JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(3), 2017, 159–171
doi: 10.1093/cybsec/tyx006
Advance Access Publication Date: 28 July 2017
Research paper

Research paper

Valuing information security from a phishing attack

Kenneth D. Nguyen[1,*], Heather Rosoff[2], Richard S. John[1]

[1]Department of Psychology, University of Southern California, Los Angeles, CA, 90089, USA and [2]Sol Price School for Public Policy, University of Southern California, Los Angeles, CA, 90089, USA

*Corresponding author: University of Southern California, Los Angeles, CA, 90089, USA. Tel: 714 752 9218; Fax: (213) 821-3926; E-mail: hoangdun@usc.edu

Received 30 December 2016; revised 30 March 2017; accepted 26 May 2017

Abstract

The extent to which users take precautionary actions against cyber risks is conditional upon how they perceive the value of information security relative to other important personal goals. In most cyber security contexts, users are faced with trade-offs between information security and other important attributes that they desire to maximize. We examined this issue by eliciting the "security premiums" that users were willing to sacrifice to protect their information security in a phishing context. We also examined the effect of usage contexts on value of information security using an experimental design. Respondents from Amazon Mechanical Turk were randomized into one of three conditions in which the context of a phishing attack was varied. Respondents were asked to make trade-offs between pairs of attributes including security, cost, latency, and productivity, from which we could quantify security premiums. Results indicated that half of the respondents were willing to pay a premium between $9 and $11 per month, willing to wait between 8 and 9 additional minutes, and willing to forgo their access to 21–29 valid pieces of information, to obtain a more effective phishing filter that reduces the number of false negatives from 24 to 6 per month. Interestingly, the value of information security was sensitive to the usage context, such that social media invoked greater security premiums in terms of productivity than email and web surfing. We also found that vulnerability and perceived net benefit significantly correlated with security premiums in terms of monthly cost. These results offer valuable insights for the design of more usable information security systems.

Key words: information security; security premiums; human values; trade-off Va+luing Information Security from a Phishing Attack

Introduction

Researchers are keenly aware that humans are the weakest link in the cyber security chain [1–2]. Yet the security of any cyber infrastructure mostly depends on the participation of users to practice self-protective information security behavior [3]. Nevertheless, getting users to participate in safe online behavior is a significant challenge. Although studies have shown that internet users are very concerned about the privacy and security of their information [4–8], many users are willing to provide access to their private information in exchange for financial gain and convenience [9–10]. This suggests that even though information security is an important priority, internet users are willing to make security compromises to achieve other goals. Conversely, users are also willing to compromise other priorities, such as usability, to protect their information privacy [11]. Therefore, if the goal is to understand when and how users adopt safety measures against information security risks, those interested in promoting safe online behaviors should consider how users weigh the value of using technology to protect their information against the costs that such preventive measures impose on the achievement of other personal objectives.

Critically, the value that users ascribe to any measures designed to enhance information security, or value of information security (VIS) in general, context dependent. Research implies that various contextual factors can affect how users view the risks, costs, and benefits associated with products designed to enhance information security [12]. Following this reasoning, it is expected that users' perceptions of VIS depend on the specific usage context. For example, an employee can be cautious in making an information security-related decision while at work, yet he or she might be less concerned when making such a decision at home.

This article describes a study wherein we explore how people value their information security within a broader value system that consists of multiple conflicting personal objectives. Importantly, we use this valuation of information security as a platform to investigate how internet users perceive and value the security of their private information in different usage contexts, as well as how perception of cyber risk relates to decision making in cyber space. We examine these research questions in the context of phishing attacks. Phishing is a socially engineered crime, through which attackers aim to steal confidential information from users. Examples include bank account details, email and social network usernames, passwords, and other sensitive data [13]. The potential economic losses from phishing attacks are enormous [14], and phishing is considered one of the most common strategies used by cyber criminals to target individual users. Hence, understanding the value users place on safety measures to mitigate against phishing attacks is an important priority.

Theory and research questions

Quantifying multidimensional value of information security

Because phishing attacks can result in severe consequences, a number of approaches have been initiated to help users become more aware and better able to protect themselves from phishing attacks, and increase information security in general. Two of the most commonly used strategies include (i) providing users with information security training, and (ii) equipping users with technologies designed for information security purposes [15]. However, these approaches have not been very successful in keeping internet users from becoming victims of cyber attacks. As an example, although a number of technologies have been created to enhance information security, many internet users simply do not know how to use those tools to protect their private information online. For example, about 20% of respondents in a recent survey indicated that they did not know how to protect their information in cyber space [16]. In addition, those lacking necessary skills to implement security technology were also reluctant to pay for services that can improve security [17]. Similarly, studies have indicated that conventional security training, in which users simply receive education materials about phishing attacks, do not significantly increase safe online behaviors [18]. However, a new and more promising education intervention has been recently developed. In this approach, internet users are actually exposed to simulated phishing attacks. When they fall prey to these attacks, they receive immediate feedback that helps them recognize illegitimate online contents. Evaluation studies suggest that this type of interactive training is retained for up to 28 days [19], and reduces the risk of users becoming victims of phishing attacks [20]. Nonetheless, such interactive training can cause unexpected and undesirable consequences. For instance, users may ignore legitimate emails, mistaking them for phishing attempts [21].

The limitations of these approaches raise the question of how best to motivate users to engage in safe online behaviors. One approach is to identify and examine values that users consider important when adopting new technology for information security purposes. In psychology, "values" have been defined as a cognitive representation of needs [22]. Although individuals differ in how they rank the importance of specific values [23], it is generally agreed that psychological values are important to maintain in the long run [24]. Thus, information security products that offer substantial value to users will be adopted quickly, whereas products that offer little value to users are unlikely to ever gain acceptance [25]. For example, the effectiveness of interactive training involving pseudo phishing attacks described earlier may be enhanced by identifying the values users appreciate and incorporating these values into the training content. Specifically, because users want to access legitimate online material, the training may become more effective by focusing on teaching users to recognize safe online content from phishing attempts, as opposed to focusing solely on recognizing cues related to phishing attacks.

However, understanding user values and concerns naturally involves accounting for multiple objectives [26–27]. Such understanding becomes even more challenging in the context of objectives that are conflicting, in the sense that high performance on one means sacrificing performance on another [28]. A usable product may sacrifice some security features (and vice versa), so both designers and users may be required to make hard choices involving trade-offs among these conflicting objectives. Isomursu et al [29] described an approach to explore (conflicting) objectives that users may have when adopting a new technology. These researchers adopted Schwartz's universal model of human values to evaluate how students, parents, and teachers at a Finnish school valued different priorities related to implementation of a new school attendance control system. Employing a case study method, the authors discovered that although both children and their parents highly valued benevolence and conformity, they also had additional distinct concerns. For instance, the children considered self-direction and achievement important priorities, while their parents considered security a top priority.

While identifying and exploring objectives that people value is an important first step, it is imperative to evaluate how individuals make decisions when their objectives are conflicting with one another. The key to understanding this decision making process is to quantitatively examine how individuals prioritize their personal values. Individual users often encounter decisions that require evaluation of multiple alternatives to meet multiple conflicting objectives. For example, users may have to evaluate multiple anti-virus software options that differ in cost and effectiveness. Yet, there has been little research to quantify information security concerns in the context of other competing priorities.

The current experiment bridges this research gap by quantitatively describing how users prioritize relevant conflicting objectives. To achieve this goal—assessing user concerns about information security, we elicited users' willingness to sacrifice for a higher level of information security, given a particular set of conflicting objectives. We called this value a "security premium," to reflect the users' willingness to pay a premium in the form of sacrificing performance in exchange for improved security. Specifically, we elicited security premiums by quantifying internet users' trade-offs between information security and each of the following competing objectives: minimizing cost, minimizing latency (delay time), and maximizing productivity (false alarm rate). Certainly, each individual user will employ an idiosyncratic set of objectives and each decision problem will call on a unique set of evaluation criteria. Thus, it would be

impossible to describe an exhaustive set of objectives that addresses all of users' concerns.

Our focus in this study, therefore, is to describe how individual users value security protection within a set of conflicting and desirable objectives that are relevant, independent, and relatively complete [29]. The selection of the aforementioned objectives is motivated by the Technology Acceptance Model (TAM) [30]. For instance, the TAM "usability" factor maps to the time required for users to interact with a security tool, which is captured by the minimizing latency objective in our model. Similarly, the TAM "usefulness" factor is conceptually linked to the maximizing productivity objective in our model. The selection of the cost objective is motivated by the fact that commercial phishing filters are licensed to users for a fee. Likewise, commercial phishing filters vary in terms of missed attacks, depending on the sophistication of the detection algorithm employed, and may also allow control by the user.

We created a decision context in which users consider the purchase of a commercial phishing filter tool that guarantees a particular detection rate of phishing attacks. Phishing attacks are of concern because free online anti-phishing tools (e.g. Gmail spam filter, Firefox 2, eBay Toolbar, etc.) have been shown to vary in their effectiveness to protect users from such attacks. For instance, the best anti-phishing tools missed over 20% of phishing websites [31]. The decision context is characterized by a choice between two filters described on four attributes: *security, cost, latency, and productivity*, corresponding to four respective objectives: 'maximizing security, minimizing cost, minimizing wait time (latency), and maximizing productivity'. An indirect, sequential binary choice method is used to estimate the value of increased security protection for each user in terms of reductions in achievement on each of the other three non-security attributes. These trade-offs allow us to quantify the value of information security in multiple metrics, i.e., monetary cost, latency, and productivity. We hereafter refer to these values as 'security premiums'.

Obtaining the security premiums is important for several reasons. First, although there is no shortage of studies on information privacy and security trade-offs [32], many previous studies focus solely on the trade-off between money and security, and ignore other non-monetary concerns. Second, a decision that includes only money and security can lead to a suboptimal choice, because other objectives are not considered. Thus, our study complements prior research by examining multiple metrics designed to triangulate on each user's trade-offs for information security.

To achieve the second goal of examining how information security values and trade-offs vary across cyber contexts and individuals, we investigated whether and how the security premiums vary across multiple manipulated usage contexts and across individuals. We also explored user characteristics that may relate to information security premiums.

Value of information security varies across contexts

Kujala and Väänänen-Vainio-Mattila [12] have argued that the value of a technology does not arise from its properties, but is contingent upon the interactions of users and the product in a particular situation. This perspective suggests that the information security premiums may be contingent on usage context. Conversely, there are reasons to believe that information security premiums are generalizable across usage contexts. These two perspectives suggest two contradictory hypotheses about the effect of usage context on information security premiums. At one extreme, the 'generalized security hypothesis' suggests that security premium(s) should be generalizable. This is because the value of a security tool should be judged in terms of the costs and benefits, independent of the context in which it is used. For example, if a phishing filter successfully detects 20 phishing attempts out of 100 suspicious online contents, its 'objective' value should not be altered whether the online content domain is Facebook posts or pop-up alerts.

In contrast, the 'context-specific hypothesis' posits that security premium(s) should be sensitive to usage context. Studies have identified several important contextual factors that can modify users' security-related behaviors, such as the purpose and requirements of different tasks [33, 34], the ordering of choices [32], and user characteristics [35, 36]. Furthermore, Boiney [37] underscored the context-based usefulness of technology by suggesting that the same technology can provide different users with distinct benefits in unique settings. The usage context can make certain pieces of information more salient and prompt users to pay more attention to specific objectives and values. In the current study, the usage context can have an influence on security concerns by highlighting certain contextual characteristics. These features, in turn, can activate different user motivations, trigger unique user perceptions, and engage the user in different judgmental and behavioral strategies. For example, users may be more familiar with, and perhaps feel more competent in handling spam messages than in dealing with social media phishing attempts, since the former are more familiar while the latter are a relatively new and emerging threat. Thus, these perceptions and feelings may lead users to value information protection to a greater extent in the social media context than in the email context.

The two aforementioned hypotheses suggest two opposite predictions. The generalized security hypothesis predicts that the security premiums are invariant across usage contexts, while the context-specific hypothesis suggests otherwise. Methodologically, we explore the effect of various usage contexts by manipulating the context where a phishing attack can occur, including email, web browsing, and social media. Because there are few empirical studies relevant to this research question, we make no *a priori* hypothesis, and instead 'explore whether the value of security premiums, as found in one context, can be generalized to other contexts'.

Predictors of the security premiums

Kurt Lewin famously postulated that behavior is a function of a person and his or her environment [38]. Thus, it is expected that individual differences play an important role in shaping how users value the security of their private information 'above and beyond' the contribution of situational factors such as the effect of usage context. A factor that can account for such individual differences is perception of cyber risk. In an adversarial context such as cyber security, risk has been defined as a function of 'threat, vulnerability, and consequence' [39]. Threat refers to an adversary's intention and capability to cause loss or damage to an asset and/or population. Vulnerabilities are weaknesses in the design, implementation, or operation of a system that an adversary can exploit. Finally, consequences include short-term and long-term, as well as direct and indirect, loss or damage. Although previous studies have examined the role of cyber risk perceptions in shaping user behavior [40], little research has examined how different components of risk such as threat, vulnerability, and consequence relate to self-protective behaviors in cyber space. Therefore, another aim of this study is to explore how different components of risk, specifically perceptions of vulnerabilities and consequences, relate to information security trade-offs.

In the current research, perceived vulnerabilities refer to users' perception of the likelihood (or frequency per unit time) of personal phishing attacks over a particular time horizon. Thus, it is expected that a person who perceives a greater likelihood of becoming a target of a phishing attack is more inclined to make greater sacrifices for security than a person who perceives a smaller likelihood of being targeted.

Likewise, internet users who perceive more severe consequences of a phishing attack are expected to indicate larger security premiums compared to those who perceive less severe consequences.

It has been implicitly presumed that users make trade-off(s) for security by evaluating the benefits and costs of a security-enhancing technology. It follows that those who perceive that the cost(s) of implementing such technology is outweighed by the benefits are likely to value the technology more than those who perceive security costs outweighing benefits [26]. This expected association, if found, would highlight the psychological mechanism underlying security trade-offs: The larger the (perceived net) benefits of utilizing technology designed for information security relative to its cost, the larger the security premiums.

User self-efficacy could be another important factor predicting trade-offs for information security. Self-efficacy has been defined as the belief that one is capable of or competent in performing a behavior [40]. Thus, individuals with a high level of self-efficacy may believe that they have the requisite knowledge and skill to protect themselves from being victimized by a phishing attack, or cybercrimes in general. Users who view themselves as technologically competent may see little value in security technologies, because they know about alternative means to protect against cyber attacks, and do not see the need to use technologies designed to specifically address a particular threat. Conversely, an alternative possibility is that users with high self-efficacy also value security-enhancing technologies more because they are more aware of personal cyber risks and feel more competent to address them. Previous research seems to provide support for the former prediction. Paine [16] found that people who had some experience with information technology were not concerned about their online privacy. We explore these contrasting predictions by examining correlations among information security premiums and individual difference variables, including 'perceived vulnerability, perceived consequence, perceived net benefit, and self-efficacy'.

Method

Procedure

The experimental session began with a four-minute video of a Powerpoint presentation with audio describing the general purpose of the study and subsequent choice tasks, including a detailed explanation of the four attribute scales on which the phishing filter alternatives were defined. Each respondent was randomly assigned to one of three phishing attack contexts: (i) email, (ii) web browsing, and (iii) social media. Respondents completed trade-off assessments for all six possible attribute pairs, with up to three binary choices per assessment (18 in total). The focus of the current study is on the three trade-offs for security: (i) security versus cost, (ii) security versus latency, and (iii) security versus productivity. The experimental session ended with respondents completing several demographic questions, and various psychometric scales including perceived vulnerability, perceived consequence, perceived net benefit, and self-efficacy. The psychometric scales were adapted from a previous study [25].

The experiment was hosted on Qualtrics.com and 294 US adults (18 years and over) were recruited from Amazon Mechanical Turk (AMT). Responses from 19 respondents were discarded because these respondents failed an attention check question regarding the assessment instruction. Thus, the final sample included 275 respondents. Previous studies have shown that AMT samples are generally more representative than other convenience samples [41, 42, 43]. The sample sizes under each of the three context conditions were 95 (email), 87 (pop up), and 93 (social media). The median age was 32 years, and 46.5% of the respondents were female.

Objective operationalization

The four relevant user objectives are (i) maximizing information security, (ii) minimizing cost, (iii) minimizing latency, and (iv) maximizing productivity (work and play). The objectives were operationalized in terms of the quantifiable attributes defined in Table 1. Security is defined as the false negative (miss) rate, or the number of phishing attempts that bypass a filter and appear in the users' inbox (web browser/social media platform) per 100 emails (pop-ups/apps), averaged over a year. Cost is defined as the additional monthly cost to the user for a (email/web browsing/social media) phishing filter. Latency is operationalized as the average time it takes the phishing filter to screen an email/pop-up/app before it is allowed (or disallowed) in the user's email inbox (web browser/social media platform). Finally, productivity is defined as the false positive (alarm) rate, or the number of valid contents that are misclassified as phishing attempts and diverted from the users' inbox (web browser/social media platform) per 100 emails (pop-ups/apps), averaged over a year.

Trade-off elicitation methodology

We used a modified version of an elicitation method used by Tversky, Sattah, and Slovic [44] to compare attribute weights based on a choice versus matching task. The method used in the current experiment requires the user (participant) to choose between two phishing filter alternatives that differ on two attributes only. The first phishing filter is more attractive than the second phishing filter on the first attribute, but the second filter is more attractive on the second attribute. Users are asked to indicate which option is preferable, or they may indicate "indifference," meaning that they perceive the two alternatives as equally attractive. We use this elicitation protocol to estimate users' trade-offs for information security against each of the other three attributes, i.e., cost, latency, and productivity.

Figure 1 graphically illustrates the elicitation procedure. The trade-off between security and cost is estimated using a series of three binary-choice trials with two phishing filter options, A and B_i ($i = 1 \ldots 7$). Filter A is less effective in detecting phishing emails, but it is inexpensive. On the other hand, B_1 is more expensive but B_1 is more effective in identifying phishing emails. Users are asked to choose either A or B_1. Depending on the decision makers' choice in the first trial, the cost for B_1 is adjusted dynamically while the cost for A is fixed in the next trial; the next trial has option $B_3 > B_1$ if respondents choose B_1; conversely, $B_2 < B_1$ if A is chosen. The procedure is repeated until the respondent is indifferent between the two options, or she completes the third trial, at which point the trade-off is bounded.

The dependent variable, a security premium, is determined by taking the difference in cost between two options whenever the respondent indicates indifference. If the respondent does not select the "indifference" option in any of the three trials, the premium for security protection is bounded using an inequality determined from the three trials.[1] For instance, if a respondent selects A in the first

1 We could continue the elicitation beyond three choices, but this was deemed unnecessary as the purpose of the study was to bound the premiums. In addition, having up to three trials already allows us to specify fifteen (small) ranges of the premiums that users were willing to exchange for a higher level of information security (see the Appendix for more details).

Table 1. Summary descriptions of the three phishing attack contexts and attribute definitions

Video elements	EmailPhishing context	Social mediaPhishing context	Pop-up windowPhishing context
General introduction	Phishing is the attempt to collect internet users' confidential information such as names, addresses, social security numbers, and credit card information ***through email***. . . Phishers carefully craft ***email messages*** asking for the recipients' personal information. The ***email recipient*** is then prompted to enter . . .	Phishing is the attempt to collect internet users' confidential information such as names, addresses, social security numbers, and credit card information. ***Phishing on social networking sites is through the use of fake applications or apps***. . . Phishers carefully craft ***fake applications*** asking for the user's personal information. The ***social media user*** is then prompted to enter . . .	Phishing is the attempt to collect internet users' confidential information such as names, addresses, social security numbers, and credit card information through ***pop-up window alerts***. . . Phishers carefully craft ***pop-up window alert messages*** asking for the recipients' personal information. The ***pop-up recipient*** is then prompted to enter. . .
Decision context	Imagine you are choosing between two ***email phishing filters***. . . In particular, ***the email phishing filters*** differ across 4 features: their miss rate, false alarm rate, email latency and cost.	Imagine you are choosing between two ***social media phishing filters*** . . . In particular, ***the social media phishing filters*** differ across 4 features: their miss rate, false alarm rate, social media app latency and cost.	Imagine you are choosing between ***two pop-up alert phishing filters*** . . . In particular, ***the pop-up phishing filters*** differ across 4 features: their miss rate, false alarm rate, pop up latency and cost.
Attribute definitions	***Cost*** *refers to the monthly dollar amount you have to pay for the (social media/email/pop-up alert) phishing filter* ***Latency*** *refers to the amount of time, in minutes, it takes the phishing filter to screen a (social media app/email/pop-up alert) before determining whether it is legitimate or not. The quicker the filter screens, the sooner you have access to the (social media app/email/pop-up alert).* ***False alarm rate*** *refers to the number of legitimate a (social media app/email/pop-up alert) per 100 a (social media app/email/pop-up alert) identified as a phishing attack per year and removed from your (social media site/inbox/browser). As such, the greater the false alarm rate, the more legitimate a (social media app/email/pop-up alert) the user will NOT have access to.* ***Miss rate*** *refers to the number of phishing (social media app/email/pop-up alert) per 100 (social media apps/emails/pop-up alerts) that bypass the filter and are accessible on your (social media site/inbox/browser) per year. The more phishing a (social media apps/emails/pop-up alerts) on your (social media site/inbox/browser), the greater the chance that you will become a victim of a (social media/email/pop-up alert) phishing attack.*		

The bold and italicize texts highlight the differences between the experimental conditions..

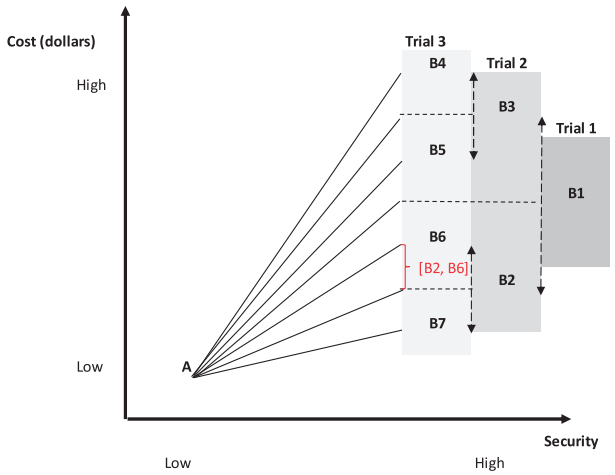

Figure 1. Graphical illustration of the trade-off method. The red texts highlight the range used in the example (see the main text for details).

trial, B_2 in the second trial, and A in the third trail, we could infer that the respondent is willing to pay between B_6 and B_2 ($B_6 < B_1$) dollars for a more effective phishing filter, i.e. the security premium in terms of dollars is in the range [B_2, B_6]. Elicitations of security premiums in terms of the other two attributes, latency and productivity, follow the same procedure. The appendix provides details on how the binary choices were constructed.

The following provides a concrete illustration of the trade-off procedure. Consider an example in which respondents are presented with two alternatives: filter A costs \$5 per month and identifies 50 out of 100 phishing emails, labeled A (\$5, 0.5), while filter B costs \$10 per month and identifies 90 out of 100 phishing emails, labeled B (\$10, 0.9). If a respondent prefers A (\$5, 0.5) over B (\$10, 0.9), then the implication is that she does not consider it worthwhile to pay an additional \$5 to reduce the number of phishing emails by 40%. The choice is then repeated, but the cost of option B is reduced to \$8 to make option B more attractive, B (\$8, 0.9) If the respondent persists in choosing option A (to save money), the cost of option B is further reduced to \$6, B (\$6, 0.5). If the respondent is indifferent, then it is inferred that she is willing to pay no more than an additional \$1 (\$6–\$5) to reduce the number of phishing emails by 40%, i.e. the security premium in terms of money is bounded between \$0 and \$1.

The context-independent versus context-specific hypotheses is tested by manipulating the phishing context. As specified, the manipulation was operationalized by varying the phishing context (email, web browsing, social media). Specifically, phishing attacks can occur when users follow the instruction in a phishing email,

Table 2. Summary of measures of security premiums and individual user characteristics

Measures	Descriptions	Characteristics
Security premiums	• The additional cost in dollars that users are willing to pay for a more effective phishing filter • The additional wait time in minutes that users are willing to tolerate for a more effective phishing filter • The additional loss of access to valid emails/apps/pop-up alerts that users are willing to sacrifice for a more effective phishing filter	Dependent (ordinal) variables with fifteen categories
Perceived consequence	Three items 5-point scale where 1 means "Not at all harmful" and 5 means "Severely harmful" • Having my confidential information accessed by someone without my consent or knowledge is: • Having someone successfully attack and damage my system is: • In terms of information security violations, attacks on my information systems and equipment are:	Independent variable Cronbach's alpha = 0.85 (Item scores were averaged)
Perceived vulnerability	Three items 5-point scale where 1 means "Not at all likely" and 5 means "Extremely likely" • I believe that trying to protect my confidential information will reduce illegal access to it. • The likelihood of someone damaging my system is: • The likelihood of an information security violation occurring to me is:	Independent variable Cronbach's alpha = 0.88 (Item scores were averaged)
Self-efficacy	Three items 7-point Likert-type scale where 1 means "Strongly Disagree" and 5 means "Strongly Agree" • I have the necessary skills to protect myself from information security violations: • I have the skills to implement the available preventative measures to stop people from getting my confidential information: • I have the skills to implement the available preventative measures to stop people from damaging my system:	Independent variable Cronbach's alpha = 0.77 (Item scores were averaged)
Perceived net benefit	Three items with 3-point scale where 1 means (cost to security protection) "Exceeds Benefits" and 3 means "Is Outweighed by Benefits" • The inconvenience to implement recommended security measures: • The cost to implement recommended security measures: • The impact to my work from recommended security measures:	Independent variable Cronbach's alpha = 0.82 (item scores were averaged)

which looks and feels as if it were from a valid entity, resulting in submission of sensitive personal information. Phishing attacks through web browsing are another common context. Attackers carefully craft pop-up window with alert messages asking the recipient to enter sensitive information into a website, from which the attacker collects the data. A third context, social media phishing attacks, has become common recently, in particular through the use of fake applications and feeds on social media sites. Attackers carefully craft fake applications or feeds asking users to "like" or asking users to click on a malicious link. Social media users are then prompted to enter their sensitive information into a website, from which the attacker obtains the data.

In this experiment, each respondent was presented with one of the phishing attack contexts in the introductory video. The presentation and audio description included four elements: (i) a general definition of a phishing attack, (ii) a description of the phishing attack context, (iii) a description of the sequential binary choice task, and (iv) definitions of the four attributes representing alternative phishing mitigation alternatives. Respondents received a unique version of the introductory video presentation, corresponding to the context condition to which they were randomly assigned. The three video presentations differed with respect to the language and graphical images used to describe the phishing attack context. For instance, respondents under the email phishing condition were told that they would be asked to select between 'email phishing' filters while respondents under the social media condition were told to select between 'social media phishing filters'. The visual images in the three videos are identical except for some modifications to fit each specific context (e.g. replacing an image of an email inbox with a particular social media app). All video presentations were audio-recorded by the same male research assistant, and were nearly identical in length: (3 minutes, 54 seconds). Table 1 provides an overall summary describing task instructions, manipulated cyber contexts, and value-relevant attributes.

Measures

Table 2 is a summary of the response variables and how they are measured in the current study. The key dependent variables are the security premiums, derived from the three security trade-off elicitations. Other variables consist of several psychometric scales that measure users' perceptions of the vulnerability and consequence of cyber threats, users' perceived net benefit, self-efficacy, and demographic information. User participants selected a response to each item contained in the rating scales (see Table 2). The measure of Perceived Vulnerability assesses users' belief in becoming a victim of a cyber-hack. The measure of Perceived Consequences assesses the degree of harm that users feel when targeted for a cyber-attack. The

Table 3. Medians and interquartile ranges for three security premiums by attack context

	Social media			Pop-up			Email		
	25th	50th	75th	25th	50th	75th	25th	50th	75th
Cost (dollars)	6	11	17	6	9	16	6	9	16
Latency (minutes)	5	9	16	3	7	13	3	9	16
False Alarm rate (the number of inaccessible app/pop up/email)	24	29	39	12	24	37	9	21	36

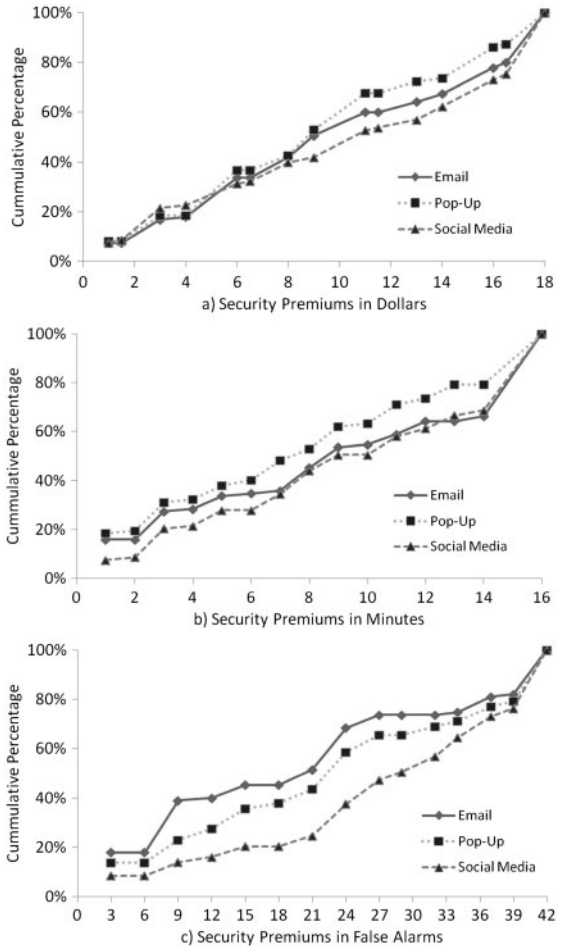

Figure 2. Cumulative distributions of the security premiums for a more effective phishing filter with a lower miss rate. The horizontal axes represent the amount of monthly payment (dollars) in Figure 2(a), the number of minutes it takes a phishing filter to screen an online email/pop-up/app in Figure 2(b), and the number of legit emails/popups/ apps misclassified out of 100 contents in Figure 2(c). The "more effective phishing filter" is defined as the reduction of the number of phishing emails/pop-ups/apps by 18 out of 100 online contents in a given year. The 50% reference horizontal lines are shown.

measure of Self-Efficacy assesses users' belief in their competency related to information security. Finally, we asked users to report perceived relative benefit(s) of implementing a self-protective security measure versus perceived cost in the measure of Perceived Net Benefit.

Results

The three security premiums were analyzed as an ordinal response variable, since the sequential binary choice method bounds the premiums into non-overlapping intervals. In particular, the three security premiums were ranked between 1 and 15 in which 1 means "the smallest premium possible" and 15 means the "largest premium possible" (for security). Hence, we applied non-parametric methods to compare contexts, and used correlations to explore individual differences in security premiums. Before comparing the effect of different usage contexts, we describe the security premium distributions.

Security premiums

In this analysis, we describe each of the three security premiums in terms of median and inter-quartile range for each of the three experimental conditions (phishing attack contexts). A more in-depth analysis of the experimental effect follows. Table 3 displays the medians and inter-quartile ranges of the three security premiums for each of the three usage context conditions. Results indicate that 50% of the respondents were willing to pay a premium between $9 and $11 per month, depending on the experimental condition, for a more effective phishing filter that reduces the number of phishing emails (pop-up alerts/apps) from 24 to 6 (per 100 emails/pop-up alerts/apps). We simply refer to the filter that reduces the number of phishing emails/pop-up alerts/apps from 24 to 6 as the 'more effective filter' hereafter. Half of the respondents reported that they chose the more effective filter despite having to wait between 7 and 9 minutes longer for the more effective filter to scan incoming emails (pop-up alerts/apps). Similarly, half of the sample was willing to forgo access to 21–29 valid emails (pop-up alerts/apps) per 100 in order to utilize the more effective filter. Clearly, median security premiums suggest that respondents reported willingness to incur non-trivial sacrifices to mitigate the risk of phishing attacks.

As suggested by the inter-quartile ranges reported, we found substantial individual differences in security premiums among respondents. The cumulative plots of the three security trade-off assessments are displayed in Fig. 2 unambiguously demonstrate striking individual differences in the elicited security premiums. The horizontal axes in all three plots correspond to three security premiums for a more effective filter (lower miss rate), and the vertical axes are the cumulative percentages—the sum of all percentage values up to each category. Each curve corresponds to different context condition. Each point on a curve reflects the proportion of respondents who were willing to pay a monthly amount of money less than or equal to X, are willing to wait an additional number of minutes for filtering less than or equal to Y, and are willing to sacrifice a specific number of valid emails less than or equal to Z, for the more effective filter. The percentage value on the vertical axis that corresponds to a particular premium on the horizontal axis represents the proportion of users who are willing to pay no more than the corresponding premium for a more effective filter. Equivalently, the proportion of respondents who were willing to pay *more* than that premium equals one minus the percentage value of that premium level.

The left-most security premium category (=1) represents the proportion of respondents who show 'little (or no) interest' in purchasing the more effective filter. In Figure 2(a), across the three

Table 4. Spearman rank order correlations among the three security premiums and the four individual user characteristics

	Cost premium	Time premium	False alarm premium	Perceived consequence	Perceived vulnerability	Efficacy
Cost premium						
Time premium	0.41*					
False alarm premium	0.22*	0.25*				
Perceived consequence	0.07	0.05	–0.03			
Perceived vulnerability	0.13*	0.05	0.06	0.27*		
Self-efficacy	0.01	–0.1	0.01	0.09	–0.23*	
Perceived net benefit	0.23*	0.14*	0.09	0.15*	0.15*	0.05

*Notes: $P < 0.0.5$; N = 275, including users from all three phishing attack context conditions.

experimental groups, on average, about 7.7% of the respondents in the study were not willing to pay an additional dollar per month to have the more effective filter. In Figure 2(b), about 13.9% of the respondents revealed their unwillingness to purchase the more effective filter if the additional filtering time required was greater than or equal to one minute per screening. Similarly, in Figure 2(c), about 13.4% of the respondents, across all three experimental groups, indicated that the value of the more effective filter was worth less than the loss of access to three or fewer valid emails/alerts/apps per 100.

On the other hand, the right-most security premium category (=15) represents the proportion of respondents who were willing to make 'any' sacrifice for protection from phishing attacks. These respondents perceived the value of security protection as "sacred," and were unwilling to compromise or trade-off such security. In Figure 2(a), across the three experimental groups, on average, about 19.1% of the respondents in the study were willing to pay an additional $18 or more per month for the more effective filter, and in Figure 2(b), on average, about 26.8% of the respondents were willing to sacrifice more than 16 minutes per screening for the more effective filter. In Figure 2(c), about 20.8% of the respondents were willing to give up access to more than 39 valid email contents (alerts/apps) per 100 to have the more effective filter.

These results demonstrate clear individual differences in users' concerns about information security. Specifically, whereas some respondents reported willingness to make very large sacrifices for greater security from phishing attacks, others were willing to make little or no sacrifice for security. For instance, 19.1% of the respondents were willing to pay more than $18 per month to eliminate 18 phishing emails, apps, or pop-ups per 100, whereas 7.7% of the respondents were not willing to pay a $1 to reduce the same number of phishing contents.

The effect of context on security premiums

The cumulative plots in Figure 2 also represent graphically the influence of attack context on security premiums. Indeed, the three curves, representing the three context conditions, do not completely overlap. Particularly, 'the lower right curve stochastically dominates the other two upper left curves'. This result indicates that for any level of sacrifice, a greater percentage of respondents in the social media context group were willing to make that level of sacrifice for information security compared to respondents in the email and web pop-up context groups. Indeed, K-independent sample Kruskal–Wallis (KW) tests detected significant differences across the three context conditions in the security premiums measured in terms of productivity (false alarms rate), KW (2) = 13.88, $p < 0.01$. KW tests also indicated that the differences across the three context conditions for security premiums measured in terms of screening latency and in terms of monthly cost were not different from each other, $p = 0.32$ and $p = 0.09$, respectively.

We explored specific differences in the trade-off patterns among context conditions. using follow-up Mann–Whitney–Wilcoxon (MWW) tests (analogous to conducting post hoc tests after an omnibus ANOVA). In the trade-off between security (false negatives per 100) and productivity (false positives per 100), we found greater security premiums in the social media group compared to the email group, $W = 5766$, $p < 0.001$, and the pop-up alert group, $W = 4829$, $p = 0.02$. However, the security premium distributions were not significantly different between the email and web browsing groups.

Relationships among security premiums and individual user characteristics

Table 4 presents correlations among the three security premiums and four individual user characteristics. The three pairs of security premiums were all significantly positively correlated. Users who were willing to sacrifice more on one attribute for security were also willing to sacrifice more on other attributes. In addition, four of the six pairs of individual user variables were also significantly correlated. Interestingly, users reporting greater cyber related self-efficacy also indicated lower levels of perceived vulnerability. Noticeably, only perceived vulnerability and perceived net benefit were significantly positively correlated with the cost premium, e.g. users with a higher perception of vulnerability or net benefit for adopting cyber security measures indicated a willingness to pay a greater additional monthly fee for a phishing filter with substantially reduced false negatives.

Discussion

We explored internet users' willingness to sacrifice monetary cost, loss in productivity (missed messages), and message delay to enhance security from phishing attacks. Furthermore, we investigated the extent to which trade-offs involving enhanced security relate to individual user characteristics and application context. Results indicate that some users are willing to make non-trivial sacrifices to mitigate their risk of being the target of a phishing attack. This result is generally consistent with those from previous studies demonstrating that some respondents were willing to pay money to protect their online information [25, 45]. However, the large premiums (see Table 3) that some users were willing to pay for an improvement on security are rather surprising. One interpretation is that security is a "protected" or sacred value for some users, who reject the fundamental premise of a trade-off. Quite possibly these users would reject all of the hypothetical forced choice options in an actual decision context, and search for a new alternative.

Table 5. Classification of respondents in current study and previous studies using Westin's Trichotomy

Studies*	Fundamentalists (%)	Pragmatists (%)	Unconcerned (%)
Murk	49	40	10
GCS1	38	57	6
GCS2	37	58	5
Harris-Westin	26	64	10
Harris-Westin	34	58	8
Prior Range	26–49	40–64	5–10
Current Study			
Money	19.1	73.2	**7.7**
Productivity	20.8	65.8	13.4
Latency	**26.8**	**59.3**	13.9

*Adopted from Woodruff et al, [48]; bolded values fall within prior ranges

Although there are limited real-world data that allows a triangulation of these results, there is available information that provides indirect support for the results. For example, the fact that Silent Circle, the company that developed the self-proclaimed most secured smartphone, charges its Black Phone customers a monthly subscription fee of 9.95 US dollars for its encryption service[2] lends some credibility to the empirical finding that users' median security premium in terms of monthly cost is between $8 and $9. Granted, encryption services and phishing filters enhance security in quite different ways, their similarity in willingness to pay does lend credibility to our assessed cost premiums. It is important to keep in mind that the assessed security premiums are analyzed in terms of relative magnitude, and accurate estimates of absolute magnitudes are not critical to test the research hypotheses. That is, estimation of only the relative magnitudes of security premiums, both in different attack contexts and across users with different beliefs, is required to address the research questions posed. Thus, while users may not be willing to make such large sacrifices for an enhanced phishing filter, the large elicited premiums reveal the relatively great concern about information security in general, and phishing attacks in particular. Additional analyses (beyond the elicited premium) further strengthen the external validity of the findings. For example, we found that users' perceived net benefits significantly correlated with the security premium in terms of monthly cost. Respondents who perceive the benefits of using an additional level of security protection outweighing the aggregate costs were also willing to pay a higher monthly fee for a more effective phishing filter.

Our findings also reveal different clusters of individuals with distinct levels of security concerns. Using Westin's privacy segmentation [46] as an analogy, we classified our respondents into one of three groups: those who were willing to make extremely large sacrifices for enhanced security—the security premium corresponding to the maximum range—were categorized as 'security fundamentalists'. These fundamentalists view information privacy as a 'protected value' [47]. Those who were willing to make minimum sacrifices for security—the security premium corresponding to the minimum range—were considered 'security marginals', and the remaining respondents whose security premiums were in between the maximum and minimum ranges, were classified as 'security pragmatics'. In Table 5, we compare our results with findings from previous research [48]. It is noteworthy that our results are relatively consistent with previous estimates. For example, the proportion of security marginals, when the trade-off is quantified in terms of monetary value, was about 7.7% (averaging values from three experimental contexts), which falls within the range 5–10% reported in previous research. It is also important to discover that the proportions of different security groups vary as a function of 'the premium type', suggesting that users' concern about security may depend on exactly what they are required to sacrifice in order to enhance security.

Another noteworthy finding is the correlations among the premiums. These significant positive correlations are relatively small, but suggest that users who are willing to incur greater monetary cost are also willing to sacrifice productivity (missed messages) and willing to incur longer delays in receiving messages in order to enhance protection from phishing attacks. This finding has a direct implication for both future research and policy making such that (i) additional efforts should be devoted to identifying individual characteristics of different segments of users and their security concerns, and (ii) customized security policies and procedures may be needed to adapt to the needs of different segments of users.

The value of the present research lies not only in the quantification of security premiums using an indirect, binary choice methodology, but also on the important finding that the value of information security varies as a function of different usage contexts. The generalized and context-specific security hypotheses postulate different predictions about the generalizability of the value of security protection. We found that our respondents placed a higher value on social media phishing filters than on email or browser pop-up phishing filters. However, the results do not completely provide support for the context-specific hypotheses. We found this pattern only when the value of security was evaluated against a loss in productivity, operationalized as miss-identified valid emails, apps, or browser pop-up windows. These mixed results call for greater caution in generalizing the value of information security across contexts. Moreover, these findings seem to suggest a potentially interesting interaction between the attack context and the attribute (monetary cost, time delay, and false alarm rate) used to quantify the security premium. Certainly, this should be the subject of future research.

Another particularly interesting finding is that both perceived vulnerability and perceived net benefit significantly correlate with willingness to pay for an enhanced phishing filter. Ng and colleagues [49] applied the Health Belief Model to explain self-protective behaviors in the context of information systems, and found that perceived consequence, perceived vulnerability, and self-efficacy significantly predicted a measure of safe online behavior. While we found the effect of perceived vulnerability, we did not find the effects of perceived consequence and self-efficacy. This suggests that further research is needed to establish the theoretical links in the Health Belief Model when it is applied in cyber behavioral research.

The current research suggests several implications for developing policies for information privacy and security. The current study presents a method for users to evaluate alternative information security products or services with multiple and conflicting objectives. Indeed, this aspect of decision making, evaluating multiple alternatives with multiple objectives, is addressed within the framework of Multi-Attribute Utility Theory [27]. Users may develop their own evaluation model including their own idiosyncratic set of objectives, and apply this model as a tool for evaluating available alternatives. Likewise, at an organizational level, Multi-Attribute Utility Theory

2 https://www.silentcircle.com/products-and-solutions/software/

can be used to evaluate different policy initiatives related to information security infrastructure. In particular, because organizations often serve multiple stakeholders, it is important to take into account diversity in stakeholder trade-offs. For example, designing a usable, efficient, productive, and secured information system requires inputs from managers, engineers, and users. Undoubtedly, each of these stakeholders has different priorities, and many of these priorities are very likely to be in conflict. The trade-off methodology enables each of the stakeholders to first understand *the objectives* relevant and important to other stakeholders, and second to quantify the extent to which they are willing to compromise these priorities for greater information security. This process is likely to facilitate communication among stakeholders, and encourage a focus on shared values, which in turn can lead to a better decision-making process and better technology design.

User behaviors are the critical component of any effective information security system. Our research examines how users evaluate their information protection in the context of unavoidable trade-offs related to information security. Further research on this topic will undoubtedly improve our insight into the critical importance of user values related to information privacy and security.

Acknowledgement

This research was supported by the United States US Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001 and the National Science Foundation under award number 1314644. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States US Department of Homeland Security, the University of Southern California, NSF or CREATE.

Appendix

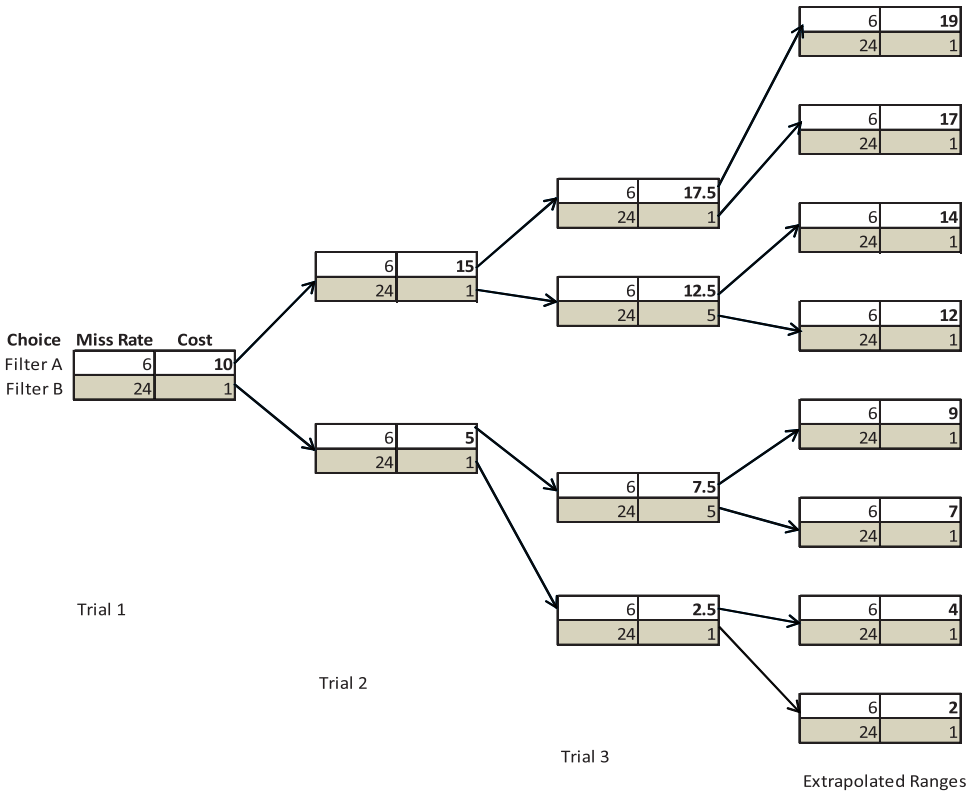

Figure A1. Assessment tree summarizes the iterative procedure used to elicit the trade-off between security (miss rate) versus cost (money). Arrows indicates the next possible pairs of choices after the previous choice. Numbers in cells indicate units of the attributes. Bolded numbers are values that were varied to make new pairs of choices. "Extrapolated Ranges" were created to bound the trade-off values for respondents who did not indicate any "indifference" in the previous three trials.

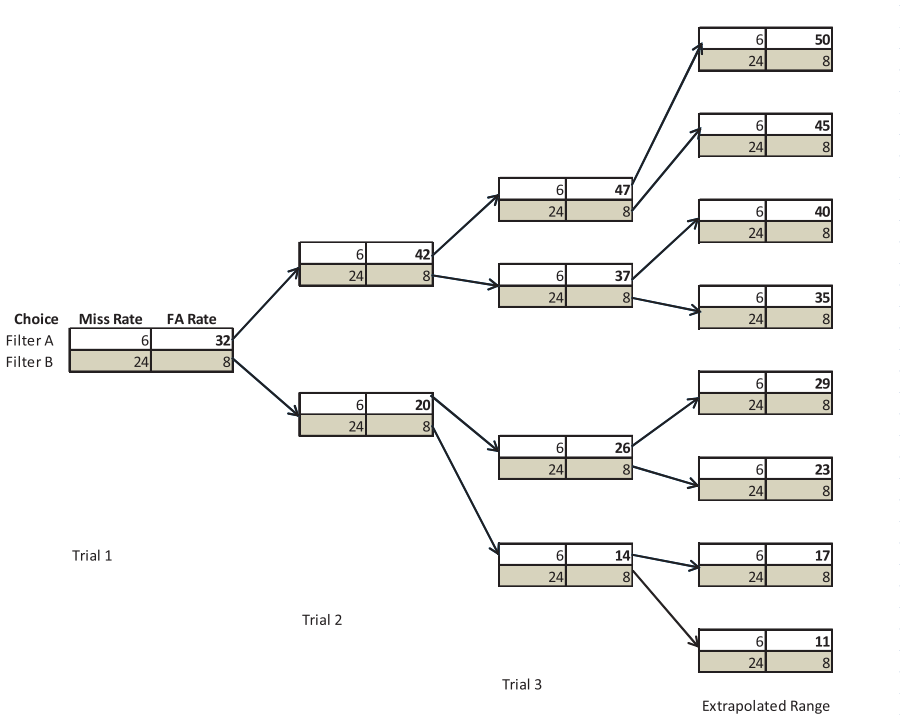

Figure A2. Assessment tree summarizes the iterative procedure used to elicit the trade-off between security (miss rate) versus productivity (false alarm rate (FA rate)). Arrows indicates the next possible pairs of choices after the previous choice. Numbers in cells indicate units of the attributes. Bolded numbers are values that were varied to make new pairs of choices. "Extrapolated Ranges" were created to bound the trade-off values for respondents who did not indicate any "indifference" in the previous three trials.

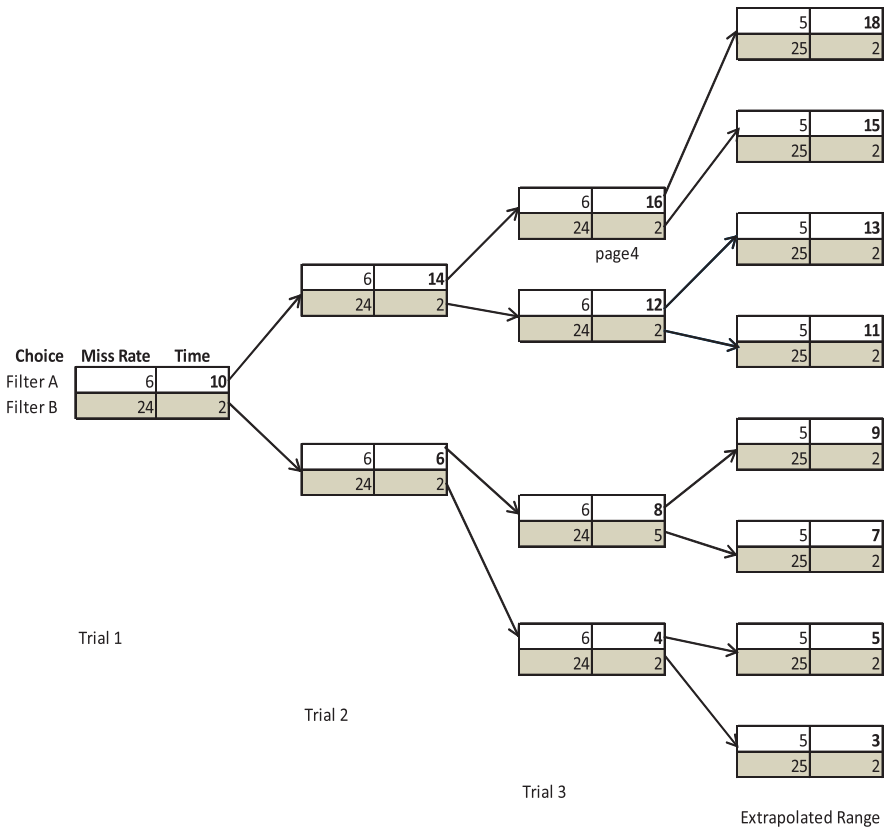

Figure A3. Assessment tree summarizes the iterative procedure used to elicit the trade-off between security (miss rate) versus latency (time). Arrows indicates the next possible pairs of choices after the previous choice. Numbers in cells indicate units of the attributes. Bolded numbers are values that were varied to make new pairs of choices. "Extrapolated Ranges" were created to bound the trade-off values for respondents who did not indicate any "indifference" in the previous three trials

Table A1. Medians and interquartile ranges for three non-security trade-offs

	IQR		
Attribute pairs	25th	50th	75th
Willingness to pay (US $ monthly) to reduce 18 false alarms per 100 messages	14	9	4
Willingness to wait (minutes) to reduce 18 false alarms per 100 messages	14	8	3
Willingness to pay (US $ monthly) to reduce 8 minutes of wait time	15.25	10.25	5.25

Note: $N = 275$, including users from all three phishing attack context conditions.

References

1. Arce I. The weakest link revisited [information. *Security]. IEEE Secur Priv* 2003;**1**:72–76.
2. Sasse MA, Brostoff S, Weirich D. Transforming the 'Weakest link' — a Human/Computer interaction approach to usable and effective security. *BT Technol J* 2001;**19**:122–31.
3. Furnell SM, Jusoh A, Katsabas D. The challenges of understanding and using security: A survey of end-users. *Computers & Security* 2006;**25**:27–35.
4. Papoutsi C, Reed E, Marston C, Lewis R, Majeed A, Bel D. Patient and public views about the security and privacy of electronic health records (EHRs) in the UK: Results from a mixed methods study. *BMC Med Inform Decis Mak* 2015;**15**:86.
5. Gandy OH. Public opinion surveys and the formation of privacy policy. *Journal of Social Issues* 2003;**59**:283–99.
6. Gross R, Acquisti A. Information revelation and privacy in online social networks. In: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 71–80. ACM. 2005.
7. TrustArc. 2016. 2016 TRUSTe/NCSA consumer privacy Infographic – GB Edition. https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-gb/ (June 2017, date last accessed).
8. Public perceptions of privacy and security in the post-Snowden era. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (June 2017, date last accessed).
9. Everybody talks about online privacy, but few do anything about it [editorial]. *New York* Times (2002).
10. Glassman M, Vandenwauver M, Tam L. The psychology of password management: A tradeoff between security and convenience. *BT Technol J* 2010;**29**:233–44.
11. Nguyen DK, Rosoff H, John SR. The effects of attacker identity and individual user characteristics on the value of information privacy. *Comput Human Behav* 2010;**55**:372.
12. Kujala S, Väänänen-Vainio-Mattila K. Value of Information systems and products: understanding the users' perspective and values. *J Info Tech Theory Appl* 2009;**9**:23–39.
13. Arachchilage NAG, Love S. A game design framework for avoiding phishing attacks. *Comput Human Behav* 2013;**29**:706–714.
14. Moore T, Clayton R, Anderson R. The economics of online crime. *J Econ Perspect* 2009;**23**:3–20.
15. Lwin M, Wirtz J, Williams JD. Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *J Acad Market Sci* 2007;**35**:572–85.
16. Paine C, Reips U, Stieger S, *et al*. Internet users' perceptions of 'privacy concerns' and 'privacy actions. *Int J Hum-Comput St* 2007;**65**:526–536.
17. Acquisti A, Grossklags J. Privacy and rationality in individual decision making. *IEEE Security and Privacy* 2005;**3**:26–33.
18. Kumaraguru P, Rhee L, Acquisti A, *et al*. Protecting people from phishing: The design and evaluation of an embedded training email system. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 905–914. ACM. 2007.
19. Kumaraguru P, Rhee L, Acquisti A. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In: *Proceedings of Symposium on Usable Security and Privacy.* Article 3. ACM. 2009.
20. Sheng S, Holbrook M, Kumaraguru P, *et al*. Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 373–382. ACM. 2010.
21. Schwartz SH, Bilsky W. Toward a psychological structure of human values. *J Pers Soc Psychol* 1987;**53**:550–62.
22. Verplanken B, Holland RW. Motivated decision making: effects of activation and self-centrality of values on choices and behavior. *J Pers Soc Psychol* 2002;**82**:434–47.
23. Isomursu M, Isomursu P, Ervasti M, *et al*. Understanding human values in adopting new technology—A case study and methodological discussion. *Int J Hum-Comput St* 2011;**69**:183–200.
24. Jurison J. Perceived value and technology adoption across four end user groups. *J. Org. & End User Comp* 2000;**12**:21–28.
25. Tsai J, Egelman S, Cranor L, *et al*. The effect of online privacy information on purchasing behavior: an experimental study. *Inform Syst Res* 2011;**22**:254–68.
26. Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput Human Behav* 2008;**24**:2799–816.
27. Keeney RL, Raiffa H. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. New York: Wiley, 1976.
28. Keeney RL. The value of internet commerce to the customer. *Manag. Sci* 1999;**45**:533–42.
29. EisenfüHr F, Weber M, Langer T. *Rational Decision Making*. Berlin: Springer, 2010.
30. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Manag Inf Syst Q* 1989;**13**:319–40.
31. Zhang Y, Egelman S, Cranor L, *et al*. Phinding phish: Evaluating anti-phishing tools. In: *Proceedings of the Network and Distributed System Security Symposium* 2007.
32. Acquisti A, John LK, Loewenstein G. What is privacy worth? *J Legal Stud* 2013;**42**:249–74.
33. van der Heijden H. User acceptance of hedonic information systems. *Manag Inf Syst Q* 2004;**28**:695–704.
34. Fang X, Chan S, Brzezinski J, *et al*. Moderating effects of task type on wireless technology acceptance. *J Manage Inform Syst* 2005;**22**:123–57.
35. Jang C. Measuring Electronic Government Procurement Success and Testing for the Moderating Effect of Computer Self-efficacy. *International Journal of Digital Content Technology and Its Applications* 2010;**4**:224–32.
36. Lee Y, Kwon O. Intimacy, familiarity and continuance intention: An extended expectation–confirmation model in Web based services. *Electronic Commerce Research and Application* 2011;**10**:342–35.
37. Boiney LG. Reaping the benefits of information technology in organizations: A framework guiding appropriation of group support systems. *The J of Appl Behavioral Science* 1998;**34**:327–46.
38. Sansone C, Morf CC, Panter AT. *The Sage Handbook of Methods in Social Psychology*. Thousand Oaks, CA: Sage Publications, 2004.
39. Cox T. Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. *Risk Anal* 2008;**28**:1749.

40. Grothmann T, Reusswig F. People at risk of flooding: Why some residents take precautionary action while others do not. *Nat Hazards* 2006;**38**:101–20.
41. Karen G, Rimer B, Viswanath K. *Health Behavior and Health Education: Theory, Research, and Practice*. San Francisco, CA: Jossey-Bass, 2008.
41. Buhrmester M, Kwang T, Gosling SD. Amazon's mechanical turk: A new source of inexpensive, yet high-quality, data? *Perspect Psychol Sci* 2011;**6**:3–5.
42. Mason W, Suri S. Conducting behavioral research on Amazon's mechanical turk. *Behav Res Methods* 2012;**44**:1–23.
43. Ipeirotis PG, Paolacci G, Chandler J. Running experiments on amazon mechanical turk. *Judgm Decis Mak* 2010;**5**:411–19.
44. Tversky A, Sattah S, Slovic P. Contingent weighing in judgment and choice. *Psychol Rev* 1988;**95**:371–84.
45. Hann I, Hui K, Lee ST, *et al*. Overcoming online information privacy concerns: An information-processing theory approach. *J Manage Inform Syst* 2007;**24**:13–42.
46. Privacy Indexes: A Survey of Westin's Studies. http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf (June 2017, date last accessed).
47. Baron J, Spranca M. Protected values. *Organ Behav Hum Dec* 1997;**70**:1–16.
48. Woodruff A, Pihur V, Consolvo S, *et al*. Would a privacy fundamentalist sell their DNA for $1000…If nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In: *Proceedings of Symposium on Usable Security and Privacy*, pp. 1–18. USENIX. 2014.
49. Ng B, Kankanhalli A, Xu Y.Studying users' computer security behavior: A health belief perspective. *Decis Support Syst* 2009;**46**:815–25.