Computers in Human Behavior 48 (2015) 199–207

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Online safety begins with you and me: Convincing Internet users to protect themselves

Ruth Shillair [a,*], Shelia R. Cotten [a], Hsin-Yi Sandy Tsai [a], Saleem Alhabash [a,b], Robert LaRose [a], Nora J. Rifon [b]

[a] Department of Media and Information, Michigan State University, 404 Wilson Road, East Lansing, MI 48824-1212, USA
[b] Department of Advertising + Public Relations, Michigan State University, 404 Wilson Road, East Lansing, MI 48824-1212, USA

ARTICLE INFO

Article history:
Available online 16 February 2015

Keywords:
Online safety
Personal responsibility
Self-efficacy
Protection motivation theory
Social cognitive theory

ABSTRACT

Serious and pervasive threats confront all Internet users. Despite frequent reports of losses due to computer security breaches, many individuals still do not follow basic safety precautions. Understanding the mental processes that motivate users to follow safe practices is key to strengthening this weak link in the security chain. Using protection motivation theory (PMT), a model within the class of social cognitive theories (SCT), we develop and assess the value of interventions strategies to enhance safe online behaviors. Furthermore, we integrate the concept of personal responsibility within the PMT approach to better understand what motivates safe, online behaviors. The online safety interventions were tested using a 2 (intervention strategy: manipulated) × 2 (personal responsibility: manipulated) × 2 (knowledge: measured and blocked), between subjects with random assignment to experimental conditions and online safety behavior intentions as the targeted outcome. Based on SCT principles of behavior change, two intervention strategies were developed, one that semantically explained behaviors, and one that offered the user an enactive mastery exercise. The sample was cross-sectional and representative of Internet users. Results showed a significant three-way interaction effect among personal responsibility, the intervention strategy and prior knowledge. Enhancing a user's sense of personal responsibility appears to be a necessary precursor to effective online safety interventions, but not necessarily sufficient; the intervention strategy should match the knowledge level of the user to enhance online safety behaviors. Potential strategies for designing effective online safety messages are discussed.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction: The online safety problem

Access to the Internet for both business and pleasure has become a fundamental element of economic growth and opportunity (Prieger, 2013). People from all backgrounds and ages use the web for everything from social and entertainment activities to work and financial transaction. However, along with these conveniences, computer and Internet use is consistently coupled with many dangers. The very devices that are easily used for everything from entertainment to work can also become an open door for unscrupulous forces to steal information and/or seize control of machines for nefarious purposes. This is a multi-faceted problem of concern to numerous technical, governmental, and legal experts. However, the key factor in online security or cyber-security is the individual user (Anderson & Agarwal, 2010; Davinson & Sillence, 2010; Workman, Bommer, & Straub, 2008).

Despite years of warnings about the dangers of online threats, a surprising number of individuals still do not follow online safety standards. User susceptibility to spam, spyware, computer viruses, fraudulent email (or phishing), and malware still remain at the top of the list for online security issues (Franke & Brynielsson, 2014; LaRose & Rifon, 2007; Siponen & Vance, 2010). Despite security concerns, many Internet users still endanger themselves by opening unexpected email attachments, downloading malware, using weak or compromised passwords, clicking inside pop-ups, clicking on links in emails, or failing to read the "fine print" before downloading files and registering at a website (LaRose & Rifon, 2007). The amount of personal information users post online also makes it easy for predators to take advantage of readily available information. For example, a recent Pew Internet and American Life Project survey found that nearly two-thirds of Internet users post photos of themselves publicly online, along with their year of birth (50%), email address (46%), employer (44%), things they've written using their real names

* Corresponding author at: 404 Wilson Road, Room 409, Communication Arts & Sciences, Michigan State University, East Lansing, MI 48824, USA.
E-mail address: Shillai7@msu.edu (R. Shillair).

http://dx.doi.org/10.1016/j.chb.2015.01.046
0747-5632/© 2015 Elsevier Ltd. All rights reserved.

(38%), and their home addresses (30%; Rainie, Kiesler, Kang, & Madden, 2013). These activities not only open users up to victimization, but also often endanger wider networks (Holtfreter, Reisig, & Pratt, 2008; Jang-Jaccard & Nepal, 2014). The excessive sharing of information and performance of risky behaviors, along with a lack of deep understanding and little effort to protect one's self online combine to make individuals targets for cybercrime and weak points for cyber security (LaRose & Rifon, 2007). These combined factors have caused Internet safety education to be an issue of national policy concern (SAFER NET, 2006).

Whether they realize it or not, each Internet user plays a role in maintaining the integrity of the overall network. Individuals compromise overall security by allowing, even inadvertently, criminal forces to access their accounts or their machines. Spear phishing is often used to get employees' passwords and access accounts to steal funds (Dhamija, Tygar, & Hearst, 2006). Malware is surreptitiously installed on the computers of users who do not perceive the high risk of downloading files or programs without scanning (Workman et al., 2008). Individuals whose computers seem to be working only a little slower than usual do not realize that these devices may have become botnets that can be used by outside forces (Leder, Werner, and Martini, 2008).

Policy makers find it problematic to find ways to communicate the seriousness of threats and what precautions should be followed. One of the barriers to protecting one's self in the online realm is the complexity of protective behaviors and practices. The number of individuals who express lack of confidence in protecting themselves online is nearly fourfold the number of those who are confident they could keep their computer safe from online threats (LaRose & Rifon, 2007). Complicating matters is conflicting advice provided by various authoritative sources (Hoban, Rader, Wash, & Vaniea, 2014). Furthermore, LaRose and Rifon (2007) found that many Internet users do not regard online safety as their responsibility or else perceive themselves to be incapable of protecting it. Even among those who take some personal responsibility for online safety, they equally place responsibility on Internet provides, industry stakeholders, software companies, the government, and experts (LaRose & Rifon, 2007). Thus, it appears that to make the Internet a safer space, users require training to enhance their knowledge and self-confidence, but perhaps also need to accept personal responsibility for protecting themselves and others in order to be motivated to expend the effort necessary for enacting online safety behaviors.

This study examines the interplay among user knowledge, personal responsibility, and training techniques for the encouragement of online safety behaviors. Extending the social-cognitive approach used to understand online safety (LaRose, Rifon, & Enbody, 2008), this study examines how a sense of user personal responsibility can add to our understanding of how to educate or train users in ways that enhance their self-confidence and eventual enactment of online safety behaviors. Furthermore, the study compares the effectiveness of vicarious experience, an enactive learning approach, with a semantic, descriptive approach to explaining online safety. Policy makers, regulators, and educators will benefit from the development of theoretical principles that can guide and inform policy and educational/intervention tools.

2. Theoretical framework

2.1. Motivating online protections

Developing messaging strategies that motivate individuals to take personal responsibility for their online safety is key to improved Internet security. Foundational to developing these messages is examining the theoretical processes that are at work in response to different message types. The protection motivation theory, as well as the social-cognitive theory, are utilized to test these processes.

2.2. Protection motivation theory

An analogy can be drawn between protecting one's health and protecting his/her computer. Protection motivation theory (PMT; Rogers, 1983), a well-known approach to health communication, has also been applied to online safety protection (e.g., Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; LaRose & Rifon, 2006; Lee, Larose, & Rifon, 2008; Siponen, Mahmood, & Pahnila, 2014; Workman et al., 2008; Youn, 2005).

PMT posits that individuals perform two types of appraisals, threat and coping, when assessing the need to engage in a behavior (either adaptive or maladaptive) in response to a threat. An adaptive response is considered to be effective in protecting an individual from a threat, whereas a maladaptive response would be to do nothing or perhaps act in ways that might actually increase risk. In completing their threat appraisals, individuals assess their own vulnerability to the threat (the likelihood that the threat will occur) and the severity of the threat (the depth and breadth of the negative consequences of the threat). In addition, individuals assess their ability to perform an adaptive response (coping self-efficacy) along with the behavior's likelihood of being an effective threat deterrent (coping response efficacy). Additionally, intention to perform a protective behavior is influenced by the rewards associated with the behavior and perceived costs of performing the behavior.

We can apply these concepts to Internet users who are faced with risky online behaviors, such as deciding whether to open an attachment received in an email, on a daily basis. Some individuals might have spam filters activated, up-to-date virus protection software on their computers, and never open unexpected attachments, even if they appear to come from a friend (adaptive behaviors). Other individuals open unexpected attachments, download unexpected files or use an easy to guess password across multiple accounts, thus indicating maladaptive behavior. In deciding whether to open the attachment or not, individuals assess the threat associated with opening the attachment (threat appraisal) by thinking about the likelihood of the attachment containing a virus or Trojan (vulnerability to threat) and about the seriousness of the consequences that may follow if any malicious content bypasses installed protections (threat severity). Of course, these assessments are also predicated on the user actually having knowledge of the threat and being able to recognize it when it presents.

Individuals also think about their ability to cope with the threat (coping appraisals) and whether they're able to protect their computer (Anderson & Agarwal, 2010; Workman et al., 2008). Coping appraisals are formed from response efficacy beliefs about the effectiveness of the adaptive responses (e.g., the belief that not opening an attachment will protect one from viruses) and coping self-efficacy beliefs about one's ability to carry out the adaptive response successfully (e.g., the belief that an individual can tell the difference between a safe attachment and a dangerous one). Coping self-efficacy is a fundamental requirement for behavioral intention. If the subject feels confident in accomplishing a task, it will have less of a "cost" or difficulty in performing that task. The lower the cost of performing a protection function (e.g., the time and effort of changing a password) the more likely they are to engage in it. Other response costs associated with the adaptive response (e.g., the time it takes to send an email or text and wait for verification from the sender of the intent to send an attachment) are also taken into account. Of course, as experience is gained, the user may not consciously go through this elaborate process every time he/she is opening an attachment, and response cost decreases. Thus, experience and training has the potential to

enhance efficacy as well as reduce the barriers to enacting adaptive behaviors.

In the online safety domain, Lee et al. (2008) also applied PMT to using virus protection. They found that perceived vulnerability to a threat, response and coping self-efficacies predicted intentions to use virus protection. Perceived severity and response costs did not have an impact on safety intentions. However, two variables not included in the basic PMT model – perceived reward of the adaptive behavior (e.g., improved efficiency) and prior experience with viruses – were significant predictors. LaRose, Rifon, Liu, and Lee (2005) expanded the criterion behavior to include a range of protective behaviors including updating operating system and browser patches, updating virus protections, deleting cookies, and changing passwords. Coping appraisal variables, notably coping self-efficacy, were strong predictors of intentions to engage in these behaviors while threat appraisal variables were not. Variables drawn from later additions to the theory of planned behavior model on which PMT was originally based also predicted safety intentions: self-identity as a safe or unsafe Internet user and habit strength.

A fairly unexplored variable that fits into both self-efficacy and habit is previous knowledge. If an individual is even vaguely familiar with a procedure through previous knowledge, this familiarity brings ease in learning new terms. Interactive effects of self-efficacy, performance and knowledge have been found (Bell & Kozlowski, 2002). Previous knowledge about a topic would indicate experience and interest in an area. Just as in accepting new technologies, experience is a moderator, this knowledge may be a moderator in accepting online safety behaviors (Venkatesh, Thong, & Xin, 2012)

Studies of employee online safety behaviors suggest that social norms and corporate culture also play a role in determining online safety behaviors. Vance, Siponen, and Pahnila (2012) also looked at incorporating PMT and how past behavior influences Internet security practices in the workplace. They found that habits indeed were a strong factor in determining whether or not individuals complied faithfully with security practices. Consistent with what would be expected from PMT, they also found that response efficacy (e.g. if they follow certain procedures they will be safe from online threats) and self-efficacy (e.g. knowing exactly how to follow security procedures) were significant predictors in compliance, but these responses were strongly linked to habits. (Vance et al., 2012). Cox (2012) examined how corporate culture or social norms affected individual compliance with corporate security procedure policies. He found several elements that did support the application of PMT in online security analysis as well as the importance of social norms in influencing an individual's decision to comply with security procedures (Cox, 2012). This opens the potential of encouraging individual compliance by appealing to a perception of social norms that values online security.

2.3. Social cognitive theory

Widely used in understanding the learning process, the social cognitive theory (SCT) was formerly known as the social learning theory (Bandura, 1986). This broad framework has been used in understanding computer behavior (Cho, Lee, & Chung, 2010; Compeau & Higgins, 1995; Workman et al., 2008; Yi & Im, 2004), SCT conceptualizes human behavior as a dynamic reciprocal environment where personal factors environmental factors interact with behavioral factors (Bandura, 1986, 1991, 1997).

SCT recognizes the value of learning through observation, or "vicarious experience" which helps build confidence and a sense of self-efficacy in performing a task (Anderson & Agarwal, 2010; Bandura, 1991). This is especially valuable if the observer is able to watch someone who has enactive mastery of a skill (Gist, 1987). For example, it is not practically possible for the employees of an entire company to individually sit down with a master teacher to practice a new procedure. Therefore, a video or presentation is developed that allows employees to vicariously observe the procedure and learn how to effectively implement it. Observing those who have enactive mastery vicariously can help build self-efficacy and confidence in attempting to perform a task (Bandura, 1997). Using computer technology, enactive mastery training can be accomplished by providing a vicarious experience that is individually controlled. This allows the learner to have the ability to reference "how to" do each step or repeat it as they attempt the task, until they feel they have achieved enactive mastery of the procedure themselves.

According to SCT, environment, or perceived social norms in this situation, also plays a role in how readily individuals accept responsibility to perform specific behaviors. If perceptions of normative behavior call for certain behaviors then individuals are far more likely to follow those norms. In the realm of online safety there are widely varying perceptions of "normative" behavior (Douba, Rütten, Scheidl, Soble, & Walsh, 2014; Ybarra, Mitchell, Finkelhor, & Wolak, 2007). For example, if individuals feel that it is a social norm for them to take personal responsibility, and they have confidence in knowing how to perform the needed tasks, they will be more likely to follow online safety practices. On the other hand, if they feel that it is the social norm to rely on their ISP, operating system manufacturer, or Internet browser maker's responsibility to protect them, they might be disinterested users and only follow minimal safety procedures Therefore, common methods to encourage individuals to take personal safety precautions are often based on appealing to their sense of social norms, or persuasion (Van Noort, Kerkhof, & Fennis, 2008).

In the online safety realm, persuasion messages are quite common; warnings about the dangers of poor cyber safety frequent the headlines of news stories. These serve as a reminder that something should be done; yet, very few of these messages tell what should be done (Hoban et al., 2014). Little is known about the efficacy of these types of messages. If individuals have knowledge and experience, these persuasive messages may serve as effective reminders since they are likely to be more confident in their ability to perform protective behaviors. However, for those who are uncertain of exactly what they should do, this method may not bring the desired response of following safe online behaviors.

2.4. Approaches to learning and behavioral change

Individuals with little experience and expertise in the area of protective behaviors, need messages that offer solutions, clear demonstrations of behaviors that are effective for protecting against online safety threats. Thus, we expect that a fear or threat based intervention strategy, intended to persuade someone to take action, is unlikely to spur behavior in those without the necessary knowledge and coping related to the response efficacy required for taking action. Theoretically, vicarious experience is most likely to be effective when individuals lack prior experience in carrying out an advocated behavior (Bandura, 1997). That is because observations of others provide useful information in the absence of personal experience, but become less instructive when first-hand experience is available. According to SCT, individuals can increase their self-efficacy through vicarious experience. Demonstrating how to enact safety behaviors will allow this vicarious experience, building coping self-efficacy. Higher self-efficacy is also connected to the coping appraisal phase of the PMT, lowering the response cost and increasing the likelihood of the protecting behavior being implemented.

Therefore, we hypothesize:

H1. Vicarious experience of enactive mastery training will create greater (a) coping self-efficacy and (b) intentions to engage in self-protective behaviors than simple persuasion/threat messages.

H2. Internet users with a stronger sense of personal responsibility for maintaining online safety are more likely to engage in protective behaviors than those with a weak sense of personal responsibility.

Technology awareness, or general consciousness and perceptions of a technology innovation and what it entails, was found to be a potent antecedent of online safety precautions involving anti-spyware programs (Dinev & Hu, 2007). In present terms, technology awareness also bespeaks involvement with online safety issues. Involvement motivates elaboration and effort in the processing of new information (Celsi & Olson, 1979; Sohn, 2011). Bandura (1997) found that there was an interaction with involvement and coping self-efficacy. Taking his concepts to the realm of online safety, those in the low involvement, low self-efficacy group should be less likely to engage in safe behavior when told that online safety was their personal responsibility (Anderson & Agarwal, 2010; Rifon, Quilliam, & LaRose, 2005). In other words, for those who have extremely low self-efficacy, the concept of personal responsibility appears to be almost overwhelming, causing a maladaptive response. Given the importance of coping self-efficacy in the online safety domain, it is possible that an effective manipulation of coping self-efficacy could improve results and possibly counteract the negative effect found among low involvement, low self-efficacy individuals. Vicarious experience, or seeing others perform a task successfully, can heighten self-efficacy (Gist, Schwoerer, & Rosen, 1989; Lam & Lee, 2006). While direct, enactive mastery experience through personalized training is traditionally considered to be more effective than vicarious experience, the vicarious approach has certain advantages when promoting safe behavior is the goal (Hsieh, Rai, & Keil, 2008; Workman et al., 2008).

Finally, if personal responsibility is indeed an indication that the target behavior is within the scope of the individual to affect, then an interaction with the self-efficacy manipulation can be expected. That is because observing how to perform protective behavior is more likely to make persons willing to accept personal responsibility than merely telling them that the behavior is easy to perform. Potentially, this interaction could reverse the boomerang effect found by LaRose and Rifon (2006), in which those in the low involvement, low self-efficacy group were less likely to engage in safe behavior when told that online safety was their personal responsibility compared to those who were asked to believe the responsibility lay with others. The motivation created by a sense of personal responsibility may also have a synergistic effect with enactive mastery, and moderate the effectiveness of the interventions. Therefore, we hypothesize:

H3. Level of personal responsibility will moderate the effects of the intervention strategy. (a) Those with low personal responsibility will have a greater response (increased safety behavior intentions) to enactive mastery than those who have a high level of personal responsibility.

H4. (a) Personal responsibility norms and (b) coping self-efficacy will be positively related to intentions to engage in protective behavior.

3. Research methods

3.1. Participants

Adult home Internet users were the population of interest for the present study. Participants were recruited by mail from a Midwestern state to complete an online survey. A commercial mailing list vendor provided a random sample of households. The initial mailing included a letter describing the purpose of the study and participants' rights as human subjects. Shortly following the initial mailing, an additional mailing included a letter containing the login ID for the survey and directed participants to the online questionnaire. The letter also included a nominal cash incentive and a postcard on which non-Internet users indicated their gender and year of birth. A reminder postcard and follow-up letter were sent to non-respondents. The entire process was over a period of two to three weeks. The mail contacts were therefore a variation of the total design method (Dillman, 2000).

Of the 2000 mail solicitations sent, 109 (5%) had bad addresses and were returned; leaving a total usable sample of 1,891. A total of 441 responded to the solicitation. One hundred and sixty-one Internet users completed the survey and 275 returned the non-Internet user postcard (22% total response rate). More than half of participants (57.76%) were male, and 40.37% female (1.86% did not indicate their gender), with an average age of 47 ($M = 47.17$, $SD = 12.64$). The majority of participants (88.20%) were Caucasian. More than a third of participants (36.66%) indicated an average household income under $50,000; the remaining 64.34% had an average annual income greater than $50,000. On average, participants had about 15 years of schooling beyond kindergarten ($M = 14.84$, $SD = 2.85$; *Range* = 2–23). They had between 1 and 25 years of Internet experience ($M = 10.77$, $SD = 4.97$).

3.2. Procedure

When participants logged into the website the online survey software randomly assigned them to one of four treatment conditions. Two factors were manipulated: the intervention strategy and the personal responsibility treatment. Respondents viewed web pages corresponding to one of the following four treatment conditions: (1) high personal responsibility-persuasion; (2) low personal responsibility-persuasion; (3) high personal responsibility-vicarious experience; or (4) low personal responsibility-vicarious experience conditions.

The personal responsibility manipulation followed that used previously by LaRose et al. (2008) except that Internet Service Providers (ISPs) were singled out as the "others" responsible for online safety. To manipulate the sense of normative behavior for this experimental study, a simple verbal manipulation of personal responsibility was administered by arguing, in the high personal responsibility condition, that "Online safety is everyone's job," while in the low personal responsibility condition, "online safety isn't my job," prefacing a series of online safety tips provided by a mock-up *Consumers Report* news article. The high personal responsibility condition respondents viewed a short introductory text that was headlined "Online Safety Is My Job and Yours." The theme was repeated four times (e.g. "it's our job to help protect ourselves," "we must all take responsibility for our own online safety"). In the low personal responsibility condition, the headline read "Online Safety Is My Internet Provider's Job." The short introductory text rephrased and repeated that notion four times (e.g., "it's their job to protect us," "it is your ISP's job to keep you safe online") and also pointed out "we are paying them for our Internet service, after all." The following pages contained information about preventing online safety hazards such as viruses and spyware reproduced from the popular press (Consumers Union, 2006).

The same safety tips were provided in both the persuasion and vicarious experience conditions. The verbal persuasion condition was designed to lead people through simple suggestion into believing that they could successfully cope with a threat. The safety tips were prefaced as follows: "Here are some simple tips for keeping yourself safe from hackers and viruses. They are easy if you try."

For example, visitors were told to "Use updated antispyware software to scan your hard drive regularly. Always download it from a trusted site." However, the verbal persuasion condition stopped short of teaching participants how to successfully accomplish the suggested behaviors.

Live or symbolic modeling is necessary to achieve a vicarious experience (Bandura, 1997). The vicarious experience condition modeled how to engage in adaptive behaviors by showing participants step-by-step instructions for executing the safety tips. These were illustrated with screen grabs from web sites as if the respondent was being shown how to perform the adaptive behavior by a knowledgeable person, the model, in socio-cognitive terms, sitting at their computer as the respondent looked on. Respondents were instructed as follows: "Here are some simple tips for keeping yourself safe from hackers and viruses. They are easy if you let us show you how. Just click on the 'Show Me How' buttons." When clicked, the "Show Me How" buttons gave respondents step-by-step visual and text-based instructions so the participant could observe the procedure for keeping safe online (e.g. "1. Select 'Internet Options' under 'Tools' in the menu bar," "2. Select the 'Security' tab in the Internet Options menu," and "3. In the 'Security' menu, press the 'Custom Level' button at the bottom of the menu. Then select 'Medium' in the 'Reset to:' drop-box"). The screen grabs included red circles that were placed around the relevant part of each screen shot that directed the respondent onward. When clicked, the circles led respondents to the next step in the sequence. Respondents were directed back into the survey application to complete the questionnaire after viewing the stimulus materials.

3.3. Operational measures

The dependent variable was a four-item additive index ($\alpha = .80$, $M = 4.93$, $SD = 1.43$) of intentions to engage in specific online safety behaviors. Participants were asked about their intentions to scan with an anti-malware program, carefully read the license agreement before downloading software, scan with an anti-Trojan program, and look for a better anti-malware program. Intentions were assessed on seven point, Likert- type scales, where very likely was scored seven and very unlikely scored one.

The personal responsibility norm was defined by three items from LaRose et al. (2008). These were assessed on a seven point Likert- type scale ($\alpha = .73$, $M = 5.40$, $SD = 1.18$) ranging from strongly agree (seven) to strongly disagree (one). Items included "online safety is my personal responsibility," "Online safety is somebody else's job, not mine (reflected)," and "online safety is something I leave to the experts (reflected)." These included two items (adapted from Lee & Kozar, 2008) indicating denial of personal responsibility, which were reflected.

Response efficacy and coping self-efficacy were assessed following establish procedures of protection motivation research in which multi-item indices are developed anew for each behavioral domain (e.g. Prentice-Dunn, Jones, & Floyd, 1997). Coping self-efficacy ($\alpha = .92$, $M = 5.28$, $SD = 1.41$) was evaluated with five, seven-point Likert- type scales ranging from strongly agree to strongly disagree. Participants were asked if they were confident they could "identify the terms of software license agreements that pose a threat," "download a Trojan scanner," "identify the terms of web site privacy policies that threaten me," "identify a new anti-malware program that will improve my safety," and "tell when it is safe to open an email attachment." Response efficacy ($\alpha = .86$, $M = 5.89$, $SD = 1.15$) was a three- item scale, also specific to the online safety domain. Items included: "read and understand the license agreement before I download software," "download a Trojan scanner," and "read and understand web site privacy policies."

A measure of prior knowledge of online safety behavior was formed from questions asking about the respondents' knowledge of two forms of malicious software: spyware and Trojans (following Dinev & Hu, 2007). The response categories were "I never heard of it (scored 0), I have heard of it but I don't know the details (1), I know about it but I don't know what to do about it (2), I know what to do about it when I get it (3), and I know what to do about it when I get it and also how to protect myself against it (4)." The combined scores ($\alpha = .82$, $M = 2.00$, $SD = 1.00$) were divided at the midpoint. Those at or below the median of 2.0 were assigned to the low knowledge level. Those with scores above the median were placed in the high knowledge category.

Technology awareness was computed from two, seven-point, Likert- type, strongly agree/strongly disagree scales (Dinev & Hu, 2007, $\alpha = .78$, $M = 4.13$, $SD = 1.52$). Participants were asked, "I follow news and developments about malware technology," and "I discuss with friends and people around me the security issues of the Internet." Message involvement was measured by two items: "how relevant was the information to you?" and "how carefully did you read the online safety information" ($\alpha = .70$, $M = 3.97$, $SD = .81$). The former was scored on a five-point scale ranging from very relevant (5) to very irrelevant (1) (adapted from Ohanian, 1989). The latter was assessed on a scale ranging from very carefully (5) to very carelessly (1).

3.4. Data analysis

Data were analyzed using SPSS version 20.0 (IBM, 2014). Average values for all multi-item indices were computed by dividing the total scores by the respective number of items. The General Linear Model procedure was used to test the hypotheses. Univariate ANOVA was used to analyze simple effects where interaction terms were found. The effects of the personal responsibility and coping self-efficacy manipulations were assessed as main effects on their respective dependent variables (personal responsibility norm and coping self-efficacy). To evaluate the effects of these treatments and prior knowledge on online safety behavior, a between-subjects $2 \times 2 \times 2$ factorial analysis of variance was performed. Personal responsibility and coping self-efficacy treatments were manipulated variables and prior knowledge was a measured variable. A common set of covariates was used in these analyses: technology awareness, message involvement, response efficacy, gender, age of respondent, years of formal education, and the log of the years of Internet experience.

To test for the proposed mediating effect, four conditions were examined (Baron & Kenny, 1986). First, the interaction among prior knowledge and the personal responsibility and self-efficacy manipulations was tested to establish that there was an effect on the dependent variable to be mediated, intentions to engage in protective behavior. Second, the relationship of the experimental manipulations to the mediating variables was tested. The $2 \times 2 \times 2$ factorial analysis was repeated with the measures of personal responsibility norms and coping self-efficacy as covariates. Since SPSS uses Type III (i.e. regression) sums of squares by default, this was equivalent to testing whether the interaction effects among prior knowledge and the personal responsibility and self-efficacy manipulations were still present while controlling for the proposed mediating variables (measures of coping self-efficacy and personal responsibility norms obtained on the posttest). In that analysis, main effects of the proposed mediating variables tested whether the mediators affected the outcome variable. The results are reported in the following section.

Eight cases were dropped from analysis of variance due to missing demographic data. In one case, a missing value of an item comprising multi-item scales was substituted with a mean value. Other than that, there were no missing data. Since the present study was believed to be the first of its kind to explore this type of online safety interventions, an alpha level of .1 was adopted.

4. Results

As a manipulation check, respondents were asked who was responsible for online safety according to the experimental website. Sixty-five percent of those in the high personal responsibility condition correctly indicated that the responsibility was said to be theirs. This was significantly more than in the low personal responsibility condition ($\chi^2(153) = 9.03$, $p < .01$). Hypothesis 1a was confirmed ($F(10,142) = 10.77$, $p < .05$, $\eta_p^2 = .43$). There was a significant main effect of the intervention strategy on coping self-efficacy ($F(1,142) = 4.06$, $p < .05$, $\eta_p^2 = .03$) after controlling for covariates. As expected, those who were exposed to the vicarious experience treatment had higher levels of coping self-efficacy than those in the persuasion condition. Those who had prior knowledge of online safety problems tended to have higher levels of coping self-efficacy ($F(1,142) = 2.40$, *ns*). However, H1b was not supported; after controlling for the covariates, there was no significant main effect of the personal responsibility condition on safety behavior intentions ($F(1,139) = 1.38$, *ns*).

In addition, there were no main effects of the personal responsibility manipulation, disconfirming H2 ($F(1,145) = 2.50$, $p = .12$) and H2b ($F = (1,139) = .54$, *ns*). After correcting for the covariates there was not a significant main effect for the personal responsibility treatment on either coping efficacy or safety behavior intentions.). There was also no main effect for prior knowledge of online protections ($F(1,139) = .32$, *ns*). However, the overall (i.e., including main effects, interaction effects, and covariates) analysis of variance of intentions to engage in online safety behavior was significant ($F(13,139) = 8.66$, $p < .001$, $\eta_p^2 = .45$.

There was a significant three-way interaction effect (See Figs. 1 and 2) among the personal responsibility and coping self-efficacy treatments and prior knowledge ($F(1,139) = 6.95$, $p < .05$, $\eta_p^2 = .05$) supporting H3. That is, the interaction effect of the two variables (the personal responsibility and vicarious experience manipulations) at the lower level of prior knowledge was different from the interaction effect of those two manipulations at the higher level of knowledge. To interpret this interaction, a univariate ANOVA analysis was performed to examine the coping self-efficacy treatment within levels of the personal responsibility manipulation and prior knowledge.

Among those with little online safety knowledge and for whom personal responsibility for online safety was stressed, the vicarious experience treatment produced an increase in safety intentions ($F(1,139) = 2.90$, $p < .1$, $\eta_p^2 = .021$) compared to persuasion (see Fig. 1). Thus Hypothesis 1b, while not supported, holds for the low-knowledge, personal responsibility group. Among those who were not knowledgeable of online safety and who were informed that online safety was *not* their personal responsibility the self-efficacy manipulation had the opposite effect (the solid line in Fig. 1). There, the persuasion condition was more effective ($F(1,139) = 2.84$, $p < .1$, $\eta_p^2 = .02$).

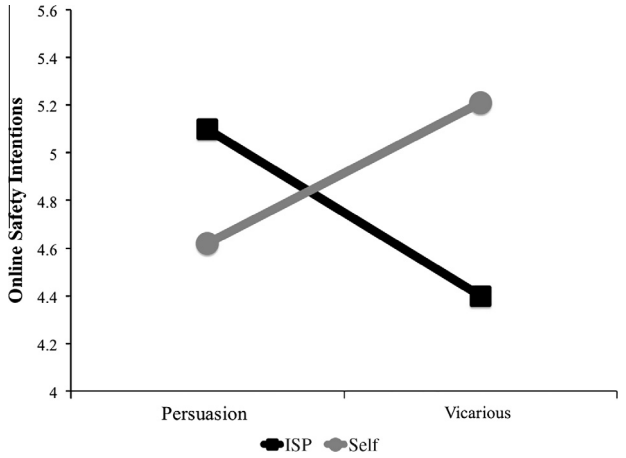

Fig. 1. Estimated marginal means of online safety intentions among those with low safety knowledge.

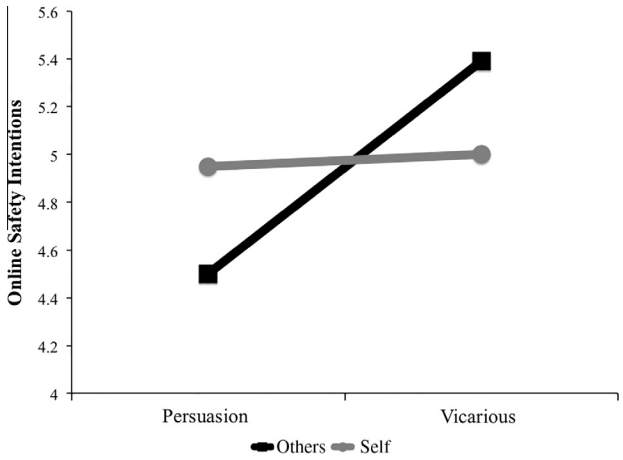

Fig. 2. Estimated marginal means of online safety intentions among those with high safety knowledge.

For those who had prior knowledge of online safety measures and who were told that online safety was their personal responsibility (the dotted line in Fig. 2), the self-efficacy manipulation had no effect ($F(1,139) = .05$, *ns*). The vicarious experience condition was more effective than persuasion among knowledgeable individuals who were told that their ISPs, rather than themselves, were responsible for online safety (the solid line in Fig. 2, $F(1,139) = 4.60$, $p < .05$, $\eta_p^2 = .03$). This was contrary to Hypothesis 1 b and also the reverse of the relationship observed among those with low levels of prior knowledge.

The difference between the high and low personal responsibility conditions was significant ($F(1,139) = 4.85$, $p < .05$, $\eta_p^2 = .03$) within the vicarious experience condition for those with little prior knowledge (the right hand points in Fig. 1). The other apparent differences between high and low responsibility conditions were not significant. Thus, Hypothesis 3 was upheld among those with low levels of prior knowledge, but not for high levels of knowledge.

Hypotheses 4 was tested in an analysis in which intentions to engage in protective behavior were the dependent variable, the previous interaction effects among prior knowledge by personal responsibility and self-efficacy manipulations were the independent variables, and personal responsibility norms and coping self-efficacy were covariates. The analysis was significant $F(9,143) = 6.48$, $p < .001$, $\eta_p^2 = .29$. There was a significant main effect for personal responsibility norms ($F(1,143) = 7.35$, $p < .01$, $\eta_p^2 = .05$) and for coping self-efficacy ($F(1,143) = 18.14$, $p < .001$, $\eta_p^2 = .11$), confirming Hypothesis 4a and b, respectively. The interaction effects predicted in Hypothesis 4 was confirmed, indicating that the manipulations had an effect on protective behavior. Also, the self-efficacy and personal responsibility manipulations had the predicted effects on their respective mediating variables (coping self-efficacy and personal responsibility norms as measured in the posttest). Therefore, there was evidence that the predicted mediation effects were present (Baron & Kenny, 1986).

5. Discussion

Despite widespread warnings of the dangers of poor online safety practices, a surprising percentage of users are still very naïve about safety (Jang-Jaccard & Nepal, 2014; Sundar & Marathe,

2010). There is a need to increase coping self-efficacy for individuals of all ages and backgrounds (Jiang et al., 2014; Tsai et al., 2014). It is important to understand what message cues related to online safety are successful in eliciting protective behaviors through activating threat and coping appraisal processes (Siponen et al., 2014). This research found the efficacy of a multi-pronged strategy. The safety deficits of the most vulnerable Internet users – those lacking knowledge about how to handle changing online threats – might be overcome by stressing personal responsibility for online safety together with providing vicarious experience with protective measures. When personal responsibility was stressed, providing naïve users with vicarious experiences with safe online behaviors had a greater effect on safety intentions than merely telling them that it was easy to protect themselves through safety tips. Also among those unfamiliar with online safety protections, emphasizing personal responsibility was more effective than emphasizing the responsibility of others when combined with vicarious experience.

Vicarious experience and personal responsibility interventions should be used in concert with one another. Vicarious experience by itself was superior to persuasion in improving coping self-efficacy, previously shown to be a key determinant of safe behavior on the Internet. This supported the argument that vicarious experience is superior to persuasion as an intervention strategy to bolster coping self-efficacy. However, the vicarious experience manipulation had no direct effect on behavioral intentions. It improved safety intentions only in combination with the personal responsibility manipulation. However, the present results suggest that although self-efficacy and personal responsibility interventions should be combined, the two treatments had complex interactions and should be used together with caution. Among naïve users lacking prior knowledge with online safety hazards, a vicarious experience treatment might be too much to them to cognitively process. There is the danger of overloading them with information and having a subsequent "shut down" with them disregarding online safety.

The partial reversal of these effects among those knowledgeable about online protections argues that it is perhaps inadvisable to allow already knowledgeable individuals to simply be reminded of social norms by informing them that their safety is a shared responsibility. Offering appropriately designed vicarious experience to users at all skill levels can be helpful in gaining better compliance with online safety standards. Even for those who claimed to be more knowledgeable about online safety were more likely to enact protections through the vicarious experience intervention than through persuasion. The protections offered by ISPs, even "automatic" ones, still require a considerable degree of effort by the user to obtain and maintain. When told that the responsibility for online safety lies with their ISP, users may willingly yield to their providers' protections and diminish their personal resolve to act safely on their own behalf when the persuasion approach is used. That is, they avoid a complex task even when they are told it is easy to perform, because their own experience has informed them otherwise. Vicarious experience generates confidence that the protective behaviors can be successfully enacted. Relieved of the anxiety-inducing onus of bearing the sole responsibility for online safety, knowledgeable users are then more likely to act safely when exposed to vicarious experience rather than just persuasion.

The two self-efficacy conditions did not produce differing results among those with prior knowledge in the personal responsibility condition. Perhaps verbal self-efficacy persuasion, even the simple "you can do it if you try" approach taken here, is sufficient to overcome the anxiety aroused by emphasizing personal responsibility among those who have already assumed some degree of responsibility in the past. However, among those who consider themselves experienced in taking safety precautions, anxiety about the adequacy of current online protections may be re-instituted by reminding users of their personal responsibility. That, coupled with a vicarious reminder of the complexity of such protections, may undermine intentions to take further protective actions, resulting in a null effect relative to persuasion.

6. Limitations and implications

6.1. Design limitations

This sample was drawn from a single state and collected through a traditional mail method, which then required participants to log into participate in the intervention. The unsurprising, but relatively low response rate, limits its external validity. However, this study does capture an understudied population for following online safety procedures, middle aged adults, since the average age of respondents was 47 ($M = 47.17$, $SD = 12.64$). The reliability of the personal responsibility measure, while adequate for exploratory studies in relatively new domains such as this one, may have attenuated the impact of the experimental manipulation. Even though technological adoption, acclimation, changes and challenges are accelerating at an astounding pace, the non-professional's understanding of safety when using technology is often at a much slower pace (Lacey, 2011).

The vicarious experience condition was designed to simulate modeling of protective actions, as if these steps were performed by an expert user sitting at the respondent's computer, while the respondent looked on. However, given the privacy concerns of adding extensive cookies to monitor participants' viewing of each page, no manipulation check was performed to verify respondents' reactions to each page. The condition was labeled vicarious experience to remain consistent with the SCT framework. However, this condition might also be characterized simply as an active intervention in which respondents were asked to interact with a web page rather than passively consume information. However, given continuing improvements in technology, a more realistic vicarious condition such as a 3D immersive environment could better test the findings of this experiment.

6.2. Implications for risk communications

Above all, the present research argues for careful targeting of messages to audiences based on their entry-level knowledge. An advantage of online interventions is that they can be tailored on the fly to the user. For example, a short self-test, two questions in the present study, could evaluate users' knowledge levels upon entering a website. Users could then be routed to the appropriate combination of self-efficacy and personal responsibility treatment based on their entry-level knowledge.

Vicarious experience interventions would seem to be easier to implement than progressive mastery interventions in which individuals must be coached to gradually improve their performance. Bandura's (1997) supposition that vicarious experience works best when knowledge is lacking was supported in the present research, although only when combined with a message stressing personal responsibility. Such interventions hold the promise of affecting those hardest to reach, those with little prior interest or exposure to protective measures.

A preliminary answer to the question of how to motivate the public to protect themselves better online can now be offered. It is vital to segment users according to their prior knowledge about online protections. Interventions aimed at naïve users, such as those enrolled in introductory computer classes, should emphasize the personal responsibility individual users have for their own safety in combination with step-by-step demonstrations of how

to carry out protective actions. For experienced users the emphasis should be placed on protections that augment those offered by their Internet providers in pursuit of a sense of shared responsibility and continued vigilance. Public information campaigns of the type proposed by the SaferNet Act of 2007 are much needed, but they should include components targeted not just to school children and parents, but also to older adult users. They should also "train the trainers" to stress personal responsibility and to focus more on protective measures rather than dwell on the dangers of online life. The cooperation of Internet providers and software companies should be sought to provide step-by-step instructions for users in a consistent and usable format.

The strength of the present personal responsibility and vicarious experience treatments can be improved. More sophisticated persuasion tactics could highlight the positive outcomes of taking responsibility and provide on-screen role models of responsibility-takers. Vicarious experience could be further improved by associating the "show me how" lessons with on-screen characters that match the demographic and user characteristics of individual viewers, since model similarity is known to enhance the effectiveness of vicarious, observational learning (Bandura, 1986).

Reflecting on both PMT and SCT, the present study suggests new directions for research focusing on experimental manipulations. A great deal of attention has focused on manipulating fear appeals (e.g., Witte, 1994; Witte & Allen, 2000) but less on changing the self-efficacy beliefs that may determine their effectiveness in promoting protective behavior. Perhaps strong self-efficacy manipulations, such as vicarious experience or enactive mastery strategies, are required when prior knowledge of protective measures is lacking. Entry-level knowledge may be crucial when the protective behaviors are themselves so complex or aversive that enacting them may induce counterproductive emotional reactions.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. #1318885. 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

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.

Bandura, A. (1986). *Social foundations of thought and action*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*, 248–287.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York: W.H. Freeman.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology, 51*, 1173–1182.

Bell, B. S., & Kozlowski, W. J. (2002). Goal orientation and ability: Interactive effects on self-efficacy, performance, and knowledge. *Journal of Applied Psychology, 87*(3), 497–505.

Celsi, R. L., & Olson, J. C. (1979). The role of involvement in attention and comprehension processes. *Journal of Consumer Research, 15*(9), 210–224.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987–995. http://dx.doi.org/10.1016/j.chb.2010.02.012.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189–211.

Consumers Union (2006). Stay safe online: Best software tools & strategies. *Consumer Reports, 71*(9), 25–29.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849–1858. http://dx.doi.org/10.1016/j.chb.2012.05.003.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among Internet users. *Computers in Human Behavior, 26*(6), 1739–1747. http://dx.doi.org/10.1016/j.chb.2010.06.023.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581–590). ACM. April.

Dillman, D. A. (2000). *Mail and internet surveys: The tailored design method* (Vol. 2). New York: Wiley.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association of Information Systems, 8*(7), 386–408.

Douba, N., Rütten, B., Scheidl, D., Soble, P., & Walsh, D. (2014). Safety in the Online World of the Future. *Technology Innovation Management Review, 4*(11).

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security, 46*, 18–31. http://dx.doi.org/10.1016/j.cose.2014.06.008.

Gist, M. E. (1987). Self-efficacy: Implications for organizational behavior and human resource management. *Academy of Management Review, 12*(3), 472–485. http://dx.doi.org/10.5465/AMR.1987.4306562.

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of Applied Psychology, 74*(6), 884–891. http://dx.doi.org/10.1037/0021-9010.74.6.884.

Hoban, K., Rader, E., Wash, R., Vaniea, K. (2014). Computer security information in stories, news articles, and education documents. Poster in Symposium on Usable Privacy and Security (SOUPS).

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low Self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189–220.

Hsieh, P.-A., Rai, A., & Keil, M. (2008). Understanding digital inequality: Comparing continued use behavioral models of the socio-economically advantaged and disadvantaged. *MIS Quarterly, 32*(1), 97–126.

IBM (2014). SPSS 20.0.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. http://dx.doi.org/10.1016/j.jcss.2014.02.005.

Jiang, M., Rifon, N. J., Cotten, S. R., Tsai, H. S., Shillair, R., LaRose, R., & Alhabash, S. (2014). Generational differences in electronic banking: Understanding what motivates older generations to adopt. In *Presented at the AMA summer marketing educators conference 2014, August 1–3, San Francisco, CA* (August).

Johnston, B. A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.

Lacey, D. (2011). *Managing the human factor in information security: How to win over staff and influence business managers*. John Wiley & Sons.

Lam, J. C. Y., & Lee, M. K. O. (2006). Digital inclusiveness-longitudinal study of internet adoption by older adults. *Journal of Management Information Systems, 22*(4), 177–206. http://dx.doi.org/10.2753/MIS0742-1222220407.

LaRose, R., & Rifon, N. (2006). Changing online safety behavior: Experiments with online security and privacy. *Paper presented to the international communication association, Dresden, Germany, June*. <www.msu.edu/~isafety>.

LaRose, R., Rifon, N., Liu, X., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. *International communication association. New York*. <www.msu.edu/~isafety>.

LaRose, R., & Rifon, N. (2007). *Michigan state university internet safety survey*. East Lansing, MI: Michigan State University. <www.msu.edu/~isafety>.

LaRose, R., & Rifon, N. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs, Summer, 41*, 127–149.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71–76.

Leder, F., Werner, T., & Martini, P. (2008). Proactive botnet countermeasures: An offensive approach. *NATO cooperative cyber defense: Centre of excellence.* <http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf>.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445–454.

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109–119.

Ohanian, R. (1989). Ego centrality as an indicator of enduring product Involvement". *Journal of Social Behavior and Personality, 4*(4), 443–455.

Prentice-Dunn, S., Jones, J. L., & Floyd, D. L. (1997). Persuasive appeals and the reduction of skin cancer risk: The roles of appearance concern, perceived benefits of a tan, and efficacy information. *Journal of Applied Social Psychology, 27*, 1041–1047.

Prieger, J. (2013). The impact of government policies on access to broadband. *School of public policy working papers*.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online*. Washington, DC: Pew Research Center's Internet & American Life Project. <http://pewinternet.org/Reports/2013/Anonymity-online.aspx> (September 5).

Rifon, N., Quilliam, E. T., & LaRose, R. (2005). Consumer perceptions of online safety. *International communication association: Communication and technology division, New York, NY, May 27*. <https://www.msu.edu/~isafety/papers/ICApanelfg.htm>.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social psychophysiology*. New York: Guilford Press.

SAFER NET Act (2006). 109 U.S.C. § H.R. 4982 <http://www.gpo.gov/fdsys/pkg/BILLS-109hr4982ih/pdf/BILLS-109hr4982ih.pdf>.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. http://dx.doi.org/10.1016/j.im.2013.08.006.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.

Sohn, D. (2011). Anatomy of interaction experience: Distinguishing sensory, semantic, and behavioral dimensions of interactivity. *New Media & Society, 13*(8), 1320–1335. http://dx.doi.org/10.1177/1461444811405806.

Sundar, S. S., & Marathe, S. S. (2010). Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research, 36*(3), 298–322. http://dx.doi.org/10.1111/j.1468-2958.2010.01377.x.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2014). Understanding online safety behavior in the online banking context. In *Presented at the international communication association's 64th annual conference, May 22–26. Seattle, WA*

Van Noort, G., Kerkhof, P., & Fennis, B. M. (2008). The persuasiveness of online safety cues: The impact of prevention focus compatibility of Web content on consumers' risk perceptions, attitudes, and intentions. *Journal of Interactive Marketing, 22*(4), 58–72. http://dx.doi.org/10.1002/dir.20121.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190–198. http://dx.doi.org/10.1016/j.im.2012.04.002.

Venkatesh, V., Thong, J. Y., & Xin, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Witte, K. (1994). Fear control and danger control – a test of the extended parallel process model (eppm). *Communication Monographs, 61*(2), 113–134.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), 591–615.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816. http://dx.doi.org/10.1016/j.chb.2008.04.005.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Internet Prevention Messages. *Archives of Pediatrics & Adolescent Medicine, 161*(2), 138. http://dx.doi.org/10.1001/archpedi.161.2.138D.

Yi, M. Y., & Im, K. S. (2004). Predicting computer task performance. *Journal of Organizational and End User Computing, 16*(2), 20–37. http://dx.doi.org/10.4018/joeuc.2004040102.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110.