Computers in Human Behavior 48 (2015) 199–207

Contents lists available at ScienceDirect

Computers in Human Behavior

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

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

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

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

ARTICLE INFO

Article history:

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

ABSTRACT

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

1. Introduction: The online safety problem

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

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

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

http://dx.doi.org/10.1016/j.chb.2015.01.046
0747-5632/

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

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

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

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

2. Theoretical framework

2.1. Motivating online protections

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

2.2. Protection motivation theory

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

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

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

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