Computers in Human Behavior 68 (2017) 359–367

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

Cyber-victimization preventive behavior: A health belief model approach

Matias Dodel[*, 1], Gustavo Mesch [1]

Department of Sociology, Faculty of Social Sciences, University of Haifa, Haifa, Israel

ARTICLE INFO

Article history:
Received 5 July 2016
Received in revised form
12 October 2016
Accepted 22 November 2016

Keywords:
Victimization
Safety
Preventive behavior
Health belief model
Security
Cybercrime

ABSTRACT

Cyber-victimization has extensive economic and personal consequences for Internet users as well as negative consequences for economies and the cyber infrastructure. This paper investigates the determinants of cyber-safety behaviors, particularly the factors associated with using anti-virus software in the general Internet user population, through a conceptual model about the determinants of non-digital preventive actions. We tested the Health Behavior Model, which considers perceptions about threats and expectations about behavior as the main determinants of health-related preventive behaviors, using a survey of Israeli Internet users 18 years old and older (N = 1850). Findings show that gender, age, education, seniority online and frequency of Internet use are basic determinants of anti-virus preventive behaviors. Nevertheless, similar to preventive health behaviors, beliefs about digital threats and actions to thwart them appear to account for more variance in anti-virus preventive behaviors than socio-demographic characteristics and Internet use. Our findings provide an innovative conceptual model and imply that the fight against cybercrime can take cues from health behavior studies demonstrating the role of perceptions and beliefs in reducing online threats. Furthermore, health behavior models are useful frameworks to conceptualize behavioral reactions to threats and to study cyber-safety.

1. Introduction

The vulnerability of mobile and Internet users to malware infections, phishing attempts and identity theft might have not only negative consequences for individual users but also cause substantial damage to the digital infrastructure and national economy (Anderson et al., 2013; McGuire & Dowling, 2013b). Cybercrime victimization has tangible outcomes for Internet users both directly and indirectly, as well as externalities for third parties. For individual users, direct impacts include threats to their digital assets, such as devices, network and software underperformance, forced access to private information, and unauthorized use of their financial assets (Clough, 2010). Indirect consequences are those that affect the users' social and affective life as well as the economies of businesses and organizations. For users, financial losses and the forced disclosure of private information can be extremely stressful and take a toll on their wellbeing (Liang & Xue, 2010). Additionally, exposure to cybercrime can inhibit e-banking, online shopping and other everyday activities (Bohme & Moore, 2012).

Internet users are conscious of potential cyber victimization risks. A study in Canada shows that 89% of Internet users report having anti-virus software, and 28% change their passwords at least once a year (Ekos Research, 2011). European Internet users are likely to have changed their behavior because of security concerns, with 38% indicating that they are less likely to give out personal information on websites and 49% refusing to open emails from unknown people (European Commission, 2014).

Of the many potential victims of cybercrimes, this study is concerned specifically with personal Internet users (PIUs), meaning individuals who use the Internet through their personal devices (as opposed to those who use the Internet through devices at work). Being a very heterogeneous group of users, not only do PIUs have fewer cyber safety guidelines than users in organizational settings but also their adoption of anti-malware software is not compulsory (Anderson & Agarwal, 2010; Kritzinger & von Solms, 2010). Network security tends not to be their main concern when using the Internet. PIUs want to satisfy their needs through the use of digital technologies and seem not to be aware of security until it becomes an issue (Dupuis, 2014). Thus, the study of the

* Corresponding author. Faculty of Social Sciences, University of Haifa, Mount Carmel, Haifa, 3498838, Israel.
E-mail addresses: matias.dodel@ucu.edu.uy (M. Dodel), gustavo@soc.haifa.ac.il (G. Mesch).
[1] Facultad de Ciencias Humanas, Universidad Católica del Uruguay. Av. 8 de Octubre 2738. CP 11600 Montevideo, Uruguay.

http://dx.doi.org/10.1016/j.chb.2016.11.044
0747-5632/

determinants of digital safety is a topic that deserves a more prominent place in research.

Whereas there is a consensus that cyber security threats are of concern and cybercrime's consequences are measured in billions of dollars (Anderson et al., 2013; McGuire & Dowling, 2013a,b), scholars have just recently come to understand that technologies alone are insufficient to ensure digital safety. Behaviors and social interactions are as crucial to cyber security as hardware or software (Liang & Xue, 2010, p. 395; Schultz, 2005, p. 426). Given that the adoption of preventive and protective measures is at its core a type of human behavior, the social sciences must become more involved in the conceptualization and study of cyber safety.

Cyber victimization research, while recent, is relatively extensive (i.e., Abawajy, 2014, p. 236; Bossler & Holt, 2009, p. 401; Pfleeger & Caputo, 2012, p. 597). Primarily based on the routine activities theory (Cohen & Felson, 1979), the cyber-victimization literature tends to focus on the proximities, available barriers or guardians and contexts in which cybercrime occurs. This emphasis leaves a gap in the conceptualization and modeling of behaviors to prevent cyber victimization.

We argue that the study of the determinants of such behaviors can benefit substantially from the application of models that originated in the health behavior literature (i.e., Ng, Kankanhalli, & Xu, 2009; Rhee, Kim, & Ryu, 2009; Rowe, Halpern, & Lentz, 2012). Behaviors that emerged from such studies seem to be analogous to those designed to prevent cyber victimization. Research has shown that as in the physical sphere, expectancies (subjective probabilities), perceptions and values related to digital threats and preventive courses of action are the most important determinants of preventive behavior in cyberspace (Claar, 2011; LaRose, Rifon, & Enbody, 2008; Liang & Xue, 2010). We continue this line of work and adopt concepts from the health behavior model as the core framework to assess cybercrime prevention behavior.

1.1. The nature of cybercrime

Of the vast group of offenses committed or facilitated through the use of digital technologies, we limit the scope of this study to one particular type of computer dependent cyber-threat: malicious software (McGuire & Dowling, 2013b). Popularly referred as malware, the term is used to describe a wide range of software designed to threaten the functionality, integrity and/or security of digital devices or networks (Rowe et al., 2012). Malware episodes are the most common negative experiences reported both in cyber-victimization surveys (i.e., 47% for European users in 2014, 15 points higher than the second victimization incident; European Commission, 2014) as well as computer security companies' reports (i.e., PandaLabs, 2014). Attacks are directed against different types of digital property such as personal data, digital currency or the control of devices, but can result in secondary outcomes such as using the data gathered to scam others, steal the users' identity or extort victims into releasing sensitive private information (McGuire & Dowling, 2013a; Yar, 2013).

While flawed software vulnerabilities will always be part of the mechanisms that cybercriminals use to disseminate malware, online delinquents also exploit particular types of human behaviors (Crossler et al., 2013). The lack of protection or safety measures can be understood as one key component of the latter and, thus, the determinants of these behaviors becomes an important research topic that merits attention.

Among the several theories developed to understand preventive behaviors, cognitive and value-expectancy preventive behavior models tend to be the most prominent in the literature. A leading model is the Health Belief Model, originally developed to explain the process of deciding to become vaccinated in the wake of the failure of immunization and screening programs in the US (Rosenstock, 1974). The next sections will detail the core constructs of the theory, both in the physical world and our adaptation to the cyber-safety arena.

1.1.1. Health behavior theories and the cognitive antecedents of preventive behavior

Health behavior models are considered some of the most developed frameworks for conceptualizing behavioral reactions to threats both in the physical sphere and online (DuBow, McCabe, & Kaplan, 1979; Ng et al., 2009). The focus is on the cognitive understanding of preventive health behaviors and viewing beliefs and expectations as their major determinants (Munro, Lewin, Swart, & Volmink, 2007). Cognitive health behavior theories are a group of related perspectives that argue that a small number of beliefs and attitudes are the best proximal determinants of preventive behavior. In this view, human beings are rational decision makers who weigh the costs of taking precautions against the benefits that might be obtained from them (Weinstein, 1987). They assume a limited version of rationality in which individuals are future oriented and assess the costs and benefits of a behavior but in a non-optimal way; they may hold incorrect beliefs and act on intentions based on old or false information (Ng et al., 2009; Sutton, 2001).

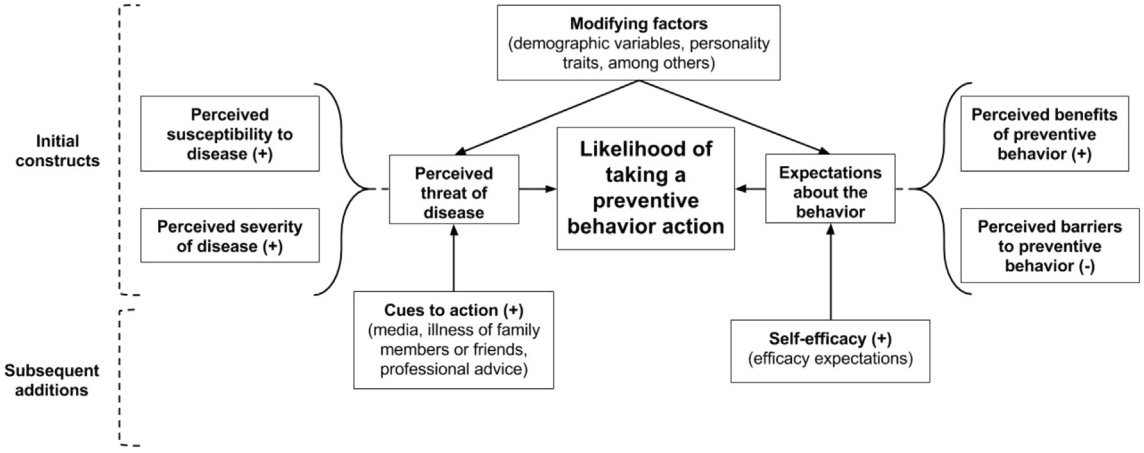

Fig. 1. The Health Belief Model as a predictor of health preventive behavior.
Source: Author's elaboration based on Rosenstock (1974); Rosenstock et al. (1988) and Champion and Skinner (2008).