COMPUTERS & SECURITY 59 (2016) 138–150

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# Understanding online safety behaviors: A protection motivation theory perspective

*Hsin-yi Sandy Tsai* [a,*], *Mengtian Jiang* [b], *Saleem Alhabash* [b,c], *Robert LaRose* [c], *Nora J. Rifon* [b], *Shelia R. Cotten* [c]

[a] *Department of Communication & Technology, National Chiao Tung University, No.1, Sec. 1, Liujia 5th Rd., Zhubei City, Hsinchu County 302, Taiwan*

[b] *Department of Advertising + Public Relations, Michigan State University, 404 Wilson Rd., East Lansing, MI 48823, USA*

[c] *Department of Media and Information, Michigan State University, 404 Wilson Rd., East Lansing, MI 48823, USA*

ARTICLE INFO

*Article history:*
Received 24 May 2015
Received in revised form 17 February 2016
Accepted 22 February 2016
Available online 2 March 2016

*Keywords:*
Online safety
Computer security
Protection motivation theory
Response cost
Habit strength

ABSTRACT

Internet users experience a variety of online security threats that require them to enact safety precautions. Protection motivation theory (PMT) provides a theoretical framework for understanding Internet users' security protection that has informed past research. Ongoing research on online safety recommends new motivational factors that are integrated here in a PMT framework for the first time. Using PMT, a cross-sectional survey (N = 988) of Amazon Mechanical Turk (MTurk) users was conducted to examine how classical and new PMT factors predicted security intentions. Coping appraisal variables were the strongest predictors of online safety intentions, especially habit strength, response efficacy, and personal responsibility. Threat severity was also a significant predictor. Incorporating additional factors (i.e., prior experiences, subjective norms, habit strength, perceived security support, and personal responsibility) into the conventional PMT model increased the model's explanatory power by 15%. Findings are discussed in relation to advancing PMT within the context of online security for home computer users.



## 1. Introduction

Internet users do not feel safe online. They experience threats related to identity theft, malware or viruses, security of financial information, and phishing attacks that may harm their professional reputation and personal lives (Cyber Security, 2012; Microsoft, 2014; Rainie et al., 2013). Online threat perceptions stem from personal experiences, others' experiences, and the news media, thus leading to a realistic understanding of online safety threats. Although Internet users use built-in system settings (e.g., antimalware software, firewall, and automatic updates) to maintain their online protections, three in five people do not believe they can be completely anonymous online and they are increasingly worried about their personal information online (Rainie et al., 2013).

Ninety-nine percent of computers are susceptible to threat attacks as a result of the prevalence of Adobe Reader, Adobe Flash, and Oracle Java (Zaharia, 2015). Despite high risks associated with common computer and technology activities,

This work was supported by the National Science Foundation under Grant No. 1318885.

* *Corresponding author.* Tel.: +886 3 5712121 ext. 58718.
*E-mail address:* circles0309@gmail.com (H.S. Tsai).

http://dx.doi.org/10.1016/j.cose.2016.02.009

Internet users take very few actions to protect their computers, smartphones, and tablets (AV Comparatives, 2013; Cyber Security, 2012). Moreover, they engage in activities that jeopardize their online safety and reputation, such as posting information that could be misused by online predators (Microsoft, 2014; Rainie et al., 2013).Threats to online safety translate into cybercrime, with U.S. financial losses ranging from $24 to $120 billion annually (Waterman, 2013), making online safety a policy and educational priority.

Taking into account the discrepancy between realizing threats and taking protective actions, the current study uses protection motivation theory (PMT) to understand what drives online safety behaviors in the context of home computer use. This paper contributes to research on computers and security by integrating a commonly ignored PMT variable: prior experience with safety hazards, and other new coping appraisal variables (i.e., habit strength, perceived security support, personal responsibility, and subjective norms) into the PMT model to further examine the cognitive coping process related to expression of intentions to take security protective actions. Prior investigations of online safety protection motivations are examined to develop integrated models of online safety protection.

## 2. PMT and the online safety question

Based on the theory of reasoned action (Fishbein and Ajzen, 1975), PMT deciphers how and why individuals decide to undertake protective behaviors (Rogers, 1975, 1983). PMT proposes that protective behavior is motivated by threat and coping appraisals. Threat appraisals are determined by perceived vulnerability and susceptibility to risks, as well as rewards associated with unsafe behaviors. Coping appraisals are based on coping self-efficacy, response efficacy, and response costs associated with safe or adaptive behaviors. Coping self-efficacy is the belief that individuals can successfully carry out protective behaviors. Response efficacy is the belief in the effectiveness of the protections. Response costs refer to the costs of using security protections. Threat appraisals and coping appraisals determine behavioral intentions to adopt protections (security intentions) in the current study. Individuals undertake safety precautions (e.g., downloading and updating antivirus software) they believe are effective in protecting them online and are able to enact with reasonable resource expenditure. Otherwise they may ignore the risk and refrain from taking any protective actions.

Ongoing consumer security research can be interpreted through the lens of PMT. Liang and Xue (2010) proposed the technology threat avoidance theory based on "protection motivation theory, the health belief model, and risk analysis research" (p. 79). In their view, TTAT integrates PMT's overall framework in identifying key factors that predict technology threat avoidance behavior, mainly in relation to threat and coping appraisal and their role in informing protective behaviors, as influenced by the level of risk tolerance (representing risk analysis research) and social influences (relating to the health belief model). In the current study, we integrate the TTAT view as a means of extending PMT. Liang and Xue (2010) found that both threat appraisals (perceived susceptibility and severity) and coping appraisals (safeguard effectiveness, safeguard cost, and self-efficacy) were significant predictors of computer threat avoidance behaviors. Other studies also found that confidence in security behaviors (coping self-efficacy), concern about security threats (threat susceptibility), perceptions that individual Internet users should protect their online safety (personal responsibility), and perceptions about others' opinions (subjective norms) predicted attitudes toward security-related behaviors (Anderson and Agarwal, 2010). Subjective norm has been incorporated into the PMT model in some studies and was found to be a significant predictor of computer security-related policy or software adoption (Herath and Rao, 2009; Ifinedo, 2012; Lee and Larsen, 2009). In this regard, subjective norms refer to an individual's perceptions about how others who are important to him or her think he/she should behave (Conner and Armitage, 1998), while social influence is a more generalist view of how an individual is influenced by others in his/her surroundings (Liang and Xue, 2010). Johnston and Warkentin (2010) express social influences as social norms, which refer to perceptions of how others are behaving. However, many of these studies were in an organizational context (e.g., Culnan and Williams, 2009; Hu et al., 2012; Lowry and Moody, 2015; Posey et al., 2013; Vance et al., 2013). In the current study, we believe that subjective norms are better equipped to grasp social influences on protective behaviors.

Other studies have pointed out the differences in factors affecting security protection for organizational and home computer use (e.g., Dang-Pham and Pittayachawan, 2015; Li and Siponen, 2011). Prior experience with safety hazards, personal responsibility, subjective norms, perceived security support and habit strength have not been previously considered as part of a comprehensive overall framework for home computer security. In the current study, we examine these five factors in an integrated PMT model to understand what predicts individuals' security intentions for home computer use.

### 2.1. *Threat appraisals and online safety behaviors*

Grounded in PMT, threat appraisals have been found to predict online safety protections. However, past research identifying the effects of threat appraisals on protective behavioral intentions provided a set of mixed findings. In some studies, threat severity was an important predictor to security-related protection (e.g., Zahedi et al., 2015), while some studies found that perceived threat severity is not a significant predictor of the intention to implement virus protections (LaRose et al., 2007; Lee et al., 2008). Threat related variables were even further extended in recent security research by either adding a fear appeal variable (e.g., Boss et al., 2015) or integrating more variables to measure threat appraisal (e.g., Johnston et al., 2015). To examine the effect of threat appraisal, threat severity was included in this study on the premise that a generic overview of Internet use engenders threats of varying levels of severity and subsequently more rigorous attention to protections that incur significant response costs. Furthermore, threat levels were found to be positively related to the intention to adopt email security services (Herath et al., 2012). Additionally, perceived threat, influenced by threat severity and susceptibility, also

predicted the intention to use protective software (Liang and Xue, 2010). Therefore, we hypothesize:

H1. *Threat severity will positively predict security intentions.*

H2. *Threat susceptibility will positively predict security intentions.*

Prior experience (with virus infections, in this case) was not included in the original PMT model (Rogers, 1975). Although Rogers (1983) has suggested adding this variable into the PMT model, few studies have incorporated it. In a survey of college students, prior experience with virus infections significantly predicted intentions to use virus protection (Lee et al., 2008). In our study, prior experience deals with an individual's previous experience in dealing with online threats; thus, it is incorporated as part of threat appraisals. We hypothesize:

H3. *Prior experience with online safety hazards will positively predict security intentions.*

### 2.2. Coping appraisals and online safety behaviors

Past studies using college student samples found that coping self-efficacy and response efficacy (facets of coping appraisals) were positively related to online safety behaviors (LaRose et al., 2007; Lee et al., 2008) and security-related software or policy adoption (Herath and Rao, 2009; Ifinedo, 2012; Lee and Larsen, 2009). Other studies also found that self-efficacy could directly or indirectly reduce intentions to open commercial email messages or attachments (Chen et al., 2011; Ng et al., 2009). Additionally, response efficacy was positively related to adoption of email authentication (Herath et al., 2012). Response efficacy and coping self-efficacy were both positive predictors of intentions to adopt spyware protection (Johnston and Warkentin, 2010) and fake-website detectors (Zahedi et al., 2015). We hypothesize:

H4. *Coping self-efficacy will positively predict security intentions.*

H5. *Response efficacy will positively predict security intentions.*

In another study, Lai et al. (2012) found that coping self-efficacy, along with social influence (subjective norms in the current study) and perceived effectiveness of using computer security software (response efficacy), predicted use of security protections for identity theft. Social influence refers to the influence of one's social network (such as family and friends) on one's behaviors (Lai et al., 2012). The concept was adapted from the unified theory of acceptance and use of technology (UTAUT) theory (Venkatesh et al., 2003), which is related to technology acceptance. Subjective norms refer to the influence of one's significant others and it has been found critical to many behaviors, including technology acceptance and others (e.g., Ajzen, 1991; Davis et al., 1989). Compared to subjective norms, social influence focuses more on the influence of people in general. Another commonly used norm, social norm, actually was used as a subjective norm in some studies (e.g., Johnston and Warkentin, 2010), can also be an important predictor to security-related behaviors. Actually, social norm and subjective norm have been used to refer to the same concept in some studies (e.g., Johnston and Warkentin, 2010). Another kind of norm, descriptive norm, refers to significant others' own attitudes or actions toward the behavior (Rivis and Sheeran, 2003). Since the online safety behaviors can be counted as a planned behavior, following the theory of planning behavior (Ajzen, 1991), in this study, we integrated the subjective norms rather than the other two (social influence and descriptive norm) into the PMT model and hypothesize:

H6. *Subjective norms will positively predict security intentions.*

Coping self-efficacy, response efficacy (safeguard effectiveness), and response costs (safeguard cost) all predicted intentions to use anti-virus software (Liang and Xue, 2010). In this study, we argue that Internet users would express greater security intentions when they believe they should perform security protections, thus indicating perceptions of subjective norms, as well as when they consider the costs of performing protective behaviors to be low (response costs). Therefore, we hypothesize:

H7. *Response costs will negatively predict security intentions.*

LaRose et al. (2007) found that two new factors – safety habits and personal responsibility – also predicted safety protection intentions. Safety habits are defined as forms "of automaticity in responding that develops as people repeat actions in stable circumstances" (Verplanken and Wood, 2006, p. 91). Compared to past behaviors, habit strength emphasizes the "automaticity" of the behaviors (please see Ouellette and Wood, 1998 for more discussions on habit strength). We argue that the stronger an individual's habit to perform protective actions, the greater his or her intentions to enact online safety protective actions. Habit has been found a critical factor for people to use a technology or service (Bruijin and Pute, 2009; LaRose and Eastin, 2004). A previous study found that habits of obeying information security policies affected both threat and coping appraisals for employees in conforming to security policies (Vance et al., 2012). Therefore, we hypothesize:

H8. *Safety habit strength will positively predict security intentions.*

Personal responsibility is defined as the belief that one must take actions to achieve a desired outcome (LaRose and Rifon, 2006). LaRose and colleagues found that higher perceptions of personal responsibility for online safety were associated with greater likelihood of performing protective actions (LaRose and Rifon, 2006; LaRose et al., 2007). Therefore, we hypothesize:

H9. *Personal responsibility will positively predict security intentions.*

Self-efficacy, at times, has been conceptualized in reference to an individual's ability to utilize external resources of support to help with enacting protective behaviors (e.g., "I would use the Internet if I could call somebody for assistance") (Luarn and Lin, 2005; Yu, 2012). In the current study, we refer to this concept as perceived security support since it is not truly a self-efficacy measure reflecting personal capabilities, yet one that contributes to an individual's perception of his/her ability to perform protective behaviors. While personal responsibility is

important, knowing that you can acquire support from others when and if you need to take protective behaviors positively predicted security intentions (Liang and Xue, 2010; Luarn and Lin, 2005). Based on this, we hypothesize:

H10. *Perceived security support will positively predict to security intentions.*

## 3. Method

A survey was conducted via Amazon's Mechanical Turk (MTurk; http://www.mturk.com), a large online crowdsourcing workforce that recruits individuals for a variety of tasks. Some studies have reported that respondents on MTurk were more representative of the U.S. population (Berinsky et al., 2012) and were more diversified than other convenience samples or college-student samples (Buhrmester et al., 2011). The value of this data collection method has been recommended by prior research (Goodman et al., 2012; Mason and Suri, 2012).

### 3.1. Procedure

We posted a Human Intelligence Task (HIT) in October 2013 with a request for 1000 U.S. MTurk workers to participate in a study about how people use the Internet and protect themselves online. For the purpose of this particular study, we limited access to the HIT to MTurk workers with a HIT approval rate of 90% or above. MTurk workers' HIT approval rates are determined by their total assignments approved and submitted. The choice of 90% HIT approval rate was arbitrary yet in line with previous studies (e.g., Carr, 2014; Gould et al., 2015), and was set to ensure better quality performance on our online survey as the approval rate signifies professionalism. To further ensure to the response quality of the online survey, we used a quality control question, also called "*honey pots*", where we asked participants to select an obvious answer ("neither agree nor disagree") as their response to one statement to detect if they carelessly rushed through the questions and did not pay attention to the task (Alonso and Baeza-Yates, 2011; Barger et al., 2011). This question was embedded in the survey amidst other survey items. As a result, 19 responses that failed the quality control question were removed from the total sample of 1007 responses, yielding a clean sample of 988.

The study has been approved by the university's institutional review board (IRB). Before answering the online survey, respondents were asked to read a consent form that provided a description of the study and probed participants to think about online safety by stating "We would like to know how you keep yourself safe online while using your home computer, smartphone or tablet." The consent form was used to ensure the voluntary nature of participation. The information about how the data will be used and reported, the aggregation in relation to anonymity of personally-identifiable information, and the contact information of the primary investigator were all provided in the consent form. Respondents could decide whether they agree or disagree to participate in the survey. They could also leave the survey at any time. Participants were given a post-incentive of 76 cents after completing the survey.

### 3.2. Participants

Among the 988 respondents, 45.3% were female, with a mean age of 32 (*SD* = 11.26; *Median* = 29 years old; *Range* = 18–80 years old), and an average of 15 years of post-kindergarten education. Most participants were Caucasians (75.6%), followed by Asians (7.8%), African Americans (5.8%), and Hispanics or Latinos (5.7%). The median household income ranged between $25,000 and $49,999. Our participants were comparable to the U.S. Internet population (File, 2013) in terms of: gender, where 49% of U.S. Internet users were female ($\chi^2 = 0.65$, *ns*); race, where 83% of Internet users were Caucasians ($\chi^2 = 1.67$, *ns*), and age, where the median age of Internet users was between 18 and 34.

### 3.3. Operational measures

Except as noted, all items were measured on a five-point Likert-type scale, ranging from strongly agree (coded as 5) to strongly disagree (1) with a neutral midpoint (3). Table 1 includes items used to measure each construct. While security intentions are displayed first in the table (in accordance with the order of hypotheses), it was measured last in the actual survey. Participants, upon consenting to participate in the study, were asked questions related to threat severity, threat susceptibility, response costs, coping self-efficacy, prior experience with safety hazards, perceived security support, subjective norms, personal responsibility, habit strength, security intentions, and demographics, respectively. Within each construct, items were presented at random order.

**Online security intentions.** To measure online security intentions, we adapted two items used by Liang and Xue (2010) focusing on avoidance behavior and reformulated them as intentions. For example, Liang and Xue (2010) asked participants to rate the statements "I update my anti-spyware software regularly" and "I run anti-spyware software regularly to remove spyware from my computer." In our survey we asked participants to rate the statements "I will update my protective software regularly" and "I will run protective software regularly to remove spyware from my computer" to indicate intentions for future protective behaviors. Additionally, we adapted one item from Anderson and Agarwal (2010): "I am likely to take security measures to protect the Internet" and created five additional items: "I will upgrade my security measures to protect myself better online;" "I will change my passwords more often;" "I will use passwords that are harder to guess;" "I will change my browser security settings to a higher level;" and "I will learn how to be more secure online."

**Threat severity.** To measure threat severity, we asked participants to report how harmful malware would be under several conditions. We adapted three items from Liang and Xue (2010) by shortening the sentences and using the term "malware" instead of "spyware" and provided the definition of the jargon. We use malware because malware has a broader definition including spyware, viruses, Trojans, key loggers, and rogue security software. We also created four new items, including "[Malware] shuts down my computer and demands payment to reactivate it," "[Malware] reveals my passwords to online criminals," "[Malware] reveals my social security number," and "[Malware] reveals my credit card information."

**Table 1 – Operational measures.**

| Measure | Items | M (SD) | α |
|---|---|---|---|
| Security intentions<br>Adapted from Anderson and Agarwal (2010), Liang and Xue (2010), with 6 new items | Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect yourself online. These questions still refer to the home computer or other device you would feel safe to use for online financial transactions.<br>1. I am likely to take security measures to protect the Internet<br>2. I will upgrade my security measures to protect myself better online<br>3. I will change my passwords more often<br>4. I will use passwords that are harder to guess<br>5. I will change my browser security settings to a higher level<br>6. I will learn how to be more secure online<br>7. I will run protective software regularly to remove spyware from my computer.<br>8. I will update my protective software regularly | 3.99 (.74) | .90 |
| Threat severity<br>Adapted from Liang & Xue (2010), with 4 new items | Malware is a general term that refers to computer programs that invade your computer, tablet or cell phone as you use email or the Internet.<br>They include spyware that collects and transmits your personal information without your knowledge, viruses and trojans that can take over your devices or disrupt their operation, key loggers that record what you type, and rogue security software that offers free security scans but are really invasive programs.<br>Cookies are files that are deposited on your computer by the websites to track your visits to your favorite websites but that can compromise personal information that they store.<br>The following are some of the threats to your online safety that malware can cause. Please rate how harmful they would be if they happened to you by clicking an answer in each row.<br>How harmful to you would malware be if…<br>1. The information is used to commit crimes against me<br>2. It makes my computer run more slowly<br>3. It causes a system crash from time to time<br>4. It shuts down my computer and demands payment to reactivate it<br>5. It reveals my passwords to online criminals<br>6. It reveals my social security number<br>7. It reveals my credit card information | 4.55 (.39) | .79 |
| Threat susceptibility<br>Adapted from Liang and Xue (2010) | Thinking about the home computer or other device you would feel safe to use for online financial transactions, please tell us how much you agree or disagree with each statement.<br>1. It is extremely likely that my computer will be infected by malware in the future<br>2. My chances of getting malware are great<br>3. There is a good possibility that my computer will have malware | 2.57 (1.00) | .87 |
| Prior experience with safety hazards | Have you ever experienced the following on your primary computer?<br>1. It slowed down or is not running as fast as it used to<br>2. Virus attack from opening a link or an attachment in a fraudulent email (called "phishing")<br>3. Virus attack from just visiting a web site<br>4. New icons or programs appeared out of nowhere<br>5. A message popped up offering a free computer security scan<br>6. Had important personal information stolen, such as your Social Security Number or credit card number<br>7. Been the victim of an online scam and lost money | 2.60 (1.62) | |
| Coping self-efficacy<br>Adapted from Anderson and Agarwal (2010), and 2 new items | 1. I feel comfortable taking measures to secure my primary home computer<br>2. Taking the necessary security measures is entirely under my control<br>3. I have the resources and the knowledge to take necessary security measures<br>4. Taking necessary security measures is easy<br>5. [Reversed] I feel nervous when I think about online security issues<br>6. In general, I am safe from online threats in my home | 4.00 (.67) | .82 |
| Response efficacy<br>Adapted from Liang and Xue (2010) | 1. Protective software would be useful for detecting and removing malware<br>2. Protective software would increase my performance in protecting myself from malware<br>3. Protective software would enable me to search and remove malware faster | 4.30 (.65) | .86 |

(*continued on next page*)

**Table 1 – (*continued*)**

| Measure | Items | M (SD) | α |
|---|---|---|---|
| Subjective norm<br>Adapted from Anderson and Agarwal (2010) | 1. Friends who influence my behavior would think that I should take measures to secure myself online<br>2. Significant others who are important to me would think that I should take measures to secure myself online<br>3. My peers would think that I should take measures to help secure the Internet | 3.66 (.95) | .87 |
| Response costs<br>Adapted from Liang and Xue (2010) | 1. I don't know how to get security protections<br>2. Security protections may cause problems to other programs on my computer<br>3. Using security protections is too much trouble | 2.06 (.75) | .58 |
| Habit strength<br>Adapted from Venkatesh et al. (2012), and three new items | 1. The use of security protections has become a habit for me<br>2. Using security protections has become natural to me<br>3. Online security protection is something I do automatically<br>4. Online protection is something I do without thinking<br>5. Online safety protection is part of my regular routine | 4.07 (.87) | .95 |
| Personal responsibility<br>Adapted from Anderson and Agarwal (2010) | 1. If I adopt security measures I can make a difference in helping to secure the Internet<br>2. [Reversed]The efforts of one person are useless in helping secure the Internet<br>3. Every person can make a difference when it comes to helping to secure the Internet | 3.81 (.81) | .75 |
| Perceived security support<br>Adapted from Liang and Xue (2010) | 1. I could install and use protective software even if there was no one around to tell me what to do<br>2. I could install and use protective software even if I had never used a package like it before<br>3. I could install and use protective software if I could call someone for help if I got stuck<br>4. I could install and use protective software if someone showed me how to do it first | 4.18 (.68) | .69 |
| Education | Not including kindergarten, how many years of formal education have you completed? | | |
| Income | What was your annual household income in 2012 from all sources, before taxes?<br>1. Under $10,000<br>2. From $10,000 to less than $25,000<br>3. From $25,000 to less than $50,000<br>4. From $50,000 to less than $75,000<br>5. From $75,000 to less than $100,000<br>6. From $100,000 to less than $125,000<br>7. $125,000 or over | | |

**Threat Susceptibility.** To measure threat susceptibility, we adapted three items from Liang and Xue (2010) by changing the word "spyware" to "malware." These items included "It is extremely likely that my computer will be infected by malware in the future;" "My chances of getting malware are great;" and "There is a good possibility that my computer will have malware."

**Prior Experience with Safety Hazards.** We created seven items to measure whether people have prior experiences with their primary computer. One example is "[I have experienced] virus attack from just visiting a web site."

**Coping Self-efficacy.** To measure coping self-efficacy, we used four items from Anderson and Agarwal's (2010) scale of security behavior self-efficacy, and created two new items: "I feel nervous when I think about online security issues" and "In general, I am safe from online threats in my home."

**Response Efficacy.** We adapted three items from Liang and Xue's (2010) scale of perceived safeguard effectiveness by changing the jargon "anti-spyware software" to a general term "protective software" in order to make it understandable to layperson.

**Subjective Norm.** We adapted three items from Anderson and Agarwal (2010) and focused on Internet security rather than home computer security. For example, Anderson and Agarwal (2010) asked participants to rate the statements: "Friends who influence my behavior would think that I should take measures to secure my primary home computer;" "Significant others who are important to me would think that I should take measures to secure my primary home computer," and "My peers would think that I should take security measures on my primary home computer to help secure the Internet." We changed them to "Friends who influence my behavior would think that I should take measures to secure myself online; "Significant others who are important to me would think that I should take measures to secure myself online;" and "My peers would think that I should take measures to help secure the Internet."

**Response Costs.** We adapted three items from Liang and Xue (2010)'s scale of perceived safeguard cost by changing "anti-spyware" to "security protections". One example of this measure is "I don't know how to get security protections."

**Habit Strength.** We adapted two items from Venkatesh et al. (2012) by changing the focus on the habit of mobile Internet to the habit of security protections. We also created three new items: "Online security protection is something I do automatically;" "Online protection is something I do without thinking;" and "Online safety protection is part of my regular routine."

**Personal Responsibility.** Three personal responsibility items were adapted from Anderson and Agarwal (2010)'s scale of perceived citizen efficacy by changing the focus of home computer to security measures. One example is "If I adopt security measures I can make a difference in helping to secure the Internet."

**Perceived Security Support.** Four items were adapted from Liang and Xue (2010)'s scale of self-efficacy that is used to measure the support from others. One example is "I could install and use protective software if I could call someone for help if I got stuck."

#### 3.3.1. *Criterion variable*

Security intentions, the criterion, was measured using eight items that asked participants about the likelihood of taking measures to protect themselves online and enhance Internet safety, adapted from Liang and Xue (2010). We grouped predictor variables into threat appraisals and coping appraisals. They are briefly described below.

#### 3.3.2. *Threat appraisals*

Threat appraisals included assessments of threat severity, threat susceptibility, and prior experience with safety hazards. Threat severity, measured with seven items, asked participants to rate how harmful threats of computer and Internet malware could be to their online safety (5 = extremely harmful; 1 = not at all harmful). Threat susceptibility was measured with three items related to assessing the likelihood of experiencing online safety threats. Prior experience with safety hazards was measured using seven yes/no questions asking participants about their experiences with online safety threats. Answers were dichotomized (1 = yes; 0 = no) and aggregated into a single variable.

#### 3.3.3. *Coping appraisals*

Coping appraisals included coping self-efficacy, response efficacy, subjective norms, response costs, safety habit strength, personal responsibility, and perceived security support. Coping self-efficacy was measured with six items related to perceived capability and comfort with regard to performing online protective behaviors. Response efficacy included three items and asked participants to assess the effectiveness of performing protective behaviors. Subjective norms were measured with three items that asked participants to indicate whether they thought their close friends, significant others, and peers think they should take measures to protect themselves online. Response costs, measured with three items, dealt with the consequences and costs of performing protective behaviors. Habit strength included five items and asked participants to indicate whether taking protective actions online was habitual for them. Personal responsibility was assessed with three items related to participants' perceptions about their own responsibility toward keeping the Internet safe. Finally, perceived security support was measured with four items dealing with participants' perceptions about whether they required help from others to install protective software on their computers.

#### 3.3.4. *Control variables*

Participants also answered demographic questions related to gender (1 = female, 0 = male), race (1 = Caucasian, 0 = non-Caucasian), education (years of education excluding kindergarten), age (birth year), and household income. Demographic variables were included as covariates in subsequent statistical analyses.

## 4. Results

Table 2 provides the correlation matrix for all predictor, covariate, and criterion variables. Findings showed that race, education, income level, and threat susceptibility were not significantly correlated with security intentions. The other predictor variables (gender, age, threat severity, prior experience, coping self-efficacy, response efficacy, perceived security support, subjective norms, personal responsibility, security habit strength, and response costs) were significantly correlated with security intentions. The strongest correlation with security intentions was with security habit strength ($r = .53$), while the weakest correlation was with gender ($r = .07$).

Hypotheses 1 through 10 predicted that threat severity (H1), threat susceptibility (H2), prior experience (H3), coping self-efficacy (H4), response efficacy (H5), subjective norms (H6), response costs (H7), safety habit strength (H8), personal responsibility (H9), and perceived security support (H10) would significantly predict security intentions. To test these hypotheses, we conducted a 15-predictor regression model (10 predictors and five demographic variables) with security intentions as the criterion (see Table 3). The risk for multicollinearity was assessed through tolerance (*Range* = .50–.96) and VIF (*Range* = 1.04–1.09) scores, which confirmed low multicollinearity risk.

Hierarchical regression analysis was performed with the five major PMT predictors in the first model. Prior experience with safety hazards and four new coping variables (perceived security support, personal responsibility, subjective norm, and habit strength) were incorporated into the second model. Demographic variables were added into the third model to examine the effect of demographic factors on security intentions. Model 1 was significant and explained 29% of the variance in security intentions, $F\ (5, 976) = 79.59$, $p < .001$, *adjusted* $R^2 = .29$. Model 2 increased the variance explained in security intentions by 15% for a total variance of 43%, $F\ (10, 971) = 75.83$, $p < .001$; *adjusted* $R^2 = .433$, $R^2$ change = .15 ($p < .001$). The strongest predictor of security intentions was security habit strength, followed by response efficacy, and personal responsibility. For the third model, none of the demographic variables were significant, $F\ (15, 966) = 50.82$, $p < .001$, $R^2 = .441$, *adjusted* $R^2 = .432$, $R^2$ change = .003 (*n.s.*).

Table 4 and Fig. 1 summarize the results pertaining to testing the 10 hypotheses based on the third model. While threat severity significantly predicted security intentions ($\beta = -.15$, $p < .001$), H1 could not be supported as the relationship was in the opposite direction. Threat susceptibility did not predict security intentions; thus H2 was not supported. In support of H3, prior experience ($\beta = .03$, $p < .05$) significantly predicted security intentions.

Most of the coping appraisal variables significantly predicted security intentions. While coping self-efficacy ($\beta = -.10$, $p < .01$) was a significant predictor of security intentions, the relationship was in the opposite direction to what we hypothesized, thus H4 was not supported. The following were significant predictors in the hypothesized directions:

**Table 2 – Pearson product-moment correlations of independent and dependent variables.**

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Security intentions | | | | | | | | | | | | | | | | |
| 2 | Gender (female = 1) | 0.07* | | | | | | | | | | | | | | | |
| 3 | Race (White = 1) | 0 | −0.03 | | | | | | | | | | | | | | |
| 4 | Age | 0.09** | 0.17** | 0.11** | | | | | | | | | | | | | |
| 5 | Education | −0.04 | 0.06 | −0.04 | 0.03 | | | | | | | | | | | | |
| 6 | Income | 0.01 | 0.01 | .06 | .09** | 0.20** | | | | | | | | | | | |
| 7 | Threat severity | 0.26** | 0.20** | −0.01 | 0.11** | 0.04 | −0.01 | | | | | | | | | | |
| 8 | Threat susceptibility | −.04 | .08* | −0.06 | 0.20** | −0.01 | 0.02 | 0.05 | | | | | | | | | |
| 9 | Prior experience with safety hazards | 0.11** | 0.02 | −0.04 | 0.12** | 0.01 | −0.02 | 0.14** | 0.35** | | | | | | | | |
| 10 | Coping self-efficacy | 0.26** | −0.19** | 0.04 | −0.13** | −0.02 | −0.03 | 0.12** | −0.44** | −0.16** | | | | | | | |
| 11 | Response efficacy | 0.46** | −0.01 | 0.06 | 0.01 | −0.03 | −0.02 | 0.21** | −0.02 | 0.15** | 0.31** | | | | | | |
| 12 | Subjective norm | 0.28** | 0.11** | 0.03 | 0.10** | −0.03 | 0.01 | 0.16** | 0.15** | 0.11** | −0.01 | 0.23** | | | | | |
| 13 | Response costs | −0.35** | 0.05 | −0.04 | −0.02 | −0.02 | −0.04 | −0.11** | 0.37** | 0.11** | −0.50** | −0.34** | −0.07** | | | | |
| 14 | Security habit strength | 0.53** | −0.06 | 0.02 | 0.06 | 0 | 0 | 0.16** | −0.26** | −0.05 | 0.58** | 0.44** | 0.13** | −0.49** | | | |
| 15 | Personal responsibility | 0.43** | 0.05 | 0.04 | 0.15** | −0.01 | 0.02 | 0.20** | −0.06 | .07* | 0.24** | 0.39** | 0.27** | −0.26** | 0.35** | | |
| 16 | Perceived security support | 0.26** | −0.11** | 0.08* | −0.08* | 0.06 | 0.04 | 0.11** | −0.14** | 0.03 | 0.35** | 0.51** | 0.19** | −0.28** | 0.38** | 0.25** | |

*Notes.* *$p < .05$, **$p < .01$.

response costs (β = –0.11, $p < .001$), coping self-efficacy (β = –0.10, $p < .01$), response efficacy (β = 0.21, $p < .001$), subjective norms (β = 0.08, $p < .001$), security habit strength (β = 0.33, $p < .001$), and personal responsibility (β = 0.16, $p < .001$). Therefore, H5-9 were supported. Finally, perceived security support was not a significant predictor of security intentions (β = –.06, *ns*). H10 was not supported.

## 5. Discussion

This study has practical and theoretical contributions. Practically, the current study furthers our understanding of how individuals seek to protect themselves online. The results can be utilized by the governments and individuals to improve online safety. Theoretically, the integration of concepts drawn from previous online safety research within the extended PMT paradigm proposed here provides additional insights and avenues for future research. Specifically, by adding new coping appraisal variables and prior experiences, the total variance of security intentions was increased by 15%. Safety habit strength, response efficacy, personal responsibility, and subjective norms could all predict security intentions.

Our findings show that for threat appraisals, it is the severity of online threats that predicted security intentions, not the susceptibility to threats, which is different from Ifinedo's (2012) findings. The discrepancy might result from the differences in organizational and home contexts, as pointed out in previous studies (Dang-Pham and Pittayachawan, 2015; Li and Siponen, 2011). As for coping appraisals, the newly proposed coping appraisal resources from the extended PMT model predicted security intentions. Consistent with LaRose et al. (2007), the strongest predictor of security intentions was online security habit strength. Response efficacy and personal responsibility for online safety were also significant predictors. The perception of social support for taking precautions, a variable introduced from recent online safety research, was not a significant predictor. However, the correlation between security support and security intentions was significant ($r = .26$, $p < .01$). Among the coping appraisal variables, response costs, coping self-efficacy, and perceived security support were negative predictors of safety intentions, and response efficacy was a positive predictor. When people think that protective software could be useful for detecting malware, they have higher intentions to use them.

Counter to PMT, threat severity, coping self-efficacy, and perceived security support were negative predictors in the regression analysis. However, we observed positive zero-order correlation between threat severity and security intentions ($r = .26$, $p < .01$), coping self-efficacy and security intentions ($r = .26$, $p < .01$), and perceived security support and security intentions ($r = .26$, $p < .01$). Although the multicollinearity risk was low, there is still a possibility of statistical suppression resulting from the other variables entered into the analysis (Table 3). The first plausible explanation is that people who know more about online security could be more aware of the severity of threats, while they also have higher coping self-efficacy and perceived security support. These people might have lower future intentions to take security measures because they have enough confidence to protect themselves online. Another

**Table 3 – Regression of PMT variables on security intentions.**

| Model | Variable | B | S.E. | Beta | t | |
|---|---|---|---|---|---|---|
| 1 | (Constant) | 2.84 | 0.25 | | 11.19 | *** |
| | Threat severity | –0.25 | 0.04 | –0.16 | –5.82 | *** |
| | Threat susceptibility | 0.04 | 0.02 | 0.06 | 1.89 | |
| | Response costs | –0.21 | 0.03 | –0.21 | –6.49 | *** |
| | Coping self-efficacy | 0.06 | 0.04 | 0.05 | 1.58 | |
| | Response efficacy | 0.38 | 0.03 | 0.34 | 11.21 | *** |
| 2 | (Constant) | 1.86 | 0.24 | | 7.67 | *** |
| | Threat severity | –0.16 | 0.04 | –0.10 | –3.99 | *** |
| | Threat susceptibility | 0.02 | 0.02 | 0.02 | 0.74 | |
| | Response costs | –0.11 | 0.03 | –0.11 | –3.67 | *** |
| | Coping self-efficacy | –0.10 | 0.04 | –0.10 | –2.89 | ** |
| | Response efficacy | 0.22 | 0.04 | 0.19 | 6.13 | *** |
| | Perceived security support | –0.06 | 0.03 | –0.06 | –2.05 | * |
| | Subjective norms | 0.09 | 0.02 | 0.11 | 4.35 | *** |
| | Personal responsibility | 0.16 | 0.03 | 0.17 | 6.24 | *** |
| | Safety habit strength | 0.33 | 0.03 | 0.39 | 12.01 | *** |
| | Prior experience with safety hazards | 0.03 | 0.01 | 0.06 | 2.28 | * |
| 3 | (Constant) | 1.97 | 0.28 | | 6.97 | *** |
| | Threat severity | –0.15 | 0.04 | –0.10 | –3.67 | *** |
| | Threat susceptibility | 0.02 | 0.02 | 0.02 | 0.79 | |
| | Response costs | –0.11 | 0.03 | –0.11 | –3.69 | *** |
| | Coping self-efficacy | –0.10 | 0.04 | –0.09 | –2.67 | ** |
| | Response efficacy | 0.21 | 0.04 | 0.19 | 5.99 | *** |
| | Perceived security support | –0.06 | 0.03 | –0.05 | –1.76 | |
| | Subjective norms | 0.08 | 0.02 | 0.11 | 4.19 | *** |
| | Personal responsibility | 0.16 | 0.03 | 0.17 | 6.18 | *** |
| | Safety habit strength | 0.33 | 0.03 | 0.39 | 11.91 | *** |
| | Prior experience with safety hazards | 0.03 | 0.01 | 0.06 | 2.34 | * |
| | Gender (female = 1) | 0.06 | 0.04 | 0.04 | 1.50 | |
| | Race (Caucasian = 1) | –0.04 | 0.05 | –0.02 | –0.78 | |
| | Age | 0.00 | 0.00 | –0.01 | –0.46 | |
| | Income | 0.00 | 0.01 | 0.00 | 0.17 | |
| | Education | –0.01 | 0.01 | –0.03 | –1.26 | |

*Notes.* $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.
Model 1: $F$ (5, 976) = 79.59, $p < .001$, $R^2 = .29$, and the adjusted $R^2 = .29$.
Model 2: $F$ (10, 971) = 75.83, $p < .001$; $R^2 = .439$; *adjusted* $R^2 = .43$, $R^2$ change = .15 ($p < .001$).
Model 3: $F$ (15, 966) = 50.82, $p < .001$, $R^2 = .441$, the adjusted $R^2 = .432$, and the $R^2$ change = .003 (*n.s.*).

plausible explanation for this pattern of results could be that individuals with high levels of self-efficacy and perceived security support are already enacting protective behaviors on a regular basis, especially that unlike a health concern (e.g., getting vaccinated), dealing with online security coincides with habitual use of computers and the Internet.

**Table 4 – Summary of hypothesis tests.**

| H | Predictors | Security Intentions |
|---|---|---|
| 1 | Threat severity | Not supported (opposite direction) |
| 2 | Threat susceptibility | Not supported (*n.s.*) |
| 3 | Prior experience with safety hazards | Supported |
| 4 | Coping self-efficacy | Not supported (opposite direction) |
| 5 | Response efficacy | Supported |
| 6 | Subjective norms | Supported |
| 7 | Response costs | Supported |
| 8 | Safety habit strength | Supported |
| 9 | Personal responsibility | Supported |
| 10 | Perceived security support | Not supported (*n.s.*) |

*Notes. ns* = Not significant at .05 level.

By conducting a cross-sectional survey of Amazon MTurk users, this study examined how classical and new PMT factors predicted security intentions. Overall, we found that among the existing PMT variables, response efficacy was the most stable predictor than the threat appraisals and other coping appraisals. As mentioned above, the negative relationship of security intention and threat severity, and that of security intention and coping self-efficacy may indicate the complexity of human cognition and the need for adding other variables into the PMT model. Specifically, based on our findings, we found that it is important to consider an individual's security habit strength, response efficacy, personal responsibility, and subjective norms. In other words, being aware of the threats is not enough. It is how one copes with the threats matters. An individual has to be aware that he or she should be responsible for his/her online security, so he/she will be motivated to take security protection behaviors. This can be achieved by taking use of the normative belief or forming a habitual protection behavior.

To summarize our findings, we found that none of the sociodemographic variables significantly predicted security intentions

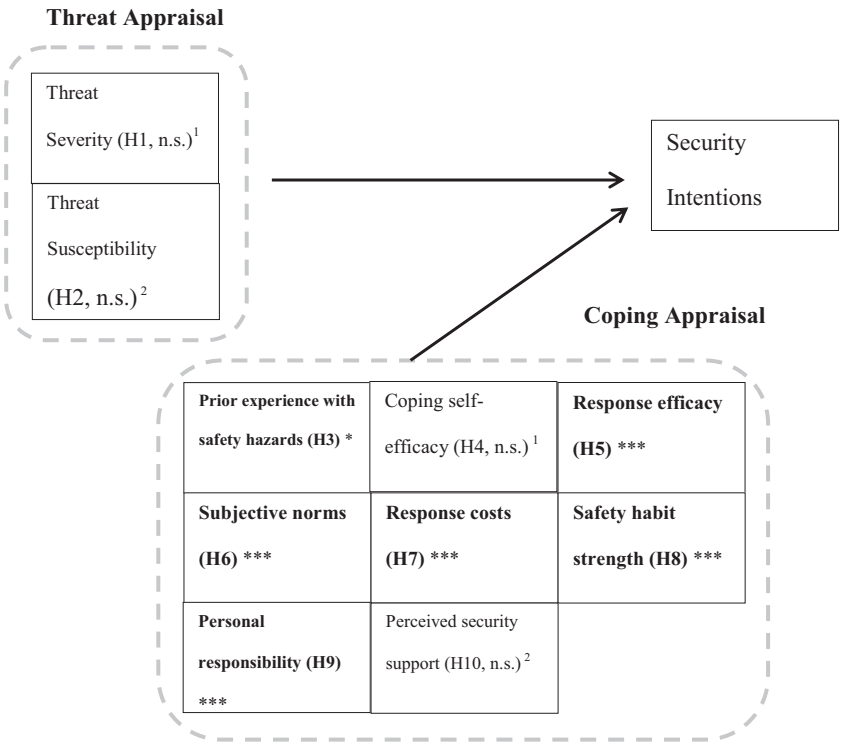


**Fig. 1 – Results of hypothesis tests.**
Note. [1] n.s.: not supported (significant, opposite direction).
[2] n.s.: not supported (Not significant at .05 level).
*$p < .05$, **$p < .01$, ***$p < .001$.
$F$ (15, 966) = 50.82, $p < .001$, $R^2 = .441$, the adjusted $R^2 = .432$.

(see Table 4). Instead, coping appraisals (e.g. safety habit strength, response efficacy, and personal responsibility) were the most important predictors. This indicates the importance of cognitive processes in security protection. Most coping appraisals were significant predictors of security intentions. Specifically, habit strength is the strongest predictor. Therefore, to increase Internet users' security intentions, in addition to revealing the severity of online threats, it will be important to help them know the efficacy of taking security actions and realize their responsibility of protecting themselves online. The government may also encourage or force the computer or software providers to develop some programs or messages that can remind users to take certain protection behaviors and help them form the habits of taking security protections.

### 5.1. *Limitations and future research*

Cross-sectional surveys such as the present one do not conclusively establish causality. Although the sample used in the present study was broadly diverse in representing the U.S. online population, it was skewed toward young adults with high education levels compared to the general population. Future research should explore the relationships conceptualized in our study with randomly-selected representative samples of the U.S. population as well as populations from other countries (Belanger and Crossler, 2011). Examining the actual security behaviors instead of security intentions can also extend our understanding of security protection behaviors (Boss et al., 2015).

Further exploration of threat appraisal and coping appraisal variables is required to establish the factors that cause online safety behaviors. As suggested in Boss et al. (2015), fear appeal can be integrated into the PMT model. Johnston et al. (2015) also provided a more elaborated model for the threat appraisal. Since this study has tested the relationship among many variables and security intention, for the concern of parsimony, we did not include more variables with regard to threat appraisal. Future studies can further examine the complexity of threat appraisal. In addition, as mentioned earlier, there are several types of "norms." In this study, subjective norm was adopted. Future studies can explore other norms, such as descriptive norm (Rivis and Sheeran, 2003) and compare the importance of different kinds of norms on security intention.

In addition, individual differences (such as personality, as mentioned in Rogers, 1983 and Shropshire et al., 2015) and the differences on security tools (Zahedi et al., 2015) might need to be considered. In the online safety domain, experimental manipulations of coping variables are desirable to identify consumer education interventions that can motivate the development of online safety habits that, on the basis of the current results, appear to be the best defense against online threats. Generally, habits are strengthened by repetition of behaviors during their trial phase in the presence of a consistent context containing stimulus cues that subsequently trigger the habitual behavior (LaRose, 2010). Thus, online safety precautions that require continuing user vigilance (e.g., detection of

phishing scams) would be better inculcated through repetition than through offering "safety tips" to consumers or providing automated software that requires no user action. Security software might instead offer warnings that prompt appropriate user actions. Future experimental research should determine and untangle the relationships among coping resources to understand the paradoxical negative relationship between coping self-efficacy and security intentions uncovered in the present study.

Finally, this study examined how the existing PMT variables and new coping appraisal variables predicted one's security intention. For future studies that aim to extend the PMT, based on the findings of this research, it will be important to add more coping appraisal variables into the PMT model. Specifically, safety habit strength, response efficacy, and personal responsibility have been found to be strong predictors to security intention. It may help to consider the subjective norms at the same time.

## REFERENCES


Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50:179–211.

Alonso O, Baeza-Yates R. Design and implementation of relevance assessments using crowdsourcing. In: Advances in information retrieval. Springer; 2011. p. 153–64, <http://link.springer.com/chapter/10.1007/978-3-642-20161-5_16>.

Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q 2010;34(3):613–43. doi:10.1016/j.chb.2004.12.002.

AV Comparatives. IT Security survey 2013, <http://www.av-comparatives.org/images/docs/security_survey2013_en.pdf>; 2013 [accessed 16.03.16].

Barger P, Behrend TS, Sharek DJ, Sinar EF. IO and the crowd: frequently asked questions about using Mechanical Turk for research. TIP 2011;49(2):11–17.

Belanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Q 2011;36(4):1017–41.

Berinsky AJ, Huber GA, Lenz GS. Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. Polit Anal 2012;20:351–68.

Boss SR, Galletta DF, Moody GD, Lowry PB, Polak P. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. MIS Q 2015;39(4):837–64.

Bruijin G, Pute B. Adolescent soft drink consumption, television viewing and habit strength: investigating clustering effects in the theory of planned behavior. Appetite 2009;53:66–75.

Buhrmester M, Kwang T, Gosling SD. Amazon's Mechanical Turk: a new source of inexpensive, yet high-quality, data? Perspectives on Psychological Science 2011;6:3–5.

Carr A. An exploration of Mechanical Turk as a feasible recruitment platform for cancer survivors [undergraduate honors thesis]. University of Colorado Boulder; 2014. Paper 59.

Chen R, Wang J, Herath T, Rao HR. An investigation of email processing from a risky decision making perspective. Decision Support Systems 2011;52(1):73–81. doi:10.1016/j.dss.2011.05.005.

Conner M, Armitage CJ. Extending the theory of planned behavior: a review and avenues for further research. J Appl Soc Psychol 1998;28:1429–64.

Culnan MJ, Williams CC. How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS Q 2009;33:673–87.

Cyber Security. 2012 NCSA? McAfee online safety survey. <http://www.staysafeonline.org/download/datasets/3890/2012_ncsa_mcafee_online_safety_study.pdf>; 2012.

Dang-Pham D, Pittayachawan S. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. Comput Secur 2015;48:281–97. doi:10.1016/j.cose.2014.11.002.

Davis FD, Bagozzi RP, Warshaw PR. User acceptance of computer-technology: a comparison of two theoretical models. Manage Sci 1989;35:982–1003. doi:10.1287/mnsc.35.8.982.

File T. Computer and Internet use in the United States. <http://www.census.gov/prod/2013pubs/p20-569.pdf>; 2013.

Fishbein M, Ajzen I. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley; 1975.

Goodman JK, Cryder CE, Cheema A. Data collection in a flat world: the strengths and weaknesses of Mechanical Turk samples. J Behav Decis Mak 2012;213–24.

Gould SJ, Cox AL, Brumby DP. Task lockouts induce crowdworkers to switch to other activities. In: Proceedings of the 33rd annual ACM conference extended abstracts on human factors in computing systems. ACM; 2015. p. 1785–90.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009;18(2):106–25. doi:10.1057/ejis.2009.6.

Herath T, Chen R, Wang J, Banjara K, Wilbur J, Rao HR. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Information Systems Journal 2012;doi:10.1111/j.1365-2575.2012.00420.x.

Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decision Sciences 2012;43(4):615–60.

Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95. doi:10.1016/j.cose.2011.10.007.

Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34(3):549–66.

Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q 2015;39:113–34.

Lai F, Li D, Hsieh C-T. Fighting identity theft: the coping perspective. Decision Support Systems 2012;52(2):353–63. doi:10.1016/j.dss.2011.09.002.

LaRose R. The problem of media habits. Commun Theory 2010;20:194–222.

LaRose R, Eastin M. A social cognitive explanation of Internet uses and gratifications: toward a new theory of media attendance. J Broadcast Electron Media 2004;48(3):358–78.

LaRose R, Rifon NJ. Changing online safety behavior: experiments with online security and privacy. Paper presented to the International Communication Association, Dresden, Germany; 2006.

LaRose R, Rifon NJ, Wirth C. Online safety begins with you and me: getting Internet users to protect themselves. Paper presented at the 57th International Communication Association Conference, San Francisco, CA; 2007.

Lee D, LaRose R, Rifon NJ. Keeping our network safe: a model of online protection behaviour. Behav Inf Technol 2008;27(5):445–54. doi:10.1080/01449290600879344.

Lee Y, Larsen KR. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur J Inf Syst 2009;18(2):177–87.
Li Y, Siponen MT. A call for research on home users' information security behaviour. In: PACIS. 2011. p. 112.
Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inf Syst 2010;11(7):394–413.
Lowry PB, Moody GD. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. Information Systems Journal 2015;25(5):433–63. doi:10.1111/isj.12043.
Luarn P, Lin H-H. Toward an understanding of the behavioral intention to use mobile banking. Comput Human Behav 2005;21(6):873–91. doi:10.1016/j.chb.2004.03.003.
Mason W, Suri S. Conducting behavioral research on Amazon's Mechanical Turk. Behav Res Methods 2012;44:1–23.
Microsoft. Safety is an active verb: 2013 Microsoft Computing Safety Index worldwide report. <http://go.microsoft.com/?linkid=9843175>; 2014.
Ng BY, Kankanhalli A, Xu YC. Studying users' computer security behavior: a health belief perspective. Decision Support Systems 2009;46(4):815–25. doi:10.1016/j.dss.2008.11.010.
Ouellette J, Wood W. Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. Psychol Bull 1998;124(1):54–74.
Posey C, Roberts T, Lowry PB, Bennett B, Courtney J. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q 2013;37(4):1189–210.
Rainie L, Kiesler S, Kang R, Madden M. Anonymity, privacy, and security online. Pew Research Center, <http://pewinternet.org/Reports/2013/Anonymity-online.aspx>; 2013.
Rivis A, Sheeran P. Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis. Curr Psychol 2003;22(3):218–33.
Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol 1975;91(1):93–114. doi:10.1080/00223980.1975.9915803.
Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo J, Petty R, editors. Social psychophysiology: a sourcebook. New York: Guilford Press; 1983. p. 153–77.
Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput Secur 2015;49:177–91. doi:10.1016/j.cose.2015.01.002.
Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 2012;49(3):190–8. doi:10.1016/j.im.2012.04.002.
Vance A, Lowry PB, Eggett D. Using accountability to reduce access policy violations in information systems. JMIS 2013;29(4):263–90.
Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: toward a unified view. MIS Q 2003;27(3):425–78.
Venkatesh V, Thong JY, Xu X. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q 2012;36(1):157–78.
Verplanken B, Wood W. Interventions to break and create consumer habits. J Public Policy Mark 2006;25:90–103.
Waterman S. Cybercrime costs the U.S. economy billions of dollars annually: study. *Washington Times*, <http://www.washingtontimes.com/news/2013/jul/23/cybercrime-costs-us-economy-billions-dollars-annua/>; 2013.
Yu CS. Factors affecting individuals to adopt mobile banking: empirical evidence from the UTAUT model. JECR 2012;13(2):104–21.
Zaharia A. 10 surprising cyber security facts that may affect your online safety. <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>; 2015.
Zahedi FM, Abbasi A, Chen Y. Fake-website detection tools: identifying elements that promote individuals' use and enhance their performance. J Assoc Inf Syst 2015;16:448–84.

**Dr.** Hsin-yi Sandy Tsai is an Assistant Professor in the Department of Communication and Technology at National Chiao Tung University. She holds a PhD in Media and Information Studies from Michigan State University. Her research interests are the use and impacts of new information and communication technologies, including telecommunication policies, technology adoption and use, public media, civic engagement, and digital inclusion. She is especially interested in how to make better policies to help people improve their quality of life and take full advantage of new technologies.

Mengtian Jiang is a PhD student in the Media and Information Studies program with a concentration in consumer psychology at Michigan State University. Prior to joining the PhD program, she earned her master degree in Advertising and her bachelor degree in Journalism. She is interested in understanding how people are influenced and persuaded by online information and online strangers, with a particular focus on consumer trust.

**Dr.** Saleem Alhabash is an Assistant Professor of Public Relations and Social Media, jointly appointed by the Department of Advertising + Public Relations and the Department of Media and Information at Michigan State University. He received his PhD from the University of Missouri's School of Journalism. His research focuses on the processes and effects of using new and social media. More specifically, his research untangles the ways in which computer-mediated communication can facilitate persuasion.

**Dr.** Robert LaRose is a full Professor in the Department of Media and Information at the Michigan State University where he teaches graduate courses in research methods and theory. His research interests are the uses and effects of new media. His current foci are the role of habits in media behavior and the adoption of broadband Internet among vulnerable populations. He is the co-author of a popular introductory textbook, *Media Now*. He was presented with the Outstanding Article Award for 2011 by the International Communication Association. He holds a PhD in Communication Theory and Research from the Annenberg School at the University of Southern California.

**Dr.** Nora J. Rifon is a full Professor in the Department of Advertising + Public Relations at Michigan State University. She earned her PhD in Business, and her MA and BA in Psychology. Her research interests include consumer privacy and online safety, marketing communications strategies, corporate reputation, sponsorship, and children and media. Her work has been published in *Communications of the ACM*, *New Media and Society*, *The Journal of Consumer Affairs*, *The Journal of Advertising*, *Advances in Consumer Research*, *Government Information Quarterly*, *The Journal of Interactive Advertising*, and *The International Journal of Advertising*, and in the proceedings of a variety of international conferences. She has served on the Executive Committee and the Publications Committee of the American Academy of Advertising, and on the editorial review boards of *The Journal of Advertising*, *The Journal of Consumer Affairs*, and *The Journal of Interactive Advertising*, and served as consultant to the State of Michigan Office of the Attorney General, private law firms, and the commercial sector.

**Dr.** Shelia R. Cotten, a sociologist, is a Professor in the Department of Media and Information at Michigan State University. She studies technology use across the life course, and the social, educational, and health outcomes of using various technologies. Her research has been funded by the National Institutes of Health and the National Science Foundation. Her work has been recently published in Computers & Education, Social Science & Medicine, Computers in Human Behavior, Journal of Family Issues, Journal of Applied Gerontology, Journal of Gerontology: Social Sciences, and Information, Communication, and Society. She and Laura Robinson are the co-editors of the *Emerald Series in Media and Communication*. In 2013, she won the award for Public Sociology from the Communication and Information Technologies section of the American Sociological Association (CITASA).