In the worst possible outcome, how severe would the consequences be? (1=Not Severe; 5=Severe)

4 Results

There were a total of 249 participants. There were 113 participants in the text group and 136 participants in the video group. 49 of the participants lived alone. 26 of those participated in the text group, while 23 participated in the video group. 199 participants lived with other people. 86 of those participated in the text group, while 113 participated in the video group. 122 of the participants were men, 56 of whom were in the text group and 66 in the video group. There were 127 women participants, of which 57 read the text and 70 saw the video.

The mean time for completing the text survey was 219.3186 minutes, while that for completing the video survey was 303.6103 minutes. There was no statistically significant difference between the mean time taken by each group, $p < .05$. The high values from mean time to complete are due to a handful of participants taking over 6000 minutes to complete the survey, i.e. several days. Thus, we also computed the medians.

The median time of completion for the text survey was 21 minutes and that for the video survey was 30.5 mins. Medians were compared by using Mann-Whitney or two-sample Wilcoxon test. This non-parametric test makes two assumptions: (1) the distribution is continuous, and (2) that the shape of the distribution of both samples is similar. Since time is a continuous variable assumption one is justified. For the second assumption, both distributions were heavily right skewed. The lower bound was 0 while the upper bound was less than 6500 minutes. On conducting a one sided test, the time to complete was significantly different between text and video; w=4851.5, p-value=2.762e-07. Participants in the video group took more time to complete the survey than those in the text group.

Risk Attitudes: The risk of responding to phishing emails is often underestimated. Phishing emails create anxiety in recipients, thereby making the risks of not responding salient, while appearing to alleviate the risks of responding; e.g. 'If you do not contact us on the following, your account may be closed'. Thus, participants were asked if they considered the risk of responding to be greater to than the risk of not responding to phishing. 62 participants answered this question for text while 65 answered this for video. 38 participants in the text group indicated responding to the email was more risky, while 48 participants indicated responding to the agent with the information was more risky. Test of proportions did not indicate a statistically significant difference; p-value= 0.1439.

Similarly, participants were asked if they considered the risk of responding to be greater to than the risk of not responding to malware. 62 participants answered this question for text while 64 answered this for video. 53 participants in the text group indicated responding was more risky, while 62 participants in the video group indicated that responding was risker. One sided test of proportions was *statistically significant*, p=0.02565.

Predicted Behavior: Even when the risk of responding is perceived to be greater, participants may choose to respond, as the implications might, for example, appear more controllable [12]. Thus, we asked participants to indicate their likely action in response to the phishing attack if they had indicated that responding was riskier than not responding (n=51 for text and n=72 for video). All text participants said that they would not respond, while 71 video participants said they would not respond. Test of proportions did not indicate a statistically significant difference; p-value= 1.

We also asked participants to indicate their likely action in response to the malware scenario if they had indicated that responding was riskier than not (n=52 for text and n=72 for video). 49 text participants said they would not respond, while 69 video participants said they would not respond. Test of proportions was not statistically significant; p-value=0.2858.

Perceived Benefit: Participants rated the benefit of responding to phishing risk on a seven point Likert scale (1=not beneficial at all; 7=highly beneficial). The mean benefit for the text group was 1.372881, while that for the video group was 1.828125. An independent two sample T-test did not indicate statistically significant difference. Participants rated the benefit of responding to malware risk on a seven point Likert scale (1=not beneficial at all; 7=highly beneficial). The mean benefit for the text group was 1.271186, while that for the video group was 1.281250. An independent two sample T-test did not indicate statistically significant difference.

Perceived Risk: Participants rated the risk of responding to phishing on a seven point Likert scale (1=not risky; 7=highly risky). The mean risk for the text group was 6.814815, while that for the video group was 6.830986. An independent two sample T-test did not indicate statistically significant difference. Participants rated the risk of responding to malware on a seven point Likert scale (1=not risky; 7=highly risky). The mean risk for the text group was 6.018868, while that for the video group was 6.555556. An independent two sample T-test indicates *statistically significant* difference, p=0.002392.

Table 1. Mean Risk Ratings of Fischhoff's nine dimensions

	Phishing			Malware		
Text vs. Video	Text	Video	p-value	Text	Video	p-value
Voluntary	2.389381	1.992593	0.02683	1.651786	1.955882	0.04183
Immediacy	1.876106	2.318519	0.005024	2.063063	2.977941	8.346e-07
Exposed	3.723214	3.830882	> 0.05	3.732143	4.082707	0.004020
Expert	1.153153	1.110294	> 0.05	1.099099	1.186567	> 0.05
Control	1.783784	2.514706	7.385e-05	3.027027	2.851852	> 0.05
Newness	2.765766	2.463235	> 0.05	3.442478	3.432836	> 0.05
Common Dread	1.781818	1.733333	> 0.05	1.928571	2.373134	0.0007834
Chronic-Catastrophic	3.919643	4.066176	> 0.05	3.814159	4.073529	0.04495
Severity	4.855856	4.867647	> 0.05	4.548673	4.850746	0.0001627

4.1 Nine Dimensional Model

Participants rated the risk of responding to phishing and malware on Fischhoff's nine dimensions of perceived risk. Table 1 reports the mean rating given for each dimension as well as the p-values of one sided T-tests between text and video. Participants rated the voluntary nature of risk (1=Voluntary; 5=Involuntary). Text and video were statistically different for both phishing as well as malware. While for phishing the risk of responding was more voluntary for the video group, for malware risk of responding was more voluntary for text. Participants rated the immediacy of the impact of risk (1=Immediate; 5=Delayed). The consequences of responding were more delayed for the video than for text, in both phishing as well as malware. Participants rated the knowledge a typical victim would have regarding the risk (1=Knows a lot; 5=Knows nothing). There was no statistical difference between text and video for phishing. However, knowledge to the exposed was higher in the video group for malware. The relationship of perceived risk with voluntary, immediacy, and knowledge to exposed is shown in figure 1.

Participants rated the knowledge an expert would have regarding the implications of phishing or malware (1=Knows a lot; 5=Knows nothing). There was no statistically significant difference between text and video for either phishing or malware. Participants rated the extent to which they can control the risk consequences (1=Uncontrollable; 5=Controllable). Phishing risk was more controllable for video than for text, while the difference was not statistically significant for malware. Participants rated the newness of phishing or malware (1=Old; 5=New). There was no statistically significant difference between text and video for either phishing or malware. The relationship of perceived risk with knowledge to expert, control, and newness is shown in figure 2.

Participants were asked to rated how common they considered the risk to be (1=Common; 5=Rare). Participants also rated whether the risk impact just the victim or if the risk was global (1=Individual; 5=Global). Finally, participants rated the severity of the consequences of phishing (1=Not Severe; 5=Severe). The difference between text and video was not statistically significant for phishing on these three dimensions. However, for malware the difference was statistically significant. Video risk was more rare, catastrophic, and severe, compared to text. The relationship of perceived risk with common-dread, chronic-catastrophic, and severity is shown in figure 2.

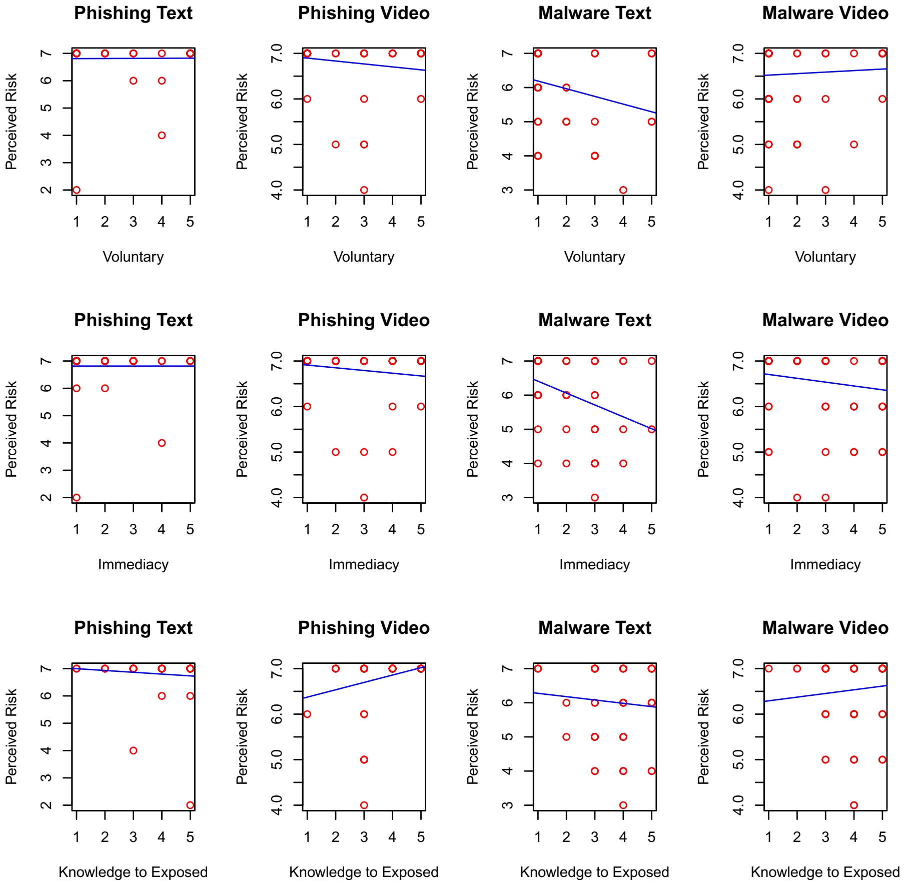

Fig. 1. Perceived Risk vs. Voluntary, Immediacy, and Knowledge to Exposed

4.2 Regression Analysis: Perceived Risk vs. Nine Dimensions Model

Figures 1-3, note that the relationship between perceived risk and the nine dimensions is linear. Thus, linear regression analysis is applicable. We then identified the best fit model, i.e. the subset of the nine dimensions that best explain variance in perceived risk. Thus, we isolated the relevant dimensions evaluate their ability to explain perceived risk.

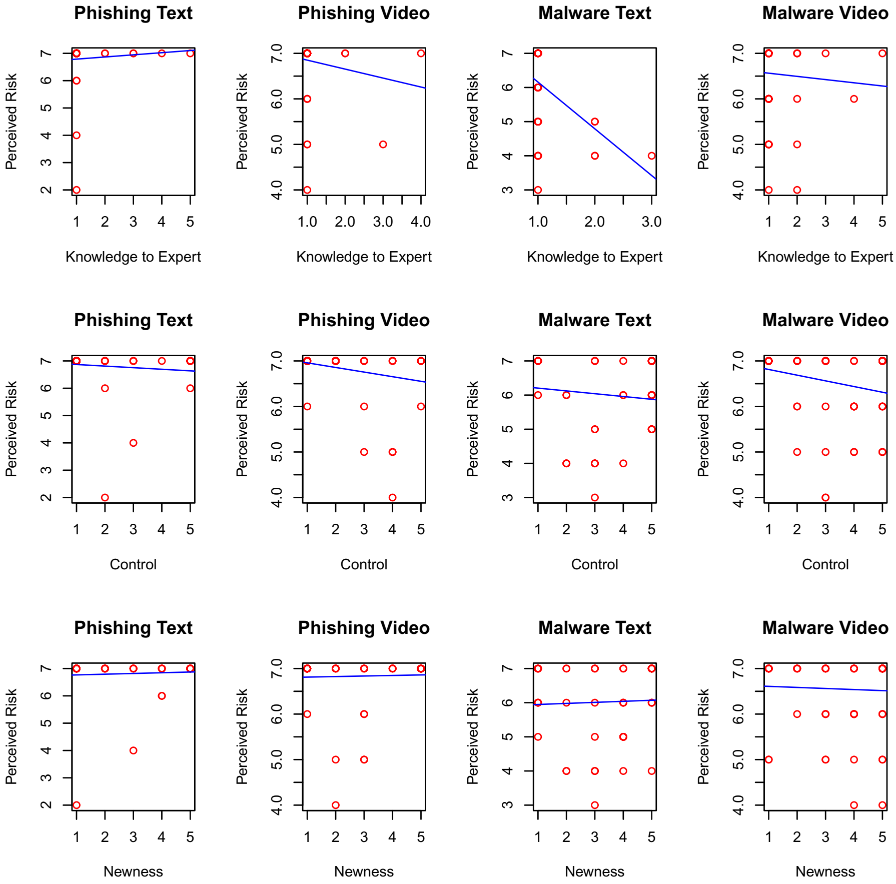

Fig. 2. Perceived Risk vs. Knowledge to Expert, Control, and Newness

We considered additional variables: (1) time taken to complete the survey, (2) whether the participant lived alone or not, (3) frequency of Internet use, and (4) frequency of cellphone use. These will be referred to as confounding variables. We measure the models explanatory power by examining *adjusted* R-square values, rather than raw R-square values. *Adjusted* R-square: 1) accounts for collinearity of independent variables, and 2) adjusts for extra variables. We first conducted the analysis for phishing text. The dependent variable was perceived risk, while the independent variables were the nine dimensions. The R-square value was negative with the complete nine dimensional model. Reducing the dimensions improved the model's explanatory power. Best fit for the model was given by severity, common dread, knowledge to the exposed, knowledge to expert, and chronic-catastrophic; R square=0.03208, p=0.27776. Adding the confounding variables further improved the model's explanatory power. The best fit for the model was given by immediacy, common dread, knowledge to expert, frequency of internet use, and cellphone use; R-square=0.1921, p=0.01468.

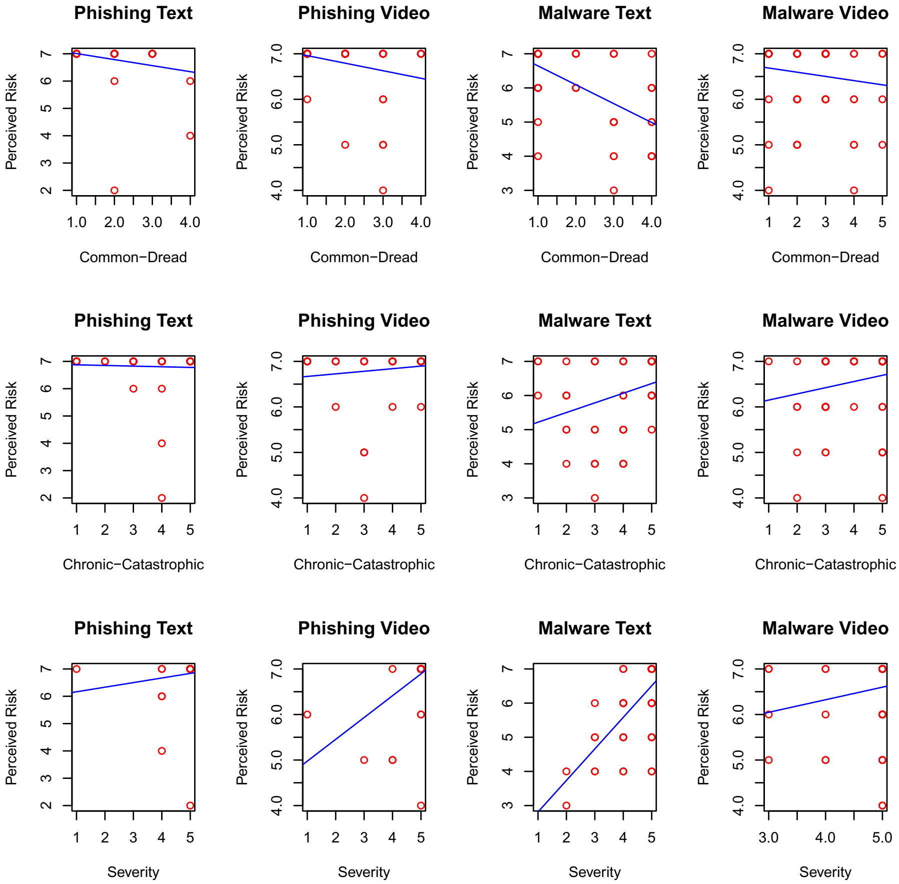

Fig. 3. Perceived Risk vs. Common-Dread, Chronic-Catastrophic, and Severity

Next we conducted the analysis for phishing video. With just the nine dimensions as the independent variables the model has good explanatory power; R square= 0.2494, p= 0.001391. Severity was statistically significant. Best fit for the model was given by voluntary, knowledge to the exposed, control, severity;

R square= 0.2849, p=2.633e-05. Knowledge to the exposed and severity were statistically significant. Adding the confounding variables did not increase the explanatory power of the model.

For malware, again, we first analyzed text. With perceived risk as the dependent variable and the nine dimensions as independent variable the model had significant explanatory power; R-square =0.6082, p=7.981e-07. Knowledge to expert, severity, and chronic-catastrophic were statistically significant. Best fit was given by voluntary, severe, newness, common-dread, knowledge to exposed, knowledge to expert, and chronic-catastrophic; R-square=0.6511 p-value=3.133e-09. Again knowledge to expert, severity, and chronic-catastrophic were statistically significant. Adding the confounding variables did not increase the model's explanatory power.

However, for malware video perceived risk was not explained by the nine dimensional model; R-square value was negative. Reducing the dimensions improved the performance slightly. Best fit was given by control, immediacy and chronic-catastrophic; R-square=0.06659 p=0.05139. Adding the confounding variables and reducing dimensions, the best fit was given by control, knowledge to the exposed, and frequency of Internet use; R-square=0.09577, p=0.02179. Control was the only statistically significant dimension.

4.3 Factor Analysis

We were also interested in the underlying structure of the nine dimensional model, specifically how it different for video vs. text as well as phishing vs. malware. Thus, we are interested in the differences between not just media but also the nature of the risks. To analyze the underlying structure we conducted exploratory factor analysis. To determine the number of factors, we conducted Scree test; figure 4. We consider eigenvalues greater than 1. Thus, we consider four factors for each scenario.

We conducted factor analysis using R's inbuilt factors analysis function factanal with varimax rotation and pairwise deletion of missing values. Tables 2, 3, 4, and 5 show the factor loadings for the different factors, the communalities for the nine dimensions, and the variance explained by the four factors.

5 Discussion

The hypotheses that this research examines are two: 1) videos are more effective risk communication media than text for older adults, and 2) perceived risk can be grounded in Fischhoff's nine dimensional model. To test the first hypothesis we examined the difference in participants' attitude towards responding to risk, predicted behavior, ranking of perceived benefit and perceived risk.

Unlike voluntary, immediacy has the same relationship with perceived risk for text as well as video, for phishing as well as malware. When the risk is immediate

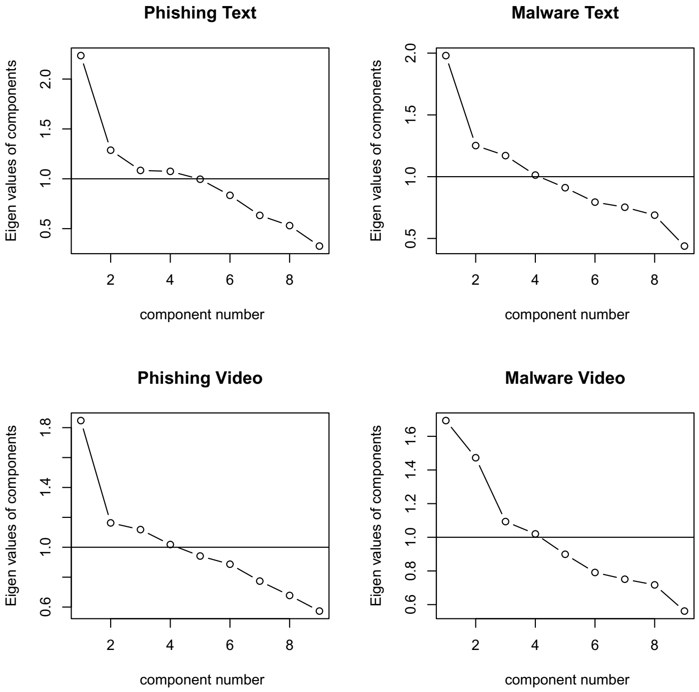

Fig. 4. Scree Test

Table 2. Phishing Text Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Communality
Voluntary			0.979	0.189	0.995
Immediacy	0.157	0.232	0.112	0.211	0.136
Knowledge to Exposed			0.182		0.040
Knowledge to Expert	0.570				0.340
Control	0.175	0.979			0.995
Newness		0.186	0.106		0.047
Common-Dread	0.123	0.411	-0.222	0.873	0.995
Chronic-Catastrophic				-0.145	0.027
Severity	-0.957	-0.150		-0.226	0.995
Proportion Var	0.146	0.139	0.120	0.103	
Cumulative Var	0.146	0.285	0.405	0.508	

it is perceived to be more risky, when the effects are delayed, less so, figure 1. Thus, a lower value for immediacy informs perceived risk better. Thus, text was better than video at informing perceived risk. For both phishing and malware, participants in the text group perceived the impact of risks to be more immediate than delayed.

Table 3. Phishing Video Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Communality
Voluntary				0.199	0.043
Immediacy	-0.111	0.233	0.151	0.354	0.215
Knowledge to Exposed			-0.347		0.124
Knowledge to Expert	-0.192	0.148	0.129		0.082
Control	-0.144	0.971			0.965
Newness		0.128			0.025
Common-Dread	-0.195		0.817	0.109	0.721
Chronic-Catastrophic	0.132			-0.629	0.417
Severity	0.991		-0.105		0.995
Proportion Var	0.124	0.116	0.094	0.065	
Cumulative Var	0.124	0.239	0.334	0.399	

Table 4. Malware Text Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Communality
Voluntary	0.219	-0.319			0.157
Immediacy		-0.355	0.119		0.154
Knowledge to Exposed			-0.160		0.032
Knowledge to Expert	0.977	-0.113	0.138		0.995
Control			0.792		0.629
Newness		0.279	-0.173	0.363	0.246
Common-Dread	0.187	-0.292	0.165	0.581	0.485
Chronic-Catastrophic		0.139		-0.383	0.168
Severity		0.801	0.120	-0.203	0.706
Proportion Var	0.119	0.118	0.085	0.075	
Cumulative Var	0.119	0.237	0.322	0.397	

Table 5. Malware Video Factor Loadings

	Factor 1	Factor 2	Factor 3	Factor 4	Communality
Voluntary				0.278	0.086
Immediacy		0.802			0.649
Knowledge to Exposed			0.390	0.292	0.244
Knowledge to Expert			-0.372		0.142
Control	0.114	0.159	-0.339		0.155
Newness		0.225		0.418	0.232
Common-Dread	0.719	0.247		0.266	0.650
Chronic-Catastrophic	-0.439			0.214	0.245
Severity	-0.254			0.430	0.256
Proportion Var	0.089	0.089	0.071	0.046	
Cumulative Var	0.089	0.178	0.249	0.295	

For knowledge to the exposed, the results were mixed. There was no statistical difference in means values for phishing text and video. However, in general higher knowledge led to higher perceived risk. The importance of this is reinforced in the linear regression model for phishing video, where knowledge to exposed is one of the dimensions in the best fit model, and is also statistically significant. For malware, knowledge to the exposed was rated lower in text than in video. However, in text lower knowledge led to higher perceived risk, while in video the relationship was reversed. Knowledge to exposed was present in the best fit models of both text and video, but was only statistically significant in text. Thus, it is unclear if text or video are better at leveraging this dimension. Knowledge to the expert was similar between text and video, for both phishing and malware. Knowledge to the expert, in general tends to reduce perceived risk. It would then lead to more risk taking behaviors. Knowledge to the expert was in the best fit model for phishing text and malware text. It was not statistically significant for phishing text, however, for malware text it was significant. Thus, text based risk communication, for malware, may lead to more risk taking behaviors based on knowledge to experts.

Control had a consistent relationship with perceived risk. Uncontrollable risks were perceived more risky, figure 2. For phishing, text group perceived phishing risk to be more uncontrollable than video group. Control was in the best fit model for both phishing video and malware video. It was statistically significant for malware video. Thus, video based risk communication would lower perceived risk on the control dimension.

Newness was similar for both text and video, for phishing as well as malware. Newness was only in the best fit model of malware text. However, it was not statistically significant. In general, newer risks were perceived to be more risky. However, there does not seem to be much evidence of newness having a significant impact on perceived risk.

Common-dread had a consistent relationship with perceived risk. Common risks were perceived to be less risky than those rarely encountered. The difference between phishing text and phishing video was not significant. The difference for malware was significant. Text group perceived malware to be more common than video. Common-dread was in the best fit models for text but not for video. Thus, text based risk communication may alleviate perceptions of risk by making them appear common. Chronic-catastrophic did not have a significant impact on phishing text. For phishing video and malware, both text and video, risks that impact more people were perceived to be more risky. The difference between phishing text and video was not statistically significant. The difference for malware was significant. Malware was seen to impact more people for video than for text. Chronic-catastrophic was in the best fit model for both malware text and malware video. It was statistically significant for malware text. Thus, text based risk communication might alleviate perceptions of malware risk.

Severity had a significant impact on perceived risk. More severe risks were perceived as more risky. The difference between phishing text and video was not significant. For malware the difference was significant. Malware risks were perceived more severe for video than for text. Severity was in the best fit model for malware text, and was statistically significant. Malware appears less severe in text than video. Thus, perceived risk might be lower for text than video.

6 Conclusion and Future Work

Recall the purpose of our experiments was to test two hypotheses. The first is that grounding risk communication in mental models empowers older adults (who are not familiar with information technology) to avoid common threats. We built on previous findings for mental models, using physical mental models. We concluded that video was more effective in making risk salient and perceived as severe; yet the prediction of behaviors was not significantly different between text and videos.

The second hypothesis was that online risk perceptions could be understood using the classic dimensions of offline risks. The perceptions differed based on the presentation of the risk and the risk itself; however, in any case there were multiple significant dimensions. Knowledge to experts was stronger in the case of text; thus text may perversely increase risk-seeking. Perceptions of severity were greater with video than text. The perception of a risk as voluntary for phishing made the risk more salient in the case of text and less so in video. Text made the risk appear more immediate and in the case of malware, less voluntary. Neither risk, reasonably so, was seen as particularly dreadful. Perceptions of severity had by far the greatest impact on perceived risk. Neither knowledge to the exposed nor newness were significant in either case.

The use of mental models proved effective in providing strategies for risk mitigation and illustrating the severity of risk; thus mental models rather than exact technical information are more powerful in decreasing potentially hazardous information-sharing. The use of video to leverage episodic memory proved somewhat mixed; yet on the most significant variable (i.e., severity) video proved more effective. Risk communication is more effective when grounded in the risk itself (e.g., phishing) than in the technical vector in which the risk is embedded. We conclude that targeting risk communication using videos and mental models has the potential to be extremely effective in the (also extremely vulnerable) online population of older adults.

Acknowledgements. We would like to thank Dr. Kelly Caine who assisted us at various stages of the research. We also acknowledge the insights provided by the Stat/Math center at Indiana University. Any mistakes are, however, authors' own responsibility.

This material is based upon work supported, in part, by the National Science Foundation under Grants NSF IIS 1036918 and NSF CNS 0943382. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

1. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce, pp. 21–29. ACM (2004)
2. Acquisti, A.: Nudging privacy: The behavioral economics of personal information. IEEE Security & Privacy 7(6), 82–85 (2009)
3. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1), 26–33 (2005)
4. Anderson, K.: Consumer fraud in the United States: An FTC survey. Federal Trade Commission (2004)
5. Anderson, N., Craik, F.: Memory in the aging brain. The Oxford Handbook of Memory, 411–425 (2000)
6. Asgharpour, F., Liu, D., Camp, L.J.: Mental Models of Security Risks. In: Dietrich, S., Dhamija, R. (eds.) FC 2007 and USEC 2007. LNCS, vol. 4886, pp. 367–377. Springer, Heidelberg (2007)
7. Aslan, A., Bäuml, K.H., Pastötter, B.: No inhibitory deficit in older adults' episodic memory. Psychological Science 18(1), 72 (2007)
8. Bachman, K.: Study: Internet user adoption of dnt hard to predict. Tech. rep., AdWeek (March 2012), `http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091`
9. Bernstein, P.: Against the gods: The remarkable story of risk. John Wiley & Sons Inc. (1998)
10. Bertoni, D.: Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, But Vulnerabilities Remain: Congressional Testimony. DIANE Publishing (2009)
11. Bonneau, J., Preibusch, S.: The privacy jungle: On the market for data protection in social networks. Economics of Information Security and Privacy, 121–167 (2010)
12. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced confidences: Privacy and the control paradox. In: Workshop of Economics and Information Security (WEIS). Harvard University (2010)
13. Breau, C.: Projected population of the united states, by age and sex: 2000 to 2050. Tech. rep., U. S. Census Bureau (2000), `http://www.census.gov/population/www/projections/usinterimproj/`
14. Brodie, C., Karat, C.M., Karat, J., Feng, J.: Usable security and privacy: a case study of developing privacy management tools. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS 2005, pp. 35–43. ACM, New York (2005)
15. Camp, L.J.: Reliable, usable signaling to defeat masquerade attacks. ISJLP 3, 211 (2007)
16. Camp, L.J.: Mental models of privacy and security. IEEE Technology and Society Magazine 28(3), 37–46 (2009)
17. Camp, L., McGrath, C., Genkina, A.: Security and morality: A tale of user deceit. In: Models of Trust for the Web (MTW 2006), Edinburgh, Scotland, vol. 22 (2006)
18. Clark, J., Van Oorschot, P., Adams, C.: Usability of anonymous web browsing: an examination of Tor interfaces and deployability. In: Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 41–51. ACM (2007)
19. Cranor, L., Garfinkel, S.: Security and usability: Designing secure systems that people can use. O'Reilly Media, Inc. (2005)

20. Dingledine, R., Mathewson, N.: Anonymity loves company: Usability and the network effect. In: Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, UK (June 2006)
21. Farahmand, F., Spafford, E.H.: Understanding insiders: An analysis of risk-taking behavior. Information Systems Frontiers, 1–11 (2010)
22. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. Policy Sciences 9(2), 127–152 (1978)
23. Fisk, A.D., Rogers, W.A., Charness, N., Sharit, J.: Designing for older adults: Principles and creative human factors approaches, vol. 2. CRC (2009)
24. Flynn, J., Slovic, P., Mertz, C.K.: Gender, race, and perception of environmental health risks. Risk Analysis 14(6), 1101–1108 (1994)
25. Garg, V., Camp, L.J.: End user perception of online risk under uncertainty. In: 45th Hawaii International Conference on System Sciences. IEEE (2012)
26. Garg, V., Camp, L.J.: Heuristics and biases: Implications for security and privacy (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933957
27. Garg, V., Camp, L.J., Lorenzen-Huber, L.M., Connelly, K.: Risk communication design for older adults. In: ISG*ISARC 2012. International Society for Gerontechnology (in press, 2012)
28. Gürses, S., Berendt, B.: Pets in the surveillance society: A critical review of the potentials and limitations of the privacy as confidentiality paradigm. Data Protection in a Profiled World, 301–321 (2010)
29. Hasher, L., Stoltzfus, E., Zacks, R., Rypma, B.: Age and inhibition. Journal of Experimental Psychology: Learning, Memory, and Cognition 17(1), 163–169 (1991)
30. Herron, C., York, H., Corrie, C., 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 23(2), 281 (2006)
31. Hoofnagle, C.J., King, J., Li, S., Turow, J.: How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? SSRN eLibrary (2010)
32. Johnson, B.B., Slovic, P.: Presenting uncertainty in health risk assessment: initial studies of its effects on risk perception and trust. Risk Analysis 15(4), 485–494 (1995)
33. Jonah, B.A., Thiessen, R., Au-Yeung, E.: Sensation seeking, risky driving and behavioral adaptation. Accident Analysis & Prevention 33(5), 679–684 (2001)
34. Kahneman, D., Frederick, S.: Representativeness revisited: Attribute substitution in intuitive judgment. Heuristics and Biases: The Psychology of Intuitive Judgment, 49–81 (2002)
35. Lövdén, M., Rönnlund, M., Wahlin, Å., Bäckman, L., Nyberg, L., Nilsson, L.G.: The extent of stability and change in episodic and semantic memory in old age: Demographic predictors of level and change. The Journals of Gerontology Series B: Psychological Sciences and Social Sciences 59(3), 130 (2004)
36. Nissenbaum, H.F.: Privacy in context: Technology, policy, and the integrity of social life. Stanford Law & Politics (2010)
37. Norberg, P.A., Horne, D.R., Horne, D.A.: The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs 41(1), 100–126 (2007)
38. Phelps, J., Nowak, G., Ferrell, E.: Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 27–41 (2000)

39. Posner, R.A.: Right of privacy, the. Ga. L. Rev. 12, 393 (1977)
40. Posner, R.A.: The economics of privacy. The American Economic Review 71(2), 405–409 (1981)
41. Schneier, B.: The psychology of security. Communications of the ACM 50(5), 128 (2007)
42. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., Nunge, E.: Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 88–99. ACM (2007)
43. Sherman, S.J.: On the self-erasing nature of errors of prediction. Journal of Personality and Social Psychology 39(2), 211–221 (1980)
44. Sloman, S.A.: The empirical case for two systems of reasoning. Psychological Bulletin 119(1), 3 (1996)
45. Smetters, D.K., Grinter, R.E.: Moving from the design of usable security technologies to the design of useful secure applications. In: Proceedings of the 2002 Workshop on New Security Paradigms, NSPW 2002, pp. 82–89. ACM, New York (2002)
46. Spencer, W.D., Raz, N.: Differential effects of aging on memory for content and context: A meta-analysis. Psychology and Aging 10(4), 527 (1995)
47. Tulving, E.: What is episodic memory? Current Directions in Psychological Science 2(3), 67–70 (1993)
48. Tversky, A., Kahneman, D.: Judgment under uncertainty: Heuristics and biases. Science 185(4157), 1124 (1974)
49. Wang, Y., Komanduri, S., Leon, P., Norcie, G., Acquisti, A., Cranor, L.: I regretted the minute I pressed share.: A qualitative study of regrets on Facebook. In: Symposium on Usable Privacy and Security (2011)
50. Whitten, A., Tygar, J.: Why Johnny cant encrypt: A usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, vol. 99 (1999)
51. Wild, K., Boise, L., Lundell, J., Foucek, A.: Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults. Journal of Applied Gerontology 27(2), 181–200 (2008)
52. Willis, S., Schaie, K., Martin, M.: Cognitive plasticity. Handbook of Theories of Aging, 295–322 (2009)