Computers in Human Behavior 70 (2017) 291–302

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

# Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors

Hongliang Chen [a, *], Christopher E. Beaudoin [b], Traci Hong [b]

[a] *Department of Communication, Texas A&M University, College Station, TX, USA*
[b] *College of Communication, Boston University, Boston, MA, USA*

ARTICLE INFO

*Article history:*
Received 3 October 2016
Received in revised form
30 December 2016
Accepted 1 January 2017
Available online 2 January 2017

*Keywords:*
Internet scam victimization
Privacy concerns
Privacy protection measures
Privacy knowledge
Routine Internet activities
Self-control abilities

ABSTRACT

The current study identified the antecedents of being an Internet scam victim and how it impacts online privacy concerns and privacy protection behaviors. Structural equation modeling on data from a survey of 11,534 Internet users revealed that one indicator of weak self-control (i.e., willingness of risky investments) and two indicators of routine Internet activities (i.e., online shopping and opening emails from unknown sources) positively predicted being an Internet scam victim. Subsequently, being an Internet scam victim predicted increased online privacy concerns, which, in turn, predicted elevated privacy protection behaviors. Moreover, we found that being an Internet scam victim mediated the effects of routine Internet activities on privacy protection behaviors and that online privacy concerns mediated the effect of being an Internet scam on privacy protection behaviors. Unlike most Internet privacy studies using protection motivation theory only, the current study contributes to the understanding of the Internet scam victimization by incorporating three new theories—extended parallel process model, self-control theory, and routine activity theory. The research findings provided valuable implications for theory and practice related to Internet scam processes and prevention.

© 2017 Elsevier Ltd. All rights reserved.

The Internet is becoming a major avenue for the business transactions of corporate users and other individuals. E-commerce retail sales reached $236.9 billion in 2014 (STATISTA, 2015). A majority of American Internet users search for online product information and make online purchases on a daily basis (Flanagin, Metzger, Pure, Markov, & Hartsell, 2014). The Internet also provides opportunities for criminals to target and attack victims. Criminals can infiltrate victims' personal online accounts and then create tailored scam emails to gain benefits from the victims (Chou, 2013). The anonymous online environment makes it difficult for users to identify such fraudulent probes (Bay, Cook, Grubisic, & Nikitkov, 2014). The reported financial loss of Internet scams was more than $800 million in 2014 (Internet Crime Complaint Center, 2014).

Internet scams aim to defraud victims (Buchanan & Whitty, 2014), with scammers applying different methods to steal victims' private information and trick them into making financial payments (Pratt, Holtfreter, & Reisig, 2010; Reyns, 2013; Salu, 2004; Vahdati & Yasini, 2015; Zahedi, Abbasi, & Yan, 2015). One of the best-known types of Internet scams is purchase fraud, in which scammers collect Internet users' credit card information and PIN numbers, which they then use to withdraw money from the victim's financial account (Yazdanifard, WanYusoff, Behora, & Sade, 2011). In another type of fraud, criminals build fake websites to induce victims with information intended to appear to be legitimate and reliable. Criminals offer fake products at extremely cheap prices and provide fake positive consumer comments to attract victims (Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010; Zahedi et al., 2015).

Research on such Internet privacy practices has been commonly based in protection motivation theory (PMT). PMT holds that, before people engage in risk reduction behaviors, they undergo risk appraisal and coping appraisal, which can spur the development of protection motivation and, in turn, actual protection behaviors (Rogers, 1983). With a basis in PMT, previous studies have yielded mixed results. Some researchers found that individuals follow the logic of PMT, in which privacy concerns do, indeed, mediate the

* Corresponding author.
*E-mail addresses:* hongliang.chen@tamu.edu (H. Chen), cebeau@bu.edu (C.E. Beaudoin), tjhong@bu.edu (T. Hong).

http://dx.doi.org/10.1016/j.chb.2017.01.003
0747-5632/© 2017 Elsevier Ltd. All rights reserved.

effects of risk appraisal and coping appraisal on the adoption of privacy protection strategies (Mohamed & Ahmad, 2012; Youn, 2009), whereas other studies failed to support the three-stage model (Chen, Beaudoin, & Hong, 2016a). The mixed support for PMT in the context of online privacy concerns could be the function of limitations in measurement or theory.

In light of these limitations, the current study tested seven antecedents of the Internet scam victimization and addressed how victim experiences influence people's privacy concerns and subsequent privacy protection behaviors. The current study contributes to the study of Internet privacy in two novel ways. First, in addition to PMT, we have incorporated extended parallel process model (EPPM) into our development of theory. Derived from PMT, EPPM explains why high perceived threat fails to predict behavioral changes under certain conditions (Witte, 1994). EPPM provides theoretical refinements to PMT, which we believe are instructive on online privacy processes. Second, we introduce two theories that are new to research on online privacy—self-control theory and routine activity theory—to explore the antecedents of Internet scam victimization.

## 1. Literature review

### 1.1. Self-control theory

Self-control theory was originally developed to explain the determinants of offending behaviors (Gottfredson & Hirschi, 1990). Self-control refers to one's ability to regulate emotions, behaviors, and desires (Beaver, Barnes, & Boutwell, 2014). People's general intelligence and personal backgrounds, such as educational level and prior experiences, determine one's ability of self-control (Halpern-Felsher et al., 2001; Hare, Camerer, & Rangel, 2009; Ommundsen, 2003). The theory proposes that criminal acts, which are unlawful (Wikström & Treiber, 2007), tend to be short-lived, impulsive, and exciting and, for these reasons, can satisfy a person's immediate gratifications (Gottfredson & Hirschi, 1990). People with low self-control, thus, are most likely to engage in criminal activities without considering the consequences of offending other people (Blanco et al., 2008; Bolin, 2004; Holtfreter, Reisig, Piquero, & Piquero, 2010; Martinez, Rutledge, & Sher, 2007; Pratt & Cullen, 2000; Vowell & Chen, 2004). Moreover, researchers found that low self-control people frequently get involved in risk-taking activities given their limited capacity to assess the severity and vulnerability of risks (Holtfreter et al., 2010). When tempted by fraudsters, low self-control people tend to gratify their immediate needs, including seeking out big discounts and free trials of new products, but underestimate long-term consequences (Holtfreter, Reisig, & Pratt, 2008). With such a limited appraisal of risks, low self-control people tend to become the primary targets of Internet scams (Van Wilsem, 2013). Related research has supported the correlation between low self-control and victimization of crime. For instance, scholars have confirmed the inverse association between self-control and the possibility of being a victim of crime (Forde & Kennedy, 1997), including in the contexts of violent crime (Schreck, Stewart, & Osgood, 2008; Schreck, Wright, & Miller, 2002; Stewart, Elifson, & Sterk, 2004) and homicide (Piquero, MacDonald, Dobrin, Daigle, & Cullen, 2005).

With the emergence of Internet crime, research has begun to test the association between low self-control and being a victim of Internet fraud. Internet fraud requires some extent of trust between victims and criminals (Holtfreter et al., 2010). In online scam attempts, criminals intentionally induce victims to make payments for promised items and services and invest in financial institutions (Titus, 2001), but, for the attempts to be successful, victims must click on pop-up links, download programs with malicious software, or engage in monetary transactions with fraudsters. According to Holtfreter et al. (2008), people with low self-control reported a higher frequency of engagement in online purchases, which may increase their chance of experiencing online fraud. Moreover, another study confirmed that irrational consumers, who are financially impulsive, tend to engage in more online purchases than rational consumers (Reisig, Pratt, & Holtfreter, 2009). In the purchase-decision process, impulsive consumers tend to be less concerned about marketers' guarantees and product reputations, which make them ideal targets for fraudsters (Holtfreter et al., 2008). Once targeted, low self-control people are less likely to scrutinize privacy risks and are more likely to behave in ways that comply with scammers.

The current study operationally defines people's self-control in two ways: 1) willingness to make risky investments; and 2) knowledge about Internet privacy. People's willingness to make risky investments reflects their desire for immediate gratifications (Holtfreter et al., 2008). People who make risky investments value potential monetary profits, but tend to be less concerned with the risks of monetary losses. When confronting related offers from criminals, people who favor risky investments are more likely to be deceived. Consistent with previous research (Van Wyk & Mason, 2001), we treat the willingness to make risky financial investments as an indicator of low self-control. Also consistent with prior research (Taylor, Davis, & Jillapalli, 2009), we rely on people's knowledge about Internet privacy to reflect high self-control. Knowledge about Internet privacy entails a person's perceptions of the following: website privacy policies, unknown collection of personal information online, and risks of disclosing personal data online. We postulate that people with higher levels of Internet privacy knowledge are more likely to recognize the suspicious offers of criminals. Thus, as shown in Fig. 1, we hypothesize that knowledge about Internet privacy is negatively associated with victimization of Internet scam, whereas willingness to make risky investments is positively associated with such victimization.

**H1a**. Willingness to make risky investments is positively associated with the likelihood of being an Internet scam victim.

**H1b**. Knowledge about Internet privacy is inversely associated with the likelihood of being an Internet scam victim.

### 1.2. Routine activity theory

Routine activity theory proposes that the possibility of being a crime victim increases when motivated offenders and targeted victims are present in the same time and physical location (Cohen & Felson, 1979). In criminology studies, a crime victim refers to an identifiable individual who has been harmed by criminals individually, whereas victimization refers to the process of suffering the brunt of crime (McShane & Williams, 1992). In traditional street crime studies, researchers have found a strong association between non-domestic routine activities and being a crime victim. For instance, frequent visits to night clubs (Mustaine & Tewksbury, 1998), participation in sports activities, and visits to restaurants (Van Wilsem, 2011) were found to increase the occurrence of victimization. Moreover, Cohen and Felson (1979) noted that changes in communication technologies may increase victims' exposure to criminals. Researchers argue that the Internet can spur criminal activities given the anonymity of online contacts, convenience of online search for others' personal information, ease of distributing scam information, and absence of strong legal regulation (Newman & Clarke, 2003).

The emergence of the Internet provides opportunities for offenders to commit Internet scams. With the evolution of the

Internet, people's participation in routine activities is not limited to a certain physical location or time of a day (Reyns, 2013). For instance, searching an e-library and shopping online do not require people's respective physical presence in a library or a shopping mall, respectively (Eck & Clarke, 2003). For this reason, crime patterns on the Internet are dramatically changing (Holt & Bossler, 2009), with the convergence of time and physical location between criminals and victims being unimportant (Newman & Clarke, 2003). In particular, cyber criminals can send messages online to target audiences at a distance and at any time of the day.

Due to the threat of Internet scams, it is important to consider the risks of routine Internet activities that could expose potential victims to cyber criminals. Prior research has documented that individuals' Internet routines are positive predictors of online crime. For example, Pratt et al. (2010) found that the greater time spent on the Internet, the greater exposure to perpetrators. The use of social networking sites and online forums can especially increase people's visibility and accessibility to potential offenders. Fraudsters may select targets according to profile information disclosed online and develop appropriate strategies to induce specific individuals (Van Wilsem, 2013). Online information disclosure can entail a person's sharing or making public of demographic information, personal contacts, and personal schedules online (Chen & Beaudoin, 2016). We, thus, expect that disclosing information online is positively associated with victimization of Internet scams.

Research has demonstrated other online routines that predict victimization of Internet scams, including online shopping (Reyns, 2013), information search (Pratt et al., 2010), and downloading files (Holtfreter et al., 2008). Online shopping allows users to purchase products directly from a seller over the Internet (Mosteller, Donthu, & Eroglu, 2014). The potential threat here is that online shopping increases the risk of information theft and monetary loss (Aghekyan-Simonian, Forsythe, Kwon, & Chattaraman, 2012). By creating fake retail websites, criminals collect and record victims' financial information when victims are making a transaction (Yazdanifard et al., 2011). In the current study, we expect a positive association between online shopping and victimization of Internet scams.

Downloading files is another pertinent online routine activity. It refers to receiving textual, audio, video files, and software from websites. Computers that download files from unreliable sources can become infected with malicious software (Provos, Rajab, & Mavrommatis, 2009). Hackers can make use of the malicious software to attack users' computers and smartphones and steal private information stored in the devices (Töyssy & Helenius, 2006). It is challenging for Internet users to recognize malicious software given that it appears to be credible (Jacob, Debar, & Filiol, 2008). In the current study, we postulate a positive association between downloading files and victimization of Internet scams.

We also examine two other types of routine Internet activities: online information consumption and opening emails from unknown sources. Online information consumption refers to viewing

\

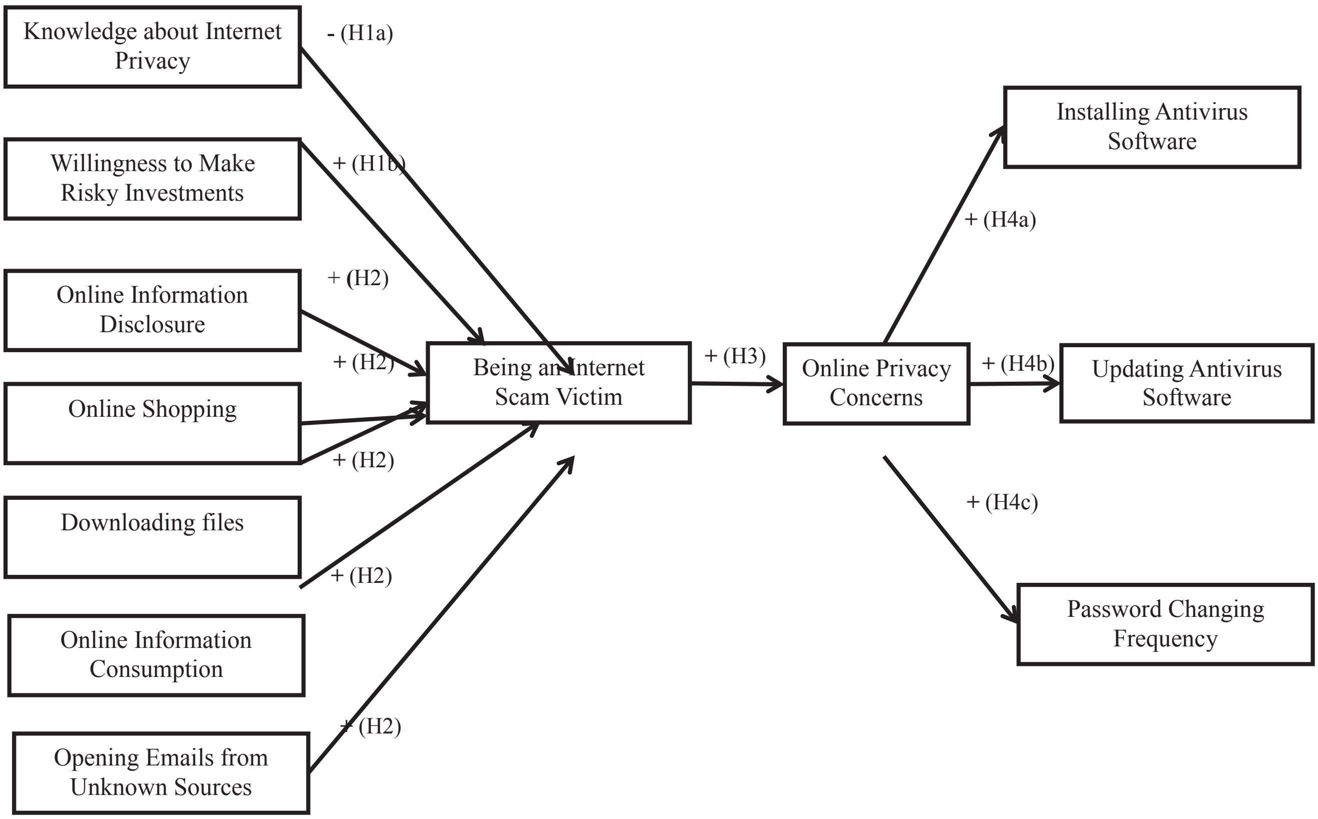
Knowledge about Internet Privacy
- (H1a)
Willingness to Make Risky Investments
+ (H1b)
Online Information Disclosure
+ (H2)
Online Shopping
+ (H2)
+ (H2)
Downloading files
+ (H2)
Online Information Consumption
Opening Emails from Unknown Sources
+ (H2)
Being an Internet Scam Victim
+ (H3)
Online Privacy Concerns
+ (H4a)
Installing Antivirus Software
+ (H4b)
Updating Antivirus Software
+ (H4c)
Password Changing Frequency

**Fig. 1.** Four-Stage Conceptual Framework (with indication of effect valence and pertinent hypothesis).

news, health information, and product descriptions, as well as reading emails and financial account information (Coiro & Dobler, 2007). Once malware is installed on a user's computer, criminals can monitor the user's online information consumption and design soliciting information accordingly. Moreover, opening emails from unknown resources can lead users to unsafe websites and result in the installation of malicious software (Bergholz et al., 2010). Perpetrators use such “phishing” emails to acquire individuals' sensitive information, such as passwords and credit card information (Almomani et al., 2012). Links on phishing emails can direct users to websites with malware and induce users to enter their personal information (Verma, Shashidhar, & Hossain, 2012). The current study postulates that online information consumption and opening emails from unknown sources are positively associated with victimization of Internet scams. We set forth a comprehensive hypothesis as depicted in Fig. 1.

**H2**. Routine Internet activities (information disclosure, online shopping, downloading files, online information consumption, and opening emails from unknown sources) are positively associated with the likelihood of being an Internet scam victim.

### 1.3. *Fear-based theories*

Fear-oriented theories, such as PMT and EPPM, provide systematic explanations for people's selection of risk-reduction strategies. Rogers (1975, 1983) developed PMT to explain the discrepancy in people's adoption of risk-reduction behaviors. PMT holds that behavior change is a function of people's undergoing cognitive appraisal and, in turn, the development of motivation to adopt a new behavior. Two parallel appraisal processes function simultaneously. Threat appraisal comprises the outcomes of risk taking, including perceptions of vulnerability, severity, and the rewards of a risky behavior (LaRose, Rifon, & Enbody, 2008; Youn, 2009). Response appraisal encompasses response efficacy, self-efficacy, and the response cost (LaRose et al., 2008; Prentice-Dunn, McMath, & Cramer, 2009). PMT suggests that protection motivation consists of six cognitive appraisal factors, including severity, vulnerability, response efficacy, self-efficacy, costs, and rewards, which lead to risk-reduction behaviors (Maddux & Rogers, 1983).

In expanding upon PMT, EPPM argues that, in the primary appraisal stage, people assess perceived severity and susceptibility of a risk threat, as well as self-efficacy and response efficacy (Witte, 1994). Perceived severity refers to people's perception of how serious a threat is, whereas perceived susceptibility reflects the likelihood that a threat will impact oneself (Witte, 1992). Self-efficacy reflects individuals' beliefs in their ability to perform actions to control the risks, whereas response efficacy refers to individuals' beliefs in the effectiveness of the risk control strategies (Witte, 1992). In differing from PMT, EPPM adds a secondary appraisal process in which individuals' assessments of perceived threat and efficacy determine whether they will engage in danger control or fear control. If perceived efficacy is low and perceived threat is high, people tend to engage in fear control, which entails their believing that they are not competent to avoid a risk. In fear control, individuals prefer to dismiss high-threat messages, avoid adaptive changes, and develop cognitive defensive avoidance (McMahan, Witte, & Meyer, 1998). In contrast, if perceived efficacy and perceived threat are both high, people tend to engage in danger control, which entails their being confident in taking mitigating adaptive actions (Witte, 1994). In danger control, people are likely to develop protection motivation and adopt protective behavioral changes. Finally, if perceived threat is low, people tend to disregard a fear appeal message altogether (Witte, 1992).

### 1.4. *Related works*

Using PMT as a theoretical framework, multiple studies have investigated Internet users' privacy protection behaviors (Dinev & Hart, 2004; Rifon, LaRose, & Choi, 2005). Privacy protection motivation and privacy protection behaviors are two concepts central to the literature on Internet privacy studies. Drawn from the definition of protection motivation and protection behaviors in PMT, privacy protection motivation reflects people's concerns about the misuse of online private information by third-parties (Dinev & Hart, 2004), whereas privacy protection behaviors entail behavioral efforts to prevent privacy loss (D. Lee, Larose, & Rifon, 2008; Mohamed & Ahmad, 2012). In the Internet privacy literature, privacy protection behaviors have been operationalized in various ways, including the installation of anti-virus software (D. Lee et al., 2008), use of false personal information (Chen, Beaudoin, & Hong, 2016b; Youn, 2005), avoidance of suspicious websites (Youn, 2009), deletion of unwanted online contacts (Chen et al., 2016b), and seeking for help from others (Youn, 2005). Privacy protection motivation has been operationalized as online privacy concerns (Chen et al., 2016b; Feng & Xie, 2014; Youn, 2009). Online privacy concerns reflect people's worries about their capacity to prevent the misuse of online personal information by others (Culnan & Bies, 2003). Online privacy concerns develop from personal encounters, such as monetary loss due to the theft of financial account information, and hearing from media reports, friends, and families about online privacy risks (Brandimarte, Acquisti, & Loewenstein, 2013; Bryce & Fraser, 2014). Moreover, consistent with PMT's suggestion that protection motivation leads to protection behaviors, Internet privacy researchers documented positive associations between online privacy concerns and privacy protection behaviors (LaRose & Rifon, 2007; Rifon et al., 2005).

A growing body of survey research has used PMT as a basis for exploring multistep processes on online privacy concerns. It is important to review and synthesize these studies as a means to stressing two areas of common divergence: 1) measurement; and 2) mediation testing. Two studies have centered exclusively on the antecedents of privacy protection behaviors. In the first study, Youn (2005) analyzed the antecedents of teen's online privacy protection behaviors. That prior study's antecedents included perceived susceptibility and perceived severity of online privacy risks, perceived benefits of Internet use, and willingness to disclose information. The regression results suggested that perceived susceptibility of privacy led to actual privacy protection behaviors, whereas teen Internet users' willingness to provide information online was found to be inversely associated with privacy protection behaviors. In the second study, Lee et al. (2008) tested seven antecedents of adopting virus protection strategies online: perceived severity of virus attacks, perceived vulnerability of virus attacks, perceived response efficacy, self-efficacy, positive outcome expectations, negative outcome expectations, and prior virus infection experiences. The results suggested that self-efficacy, response efficacy, positive outcome expectations, perceived vulnerability, and prior virus infection experiences were strong predictors of privacy protection behaviors. A third study independently considered the separate predictors of online privacy concerns and of privacy protection behaviors. In that study, Mohamed and Ahmad (2012) tested five antecedents of online privacy concerns: self-efficacy, perceived severity, perceived vulnerability, response efficacy, and perceived rewards of providing personal information. Results suggested that perceived severity, perceived vulnerability, and self-efficacy were positive predictors of online privacy concerns and that online privacy concerns predicted privacy protection behaviors. None of these three studies tested multistep mediation processes. In addition, in terms of variation in measurement, Lee et al. (2008) and

Mohamed and Ahmad (2012) employed comprehensive measurement of the four core constructs of PMT and EPPM (i.e., severity, vulnerability, self-efficacy, response efficacy), whereas Youn (2005) only measured two (i.e., severity and vulnerability).

Two more recent studies have advanced this research by building multistep models that are generally as follows: 1) antecedents; 2) online privacy concerns; and 3) protection behaviors. In the first study, the three stages of a structural equation model were as follows: 1) Internet use, persuasion knowledge, privacy knowledge, vulnerability to risks, disclosure benefits, and privacy self-efficacy; 2) online privacy concerns; and 3) privacy protection behaviors (Youn, 2009). This study found that privacy concerns mediated the effects of perceived risks and perceived benefits on privacy protection behaviors. In the second study, scholars also used structural equation modeling to test a multistep model on the online privacy processes of teen Internet users (Chen et al., 2016b). The four stage-model was as follows: 1) cost/benefits appraisal, interpersonal trust, and parental influence; 2) privacy concerns; 3) protection behaviors; and 4) information disclosure online. Results suggested that mediation effects were quite rare, limited to only teen privacy concerns mediating the effects of parental privacy concerns and parental interpersonal trust on teen privacy protection behaviors. Only Youn (2009) has found strong support for how online privacy concerns can mediate the effects of antecedents on protection behaviors—and both of these studies (Chen et al., 2016b; Youn, 2009) employed quite limited measurement approaches to protection motivation via operational definition with online privacy concerns.

Consistent with prior studies, in our conceptual model (see Fig. 1), privacy protection motivation is operationalized as online privacy concerns (Feng & Xie, 2014; Mohamed & Ahmad, 2012; Youn, 2009). One novel contribution of the current study is to test the association between prior experiences of being an Internet scam victim and online privacy concerns. Prior research suggested that people often use prior experiences to predict future online privacy decisions (Cho, Lee, & Chung, 2010). The experience of online privacy loss can help users understand that online privacy risks are relevant to themselves (X. Li, 2008). Moreover, the victims of online privacy invasion tend to understand the severe consequences of privacy loss. People who have been victim to Internet scams are more likely to build knowledge about related severity and vulnerability (Mohamed & Ahmad, 2012). Consistent with PMT and EPPM, which hold that severity and vulnerability appraisals are influential factors in determining people's protection motivation and subsequent protection behaviors (Rogers, 1975), the current study expects that being an Internet scam victim positively predicts online privacy concerns (see Fig. 1).

**H3**. Being an Internet scam victim is positively associated with online privacy concerns.

According to PMT and EPPM, protection motivation leads to actual risk-reducing behavioral changes (Rogers, 1975). The current study examines three types of privacy protection behaviors: installing antivirus software, updating antivirus software, and password changing frequency for email and financial accounts. Antivirus software provides protection against online privacy invasion, helping monitor such attacks, filter out spy software, and clean up suspicious computer programs (Y. Lee & Kozar, 2008). As depicted in Fig. 1, we hypothesize that people who are concerned about online privacy are likely to install and update antivirus software for their computers.

**H4a**. Online privacy concerns are positively associated with installing antivirus software.

**H4b**. Online privacy concerns are positively associated with updating antivirus software.

The use of passwords is another popular strategy to protect one's privacy online. Researchers recommend that Internet users construct passwords with a combination of complex codes and avoid using codes in association with personal information (Andrews, 2002; Brown, Bracken, Zoccoli, & Douglas, 2004; Groves, 2002). With the advances of technology, however, even strong passwords are unable to resist the encroachment of hackers. To mitigate potential risks, one of the most effective strategies is to change passwords frequently (Inglesant & Sasse, 2010). In the current study, we measured password changing frequency specific to financial and email accounts. It would be expected that people with high privacy concerns are likely to understand passwords risks and change passwords frequently (see Fig. 1).

**H4c**. Online privacy concerns are positively associated with password changing frequency.

Finally, we draft two hypotheses specific to potential mediation paths in the theoretical model (see Fig. 1). Integral to the model are two types of mediated effects. First, being an Internet scam victim is expected to mediate the effects of the first-stage measures of self-control and routine Internet activities on online privacy concerns. Second, online privacy concerns are expected to mediate the effects of being an Internet scam victim on the fourth-stage privacy protection behavior variables (i.e., installing antivirus software, updating antivirus software, password changing frequency). These mediated paths are somewhat different from those examined in prior research, which has tested how privacy concerns mediate the effects of risk appraisals on privacy protection behaviors (Chen et al., 2016b; Youn, 2009) and how privacy protection behaviors mediate the effects of online privacy concerns on information disclosure (Chen et al., 2016b). In the current study, we tested a four-stage model with two types of mediation processes. We posit two related hypotheses:

**H5a**. Being an Internet scam victim mediates the effects of self-control and routine Internet activities on online privacy concerns.

**H5b**. Online privacy concerns mediate the effects of being an Internet scam victim on privacy protection behaviors.

## 2. Methods

The survey data (N = 11,741) were collected by GfK Knowledge Networks from November 23 to December 30 in 2013. The online survey was conducted among adults aged 18 and older residing in the United States. The respondents were sampled from the GfK panel, which is a probability based panel that is representative of the Unite States population. Because the current study focused on Internet scams, we dropped non-Internet users, resulting in a final sample size of 11,534. Such a large sample size poses some natural problems for statistical inference. After all, with large samples, even small effects can be statistically significant, which is consistent with Type I error (Lin, Lucas Jr., & Shmueli, 2013). To address this issue, we present effect sizes and, for determining significance, use 0.001 as the critical p-value. Finally, given that the missing data of various variables were present in fewer than 5% of the cases (Tabachnick & Fidell, 2007), we recoded the missing values in continuous variables with the grand mean and missing values in dichotomous variables with zero (Eekhout, de Boer, Twisk, de Vet, & Heymans, 2012).

We completed a series of Kolmogorov-Smirnov tests to identify if the dependent variables had univariate normal distributions (Justel, Peña, & Zamar, 1997). For the significantly skewed variables, we used histograms to identify the direction of skewness. Consistent with previous studies, we conducted square transformations for continuous variables that were skewed left and log transformations for variables that were skewed right (Manning & Mullahy, 2001; Osborne, 2005). The transformed variables were used for SEM, whereas the untransformed variables are presented for descriptive statistics.

### 2.1. Measurement

We treated age, education, gender, household income, ethnicity (i.e., black, Hispanic, mixed race, and non-white other race), and hardships in life as exogenous control variables (See Table 1). Most of the respondents identified themselves as White (81%), followed by African American (7%), Hispanic American (7%), Mixed Race (3%), and other race (2%). Age was measured with seven categories: 18–24 (1), 25–34 (2), 35–44 (3), 45–54 (4), 55–64 (5), 65–74 (6), and above 75 years old (7). The average age of respondents was between 45 and 54 years old. Household income was measured on a 19-point scale from "less than $5000" (1) to "$175,000 or more" (19). The mean was about 11, which represented household income between $40,000 and $50,000. Education was measured on a 14-point scale from "no formal education" (1) to "professional or doctoral degree" (14). The mean was 10, which represented "some college, no degree." In terms of gender, 41.17% of respondents were male. Hardships in life was measured with 10 dichotomous questions, asking about people's negative experiences in the past two years (i.e., loss of job, stress associated with moving, divorce). The rest of the variables were endogenous. To reflect the reliability of measurements in the current study, we reported Pearson correlation for 2-item scales with continuous variables and Kuder-Richardson 20 (KR-20) for indexes with multiple binary items.

**Table 1**
Descriptive statistics of variables (N = 11,534).

| Variables | Mean | SD | Min | Max |
|---|---|---|---|---|
| Exogenous Variables | | | | |
| Age[a] | | | | |
| 18-24 | 6.17% | | | |
| 25-34 | 13.42% | | | |
| 35-44 | 13.25% | | | |
| 45-54 | 17.83% | | | |
| 55-64 | 4.07% | | | |
| 65-74 | 18.35% | | | |
| 75+ | 6.92% | | | |
| Education | 10.77 | 1.67 | 1 | 14 |
| White[a] | 81.65% | | | |
| Black[a] | 6.83% | | | |
| Hispanic[a] | 6.59% | | | |
| Mixed Race[a] | 2.64% | | | |
| Other Race[a] | 2.28% | | | |
| Sex (Male)[a] | 41.17% | | | |
| Household Income | 11.32 | 4.26 | 1 | 19 |
| Hardships in Life | 1.56 | 1.54 | 0 | 10 |
| Endogenous Variables | | | | |
| Knowledge about Internet Privacy | 5.23 | 2.60 | 0 | 11 |
| Willingness to Make Risky Investments | 2.11 | 1.02 | 0 | 5 |
| Online Information Disclosure | 1.93 | 1.80 | 0 | 9 |
| Online Shopping[a] | 31.32% | | | |
| Downloading Files | 2.90 | 1.84 | 0 | 6 |
| Online Information Consumption | 6.10 | 1.93 | 0 | 8 |
| Opening Emails from Unknown Sources[a] | 17.35% | | | |
| Being an Internet Scam Victim | 0.02 | 0.20 | 0 | 8 |
| Online Privacy Concerns | 3.74 | 0.96 | 1 | 5 |
| Installing Antivirus Software[a] | 87.15% | | | |
| Updating Antivirus Software | 4.28 | 1.00 | 1 | 5 |
| Password Changing Frequency | 2.29 | 0.93 | 1 | 5 |

[a] Represents the frequency of a dichotomous variable.

#### 2.1.1. Knowledge about Internet privacy

Much like prior research (Smit, Van Noort, & Voorveld, 2014), knowledge about Internet privacy was measured using 11 true/false statements. The questions tested respondents' understanding of website privacy policies, use of personal information by websites, online bank account security, privacy settings on social networking sites, and third-party access to personal information. The total score ranged from 0 to 11 correct answers. The 11 items were added to create an index (M = 5.23, SD = 2.60; KR-20 = 0.71).

#### 2.1.2. Willingness to make risky investments

The measurement of willingness to make risky investments was based in prior research (Van Wyk & Mason, 2001). The following two items were used for willingness of risky investments: "I don't mind taking chances with my money, as long as I think there's a change it might pay off" and "I enjoy making risking financial investments now and then" (M = 2.11, SD = 2.60; r = 0.60, p < 0.001). Responses were on a 5-point scale from "strongly disagree" (1) to "strongly agree" (5).

#### 2.1.3. Routine Internet activities

We assessed five types of routine Internet activities: online information disclosure, online shopping, downloading files, online information consumption, and opening emails from unknown sources. Consistent with previous research (Chen & Beaudoin, 2016), we measured online information disclosure with nine dichotomous items, including birthdate, home address, social security number, maiden name, cell phone number, landline number, relationship status, names of family members, and personal schedule. The nine items were added to create an index (M = 1.93, SD = 1.80, KR-20 = 0.70).

Online shopping was measured with a single item, asking respondents if they had purchased a product through electronic money payment in the past seven days. About 31.32% of respondents reported online shopping behaviors within the past week.

We measured various types of downloading, including video, music, games, and applications for social media and instant messaging. Respondents reported if they conducted such online downloading in the past seven days (yes = 1, no = 0). The six items were added to create an index (M = 2.90, SD = 1.84, KR-20 = 0.71).

In line with previous research (Coiro & Dobler, 2007), the current study measured online information consumption with eight items, including reading email, news, health information, product descriptions, weather information, and travel websites. The dichotomous answers were added to create an index (M = 6.10, SD = 1.93, KR-20 = 0.74).

We measured opening emails from unknown sources with a single item, asking respondents if they had opened emails from strangers. About 17% of respondents reported the experience of opening emails from unknown sources in the past seven days.

#### 2.1.4. Being an Internet scam victim

With a basis in previous research (Holt & Bossler, 2009), we operationally defined being an Internet scam victim in terms of losing money to online scammers. The current study examined eight types of Internet scams, including advance fee for debt relief, relative in distress, sweepstakes offer, foreign lottery, secret shoppers, credit cards, and general Internet scams. In total, 283 respondents claimed to experience at least one of the Internet scams. We added the dichotomous items to create an additive index (M = 0.02, SD = 0.20, KR-20 = 0.59).

#### 2.1.5. Online privacy concerns

Prior studies have measured online privacy concerns with a

**Table 2**
Standardized direct effects of exogenous variables on endogenous variables in structural equation model.

| | Age | Edu-cation | Black | His-panic | Mixed race | Non-white other race | Sex (Male) | House-hold Income | Hardships in Life |
|---|---|---|---|---|---|---|---|---|---|
| Knowledge about Internet Privacy | −0.11* | 0.18* | −0.06* | −0.05* | 0.01 | −0.01 | 0.09* | 0.11* | 0.10* |
| Willingness to Make Risky Investments | −0.15* | 0.02 | 0.03 | 0.04* | 0.02 | 0.04* | 0.18* | 0.09* | 0.02 |
| Online Information Disclosure | −0.28* | 0.01 | −0.03* | −0.03* | 0.00 | −0.01 | −0.12* | −0.01 | 0.15* |
| Online Shopping | −0.07* | 0.04* | −0.03 | −0.02 | 0.01 | 0.01 | 0.00 | 0.06* | 0.05* |
| Downloading Files | −0.38* | 0.07* | −0.03 | −0.01 | 0.01 | 0.00 | −0.05* | 0.05* | 0.13* |
| Online Information Consumption | −0.14* | 0.22* | −0.01 | −0.01 | −0.01 | 0.00 | −0.07* | 0.22* | 0.12* |
| Opening Emails from Unknown Sources | −0.05* | 0.03 | 0.02 | −0.02 | 0.00 | 0.01 | 0.07* | −0.02 | 0.12* |
| Being an Internet Scam Victim | 0.03 | 0.00 | 0.02 | 0.03* | 0.01 | 0.02 | 0.00 | −0.02 | 0.05* |
| Online Privacy Concerns | 0.20* | −0.10* | 0.10* | 0.09* | 0.01 | 0.07* | −0.05* | −0.05* | 0.07* |
| Installing Antivirus Software | 0.12* | 0.06* | −0.05* | −0.06* | 0.00 | −0.01 | 0.01 | 0.08* | 0.04* |
| Updating of Antivirus Software | 0.00 | 0.01 | −0.07* | −0.03 | 0.01 | −0.01 | 0.09* | −0.03 | 0.01 |
| Password Changing Frequency | −0.13* | 0.03 | −0.04* | −0.01 | 0.01 | 0.01 | 0.01 | −0.01 | 0.02 |

*p < 0.001.

single item, focusing on levels of concerns about online privacy safety (Youn & Hall, 2008; Youn, 2009). We used a related measure, as well as a second measure on concerns about being scammed (r = 0.68, p < 0.001). Responses to each measure were on a 5-point scale from “not at all concerned” (1) to “extremely concerned” (5) (M = 3.73, SD = 0.96).

### 2.1.6. *Privacy protection behaviors*

Respondents were asked if they have antivirus programs loaded on at least one computer, laptop, or other device with Internet access at home. About 87% of respondents reported that they have installed protection software. Moreover, we measured people's frequency of updating antivirus software. Respondents were asked to recall the most recent updating of antivirus software from “never” (1) to “within the past month” (5) (M = 4.28, SD = 1.00). We also measured the frequency of changing passwords for financial and email accounts. Respondents were asked to recall their frequency in changing these passwords, with responses ranging from “never” (1) to “at least once a week” (5). This resulted in a two-item composite measure (M = 2.29, SD = 0.93; r = 0.62, p < 0.001).

### 2.2. *Analysis procedure*

Using maximum likelihood estimation, we tested the multi-stage model with structural equation modeling (SEM) with STATA 13.0. The model consists of five stages: 1) exogenous control variables; 2) routine Internet activities and indicators of self-control; 3) being an Internet scam victim; 4) online privacy concerns; and 5) privacy protection behaviors. In particular, paths were positioned from stage 1 exogenous variables to all of the endogenous variables, from stage 2 variables to the stage 3 variable, from the stage 3 variable to the stage 4 variable, and from the stage 4 variable to the stage 5 variable. Moreover, we added 22 covariance paths between same-stage endogenous variables. We reported the comparative fit index (CFI) and root mean square error of approximation (RMSEA) to reflect the model fit. For CFI, scholars have recommended different benchmarks, including 0.90 or greater (Kline, 2005) and 0.95 or greater (Hu & Bentler, 1999). For RMSEA, Hu and Bentler (1999) recommended a benchmark of near or greater than 0.06, whereas Kline (2005) specified that 0.05 indicates good fit, 0.08 fair fit, and 0.10 marginal fit. Also, we reported $\chi^2$ statistics. Mediation was also closely tested with the product of coefficients test (MacKinnon, Lockwood, Hoffman, West, & Sheets, 2002).

## 3. Results

The fit of our model was good ($\chi^2$ = 1372.349, p < 0.001; RMSEA = 0.059; CFI = 0.928). The effects of exogenous control variables and endogenous variables are depicted in Table 2 and Table 3, respectively. The Bentler-Taykov squared multiple correlation coefficients were as follows: knowledge about Internet privacy, 8.82%; willingness to make risky investments, 6.54%; online information disclosure, 13.35%; online shopping, 1.37%; downloading files, 17.97%; online information consumption, 14.80%; opening emails from unknown sources, 2.24%; being an Internet scam victim, 2.37%; online privacy concerns, 7.73%; installing

**Table 3**
Standardized effects of endogenous variables on other endogenous variables in structural equation model.

| | Effect | Knowledge about Internet privacy | Willingness to make risky investments | Online information disclosure | Online shopping | Downloading files | Online information consumption | Opening emails from unknown sources | Being an Internet scam victim | Online privacy concerns |
|---|---|---|---|---|---|---|---|---|---|---|
| Being an Internet Scam Victim | Direct | −0.03 | 0.05* | 0.06* | 0.04* | 0.01 | −0.04* | 0.08* | NA | NA |
| | Indirect | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| Online Privacy Concerns | Direct | NA | NA | NA | NA | NA | NA | NA | 0.04* | NA |
| | Indirect | −0.00 | 0.00* | 0.00* | 0.00* | 0.00 | −0.00* | 0.00* | NA | NA |
| Installing Antivirus Software | Direct | NA | NA | NA | NA | NA | NA | NA | NA | 0.02 |
| | Indirect | −0.00 | 0.00* | 0.00* | 0.00* | 0.00 | −0.00* | 0.00* | 0.00* | NA |
| Updating Antivirus Software | Direct | NA | NA | NA | NA | NA | NA | NA | NA | 0.01 |
| | Indirect | −0.00 | 0.00* | 0.00* | 0.00* | 0.00 | −0.00* | 0.00* | 0.00* | NA |
| Password Changing Frequency | Direct | NA | NA | NA | NA | NA | NA | NA | NA | 0.16* |
| | Indirect | −0.00 | 0.00* | 0.00* | 0.00* | 0.00 | −0.00* | 0.00* | 0.01* | NA |

*p < 0.001.; NA means not applied.

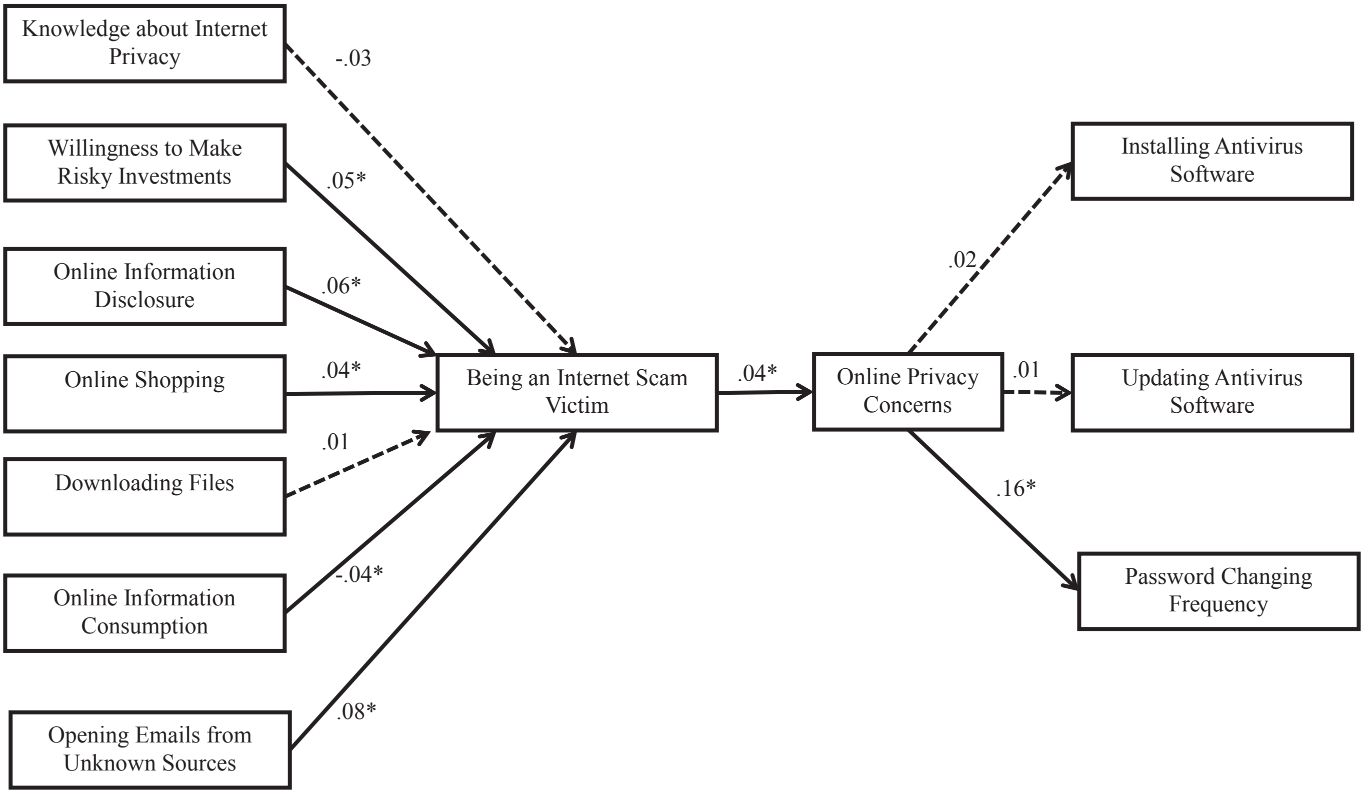
Knowledge about Internet Privacy
-.03
Willingness to Make Risky Investments
.05*
Online Information Disclosure
.06*
Online Shopping
.04*
Downloading Files
.01
Online Information Consumption
-.04*
Opening Emails from Unknown Sources
.08*
Being an Internet Scam Victim
.04*
Online Privacy Concerns
.02
.01
.16*
Installing Antivirus Software
Updating Antivirus Software
Password Changing Frequency

**Fig. 2.** Four-Stage Structural Equation Model (with non-significant paths dotted).

antivirus software, 3.80%; updating antivirus software, 1.30%; frequency of password changes, 3.40%.

Results pertinent to hypotheses are depicted in Table 3 and Fig. 2. (For clarity of presentation, the effects of endogenous variables are not depicted in Fig. 2.) Hypothesis 1a postulated that knowledge about Internet privacy negatively predicts being an Internet scam victim. This hypothesis was not supported given the non-significant effect of knowledge about Internet privacy on online privacy concerns. Hypothesis 1b postulated that willingness to make risky investments positively predicts being an Internet scam victim. This path was positive and significant at the 0.001 level ($\beta = 0.05$), which provides support for this hypothesis.

Hypothesis 2 held that the routine Internet activities are positively associated with being an Internet scam victim. The effects of online information disclosure ($\beta = 0.06$), online shopping ($\beta = 0.04$), and opening emails from unknown sources ($\beta = 0.08$) were positive and significant at the 0.001 level, whereas the effect of downloading files was not significant. The effect of online information consumption was inversely associated with being an Internet scam victim ($\beta = -0.04$, $p < 0.001$), which is contrary to the hypothesis. Hence, H2 was supported in three of five cases.

Hypothesis 3 posited that being an Internet scam victim positively predicts online privacy concerns. The effect was positive and significant ($\beta = 0.04$, $p < 0.001$), providing support for H3.

Hypotheses 4a, 4b, and 4c held that online privacy concerns positively predict installing antivirus software, updating antivirus software, and frequency of password changes. Online privacy concerns were found to be positively correlated with password changing frequency ($\beta = 0.16$, $p < 0.001$), which provides support for H4c. The effects on installing and updating antivirus software were not significant, which provides no support for H4a and H4b.

Hypothesis 5a predicted that being an Internet scam victim mediates the effects of self-control and routine Internet activities on online privacy concerns. SEM suggested five relevant mediation path frameworks: 1) willingness to make risky investments → being an Internet scam victim → online privacy concerns; 2) online information disclosure → being an Internet scam victim → online privacy concerns; 3) online shopping → being an Internet scam

**Table 4**
Test of two-step mediation.

| Antecedent | Mediator | Outcome | Antecedents → Mediators | | Mediators → Outcomes | | z-score product |
|---|---|---|---|---|---|---|---|
| | | | Coefficients | S.E. | Coefficients | S.E. | |
| Willingness to Make Risky Investments | Being an Internet Scam Victim | Online Privacy Concerns | 0.046 | 0.010 | 0.042 | 0.009 | 22.120* |
| Online Information Disclosure | Being an Internet Scam Victim | Online Privacy Concerns | 0.061 | 0.011 | 0.042 | 0.009 | 26.194* |
| Online Shopping | Being an Internet Scam Victim | Online Privacy Concerns | 0.040 | 0.010 | 0.042 | 0.009 | 19.108* |
| Online Information Consumption | Being an Internet Scam Victim | Online Privacy Concerns | −0.041 | 0.011 | 0.042 | 0.009 | −16.637* |
| Opening Emails from Unknown Sources | Being an Internet Scam Victim | Online Privacy Concerns | 0.082 | 0.009 | 0.042 | 0.009 | 40.379* |
| Being an Internet Scam Victim | Online Privacy Concerns | Password changing Frequency | 0.042 | 0.009 | 0.157 | 0.009 | 77.382* |

*p < 0.001.

victim → online privacy concerns; 4) online information consumption → being an Internet scam victim → online privacy concerns; and 5) opening emails from unknown sources → being an Internet scam victim → online privacy concerns. The relevant products of coefficients (MacKinnon et al., 2002) are depicted in Table 4. The first five such z-score products involve this hypothesis, and each is significant at the 0.001 level (Craig, 1936). Thus, Hypothesis 5a is supported in these five cases.

Hypothesis 5b posited that online privacy concerns mediate the effects of being an Internet scam victim on the privacy protection behaviors. SEM suggested general support for one such mediation path framework: being an Internet scam victim → online privacy concerns → password changing frequency. The relevant product of coefficients (MacKinnon et al., 2002) is depicted in Table 4. It is significant at the 0.001 level (Craig, 1936) and provides support for this hypothesis.

## 4. Discussion

Our conceptual model proposes a four-stage progression: 1) Internet routine activities and self-control; 2) being an Internet scam victim; 3) online privacy concerns; and 4) privacy protection behaviors. Unlike previous studies primarily based on PMT (Chen et al., 2016b; LaRose et al., 2008; Mohamed & Ahmad, 2012; Youn, 2009), the current study contributes to the Internet privacy literature by incorporating extended parallel process model, along with routine activity theory and self-control theory to predict people's privacy concerns and online privacy practices. Consistent with self-control theory's postulation that low self-control increases the likelihood of being a crime victim (Gottfredson & Hirschi, 1990), our analysis documented that one indicator of low self-control—willingness to make risky investments—was positively associated with being an Internet scam victim. This result may imply that financially impulsive individuals fail to consider the risks of financial loss, with this latter ignorance increasing one's chances of being the victim of an online scam. However, contrary to the hypothesis on self-control, knowledge about Internet privacy did not predict being an Internet scam victim. This result may indicate a discrepancy between individuals' perceptions of privacy risks and actual privacy protection behaviors. This non-significant relationship may be a function of how Internet users usually attribute the risks of privacy loss to others and not to oneself, which, in turn, renders people to have lower levels of interest in engaging in privacy protection behaviors (Debatin, Lovejoy, Horn, & Hughes, 2009). Thus, people who are knowledgeable about Internet privacy may not actually adopt protection behaviors but simply believe that they themselves are immune to privacy invasion.

Also involving the first two stages in our conceptual model and consistent with routine activity theory (Cohen & Felson, 1979), being an Internet scam victim was positively predicted by three routine Internet activities: online information disclosure, online shopping, and opening emails from unknown sources. These results are in line with previous research that found that criminals design individualized information to target and induce victims according to the personal information they disclose online (Van Wilsem, 2013). For instance, if an individual discloses information about losing a job, cyber criminals could disseminate employment-related solicitation information accordingly. Moreover, online shopping and opening emails from unknown sources could also result in victimization of Internet scams. Criminals could, for example, acquire sensitive information through online transactions with victims or installing malware on victims' computers. Finally, it is interesting that online information consumption was inversely associated with being an Internet scam victim, which is contrary to the hypothesis. One reasonable explanation is that people's consumption of online information could include reports of privacy invasion online, which would be expected to increase perceptions of online privacy risks. As a result, people with high levels of online information consumption would be more alert to suspicious offers.

Specific to the second and third stages in our conceptual model, there was a significant association between being an Internet scam victim and online privacy concerns. Prior research centered only on online privacy concerns to represent privacy protection motivation (Chen et al., 2016b; Mohamed & Ahmad, 2012; Youn, 2009). Our finding here, however, is generally consistent with other research that has documented that actual negative privacy experiences predict online privacy concerns (Chen et al., 2016a; H.; Li, Sarathy, & Xu, 2010). Our demonstrating that online privacy concerns—an indicator of privacy protection motivation—are predicted by being an Internet scam victim suggests that people who experience monetary loss of Internet scams are likely to recognize the severity and susceptibility of Internet privacy risks. Given that prevention of Internet scams is relatively easy (e.g., detecting a fake offer and rejecting the offer), victims who experience monetary loss would tend to have higher levels of both perceived efficacy and perceived threat. Following the logic of EPPM and PMT, victim experiences would, thus, lead individuals into the danger control process, which entailed the development of privacy concerns and adoption of privacy protection methods.

Specific to the third and fourth stages in our conceptual model, the current study found support for the association between online privacy concerns and one operational measure of privacy protection behavior, which is consistent with PMT and EPPM, as well as some prior empirical findings. For instance, previous research detected that online privacy concerns could lead individuals to fabricate personal information for online registration, seek help for privacy settings, and avoid visiting suspicious websites (Chen et al., 2016b; Youn, 2009). The current study expands upon this prior research by implementing three different types of privacy protection—installing and updating anti-virus software and changing password frequency—and we found support for the effect of online privacy concerns on changing password frequency.

Finally, it is important to consider this study's documented cases of statistical mediation. Prior research has explored how online privacy concerns mediate the effects of antecedents on privacy protection behaviors, documenting a mix of strong support (Youn, 2009) and limited support (Chen et al., 2016b). In our more complex four-stage model, we tested the mediation roles of being an Internet scam victim and online privacy concerns. In the first regard, SEM, as well as the follow-up product of coefficients approach (MacKinnon et al., 2002), demonstrated mediation in five cases: 1) willingness of risky investments → being an Internet scam victim → online privacy concerns; 2) online information disclosure → being an Internet scam victim → online privacy concerns; 3) online shopping → being an Internet scam victim → online privacy concerns; 4) online information consumption → being an Internet scam victim → online privacy concerns; and 5) opening emails from unknown sources → being an Internet scam victim → online privacy concerns. This mediation role suggests that self-control and frequent involvement in online routines influence online privacy concerns through the experience of being an Internet scam victim. According to PMT, the cognitive appraisal process is influenced by prior experiences (Rogers, 1983). Similarly, the current study suggested that people with victim experiences tend to perceive high severity and vulnerability of privacy risks online, which, in turn, lead to high privacy concerns. Moreover, we extended upon the original PMT model by testing the antecedents of prior victim experiences. The results indicated that the antecedents of prior experiences—Internet use habits and self-control ability—can influence online privacy concerns through the mediation of prior victim experiences. In the second regard, SEM, as well as the follow-up product of coefficients approach (MacKinnon et al., 2002), demonstrated mediation in one case: being an Internet scam victim → online privacy concerns → password changing frequency. Such a mediation effect suggests that, before engaging in actual privacy protection behaviors, people tend to follow the sequence of cognitive appraisal, protection motivation, and protection behaviors, which is consistent with PMT (Rogers, 1975). Thus, being an Internet scam victim is not a sufficient basis for protection behaviors, with the development of online privacy concerns also requisite. Following the logic of EPPM, this finding suggests that people with victim experiences tend to be high in both perceived threat and perceived efficacy, which, in turn, lead to the danger control process.

### 4.1. Limitations

Four limitations should be noted. First, data used in this study are cross-sectional, which does not permit the testing of causal relationships. The ordering of variables in current study, however, is consistent with previous online privacy studies using PMT (Chen et al., 2016b, 2016a; Mohamed & Ahmad, 2012; Youn, 2009). Second, our reliance on secondary survey data brought with it some limitations in measurement. For example, we could not measure some core concepts of EPPM and PMT, such as perceived susceptibility, perceived severity, self-efficacy, and response efficacy. Third, in regards to privacy protection behaviors, we only tested installing and updating anti-virus software and password changing frequency, which are likely to be common practices of people with high Internet efficacy. We did not measure other simple protection measures, such as avoiding insecure web links or using fabricated personal information for registration. Fourth, some respondents may refuse to report prior victim experiences because the disclosure of traumatic experiences could be associated with shameful thoughts and painful feelings. In the current study, we cannot identify related cases of response bias, which can skew research findings.

## 5. Contributions and implications for future research

This study contributes to the Internet privacy literature in two novel ways. First, the current study introduced new theories to explain people's online privacy practices. Prior research with basis on PMT assumed that individuals follow the logic of PMT to assess the privacy risks, develop privacy concerns, and then make adaptive changes. The findings of the current study suggested that Internet users tend to ignore privacy risks until they encounter monetary loss online in person. The complex psychological mechanism behind people's privacy risk assessment requires other theoretical explanations, such as EPPM. Second, this study systematically assessed two antecedents of the Internet scam victimization—self-control ability and routine Internet activities. This study revealed that privacy risk on the Internet is ubiquitous and people with weak self-control ability appear to be the primary targets of Internet scams. The findings suggested that, to avoid the Internet scam, Internet users need to understand how Internet scams work and resist the desire for immediate monetary benefits.

We conclude this paper with three recommendations for future research. First, given that knowledge about Internet privacy did not decrease the likelihood of being an Internet scam victim, future research should expand its operational definition of high self-control specific to online privacy protection to include other factors, such as Internet efficacy. Second, the current study tested only five types of Internet routines. Future study should employ other common Internet routines such as social media use and online gaming. Unlike reading news and searching for information, social media use and online gaming involve the frequent exchange of information between users, which could especially increase the risk of privacy invasion. Third, future research should operationally define the core concepts of cognitive risk appraisal in PMT and EPPM, which would permit the more refined study of how the experiences of being an Internet victim influence people's cognitive appraisal of online privacy risks and privacy protection behaviors.

## References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly, 34*(3), 435–461.

Aghekyan-Simonian, M., Forsythe, S., Kwon, W. S., & Chattaraman, V. (2012). The role of product brand image and online store image on perceived risks and online purchase intentions for apparel. *Journal of Retailing and Consumer Services, 19*(3), 325–331.

Almomani, A., Wan, T.-C., Altaher, A., Manasrah, A., ALmomani, E., Anbar, M., … Ramadass, S. (2012). Evolving fuzzy neural network for phishing emails detection. *Journal of Computer Science, 8*(7), 1099–1107.

Andrews, L. W. (2002). Passwords reveal your personality. *Psychology Today, 35*(1), 16.

Bay, D., Cook, G. L., Grubisic, J., & Nikitkov, A. (2014). Identifying fraud in online auctions: A case study. *Accounting Perspectives, 13*(4), 283–299.

Beaver, K. M., Barnes, J. C., & Boutwell, B. B. (2014). *The nurture versus biosocial debate in criminology: On the origins of criminal behavior and criminology.* Thousand Oaks, CA: SAGE.

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of Computer Security, 18*(1), 7–35.

Blanco, C., Grant, J., Petry, N. M., Simpson, H. B., Alegria, A., Liu, S. M., et al. (2008). Prevalence and correlates of shoplifting in the United States: Results from the national epidemiologic survey on alcohol and related conditions (NESARC). *American Journal of Psychiatry, 165*(7), 905–913.

Bolin, A. U. (2004). Self-control, perceived opportunity, and attitudes as predictors of academic dishonesty. *Journal of Psychology, 138*(2), 101–114.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology, 18*(6), 641–651.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behavior, 30*, 299–306.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law, 20*(3), 261–283.

Chen, H., & Beaudoin, C. E. (2016). An empirical study of a social network site: Exploring the effects of social capital and information disclosure. *Telematics and Informatics, 33*(2), 432–435.

Chen, H., Beaudoin, C. E., & Hong, T. (2016a). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly, 93*(2), 409–429.

Chen, H., Beaudoin, C. E., & Hong, T. (2016b). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology, 67*(12), 2871–2881.

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.

Chou, T.-S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology, 5*(3), 79–88.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Coiro, J., & Dobler, E. (2007). Exploring the online reading comprehension strategies used by sixth-grade skilled readers to search for and locate information on the Internet. *Reading Research Quarterly, 42*(2), 214–257.

Craig, C. C. (1936). On the frequency of function of xy. *Annals of Mathematical Statistics, 7*(1), 1–15.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Mediated Communication, 15*(1), 83–108.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information*

*Technology, 23*(6), 413–422.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies, 16*(1), 7–39.

Eekhout, I., de Boer, R. M., Twisk, J. W., de Vet, H. C., et al. (2012). Missing data: A systematic review of how they are reported and handled. *Epidemiology, 23*(5), 729–732.

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33*(1), 153–162.

Flanagin, A., Metzger, M., Pure, R., Markov, A., & Hartsell, E. (2014). Mitigating risk in ecommerce transactions: Perceptions of information credibility and the role of user-generated ratings in product quality and purchase intention. *Electronic Commerce Research, 14*(1), 1–23.

Forde, D. R., & Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly, 14*(2), 265–294.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Groves, J. (2002). Feature: Truffles — myth or strategic plan? Sniffing out some bizarre and inspired ways of motivating people to remember their passwords. *Computer Fraud & Security, 2002*(1), 9–12.

Halpern-Felsher, B. L., Millstein, S. G., Ellen, J. M., Adler, N. E., Tschann, J. M., & Biehl, M. (2001). The role of behavioral experience in judging risks. *Health Psychology, 20*(2), 120.

Hare, T. A., Camerer, C. F., & Rangel, A. (2009). Self-control in decision-making involves modulation of the vmPFC valuation system. *Science, 324*(5927), 646–648.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holtfreter, K., Reisig, M. D., Piquero, N. L., & Piquero, A. R. (2010). Low self-control and fraud: Offending, victimization, and their overlap. *Criminal Justice and Behavior, 37*(2), 188–203.

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

Hu, L.-T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternative. *Structural Equation Modeling, 6*(1), 1–55.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Paper presented at the association for computing machinery, Chicago, IL*.

Internet Crime Complaint Center. (2014). *Internet crime annual report* (p. 2014). Retrieved from https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

Jacob, G., Debar, H., & Filiol, E. (2008). Behavioral detection of malware: From a survey towards an established taxonomy. *Journal in Computer Virology, 4*(3), 251–266.

Justel, A., Peña, D., & Zamar, R. (1997). A multivariate Kolmogorov-Smirnov test of goodness of fit. *Statistics & Probability Letters, 35*(3), 251–259.

Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: The Guilford Press.

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127–149.

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

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

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

Li, X. (2008). Third-person effect, optimistic bias, and sufficiency resource in Internet use. *Journal of Communication, 58*(3), 568–587.

Lin, M., Lucas, H. C., Jr., & Shmueli, G. (2013). Research commentary-too big to fail: Large samples and the p-value problem. *Information Systems Research, 24*(4), 906–917.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62–71.

MacKinnon, D. P., Lockwood, C. M., Hoffman, J. M., West, S. G., & Sheets, V. (2002). A comparison of methods to test mediation and other intervening variable effects. *Psychological Methods, 7*(1), 83–104.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479.

Manning, W. G., & Mullahy, J. (2001). Estimating log models: To transform or not to transform? *Journal of Health Economics, 20*(4), 461–494.

Martinez, J. A., Rutledge, P. C., & Sher, K. J. (2007). Fake ID ownership and heavy drinking in underage college students: Prospective findings. *Psychology of Addictive Behaviors, 21*(2), 226–232.

McMahan, S., Witte, K., & Meyer, J. A. (1998). The perception of risk messages regarding electromagnetic fields: Extending the extended parallel process model to an unknown risk. *Health Communication, 10*(3), 247–259.

McShane, M. D., & Williams, F. P. (1992). Radical victimology: A critique of the concept of victim in traditional victimology. *Crime and Delinquency, 38*(2), 258–271.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*, 2366–2375.

Mosteller, J., Donthu, N., & Eroglu, S. (2014). The fluent online shopping experience. *Journal of Business Research, 67*(11), 2486–2493.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology, 36*(4), 829–857.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing E-commerce crime*. Devon, UK: Willan Publishing.

Ommundsen, Y. (2003). Implicit theories of ability and self-regulation strategies in physical education classes. *Educational Psychology, 23*(2), 141–157.

Osborne, J. (2005). Notes on the use of data transformations. *Practical Assessment, Research and Evaluation, 9*(1), 42–50.

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology, 21*(1), 55–71.

Pratt, T. C., & Cullen, F. T. (2000). Empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology, 42*(1), 111–136.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296.

Prentice-Dunn, S., McMath, B. F., & Cramer, R. J. (2009). Protection motivation theory and stages of change in sun protective behavior. *Journal of Health Psychology, 14*(2), 297–305.

Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM, 52*(4), 42–47.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of Internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369–384.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency, 50*(2), 216–238.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339–362.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*, 93–114.

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.

Salu, A. O. (2004). Online crimes and advance fee fraud in Nigeria. Are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159–167.

Schreck, C. J., Stewart, E. A., & Osgood, D. W. (2008). Reappraisal of the overlap of violent offenders and victims. *Criminology, 46*(4), 871–906.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). Study of individual and situational antecedents of violent victimization. *Justice Quarterly, 16*(1), 159–180.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior, 32*, 15–22.

STATISTA. (2015). *U.S. retail e-commerce sales*. Retrieved from http://www.statista.com/statistics/273424/retail-e-commerce-sales-in-the-united-states/.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*(1), 159–181.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). Boston: Pearson.

Taylor, D., Davis, D., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203–223.

Titus, R. (2001). Personal fraud and its victims. In N. Shover, & J. P. Wright (Eds.), *Crimes of priviledge: Readings in white-collar crime*. New York: Oxford University Press.

Töyssy, S., & Helenius, M. (2006). About malicious software in smartphones. *Journal in Computer Virology, 2*(2), 109–119.

Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers in Human Behavior, 51*, 180–187.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115–127.

Van Wilsem, J. (2013). 'Bought it, but never got it' Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168–178.

Van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization. *Journal of Contemporary Criminal Justice, 17*(4), 328–345.

Verma, R., Shashidhar, N., & Hossain, N. (2012). *Detecting phishing emails the natural language way Computer Security—ESORICS 2012* (pp. 824–841). Berlin, Germany: Springer.

Vowell, P. R., & Chen, J. (2004). Predicting academic misconduct: A comparative test of four sociological explanations. *Sociological Inquiry, 74*(2), 226–249.

Wikström, P.-O. H., & Treiber, K. (2007). The role of self-control in crime causation: Beyond Gottfredson and Hirschi's general theory of crime. *European Journal of Criminology, 4*(2), 237–264.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59*, 329–349.

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

Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. (2011). Electronic banking fraud: The need to enhance security and customer trust in online banking. *Advances in Information Sciences & Service Sciences, 3*(10), 505–509.

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.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior, 11*(6), 763–765.

Zahedi, F. M., Abbasi, A., & Yan, C. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems, 16*(6), 448–484.