Computers in Human Behavior 83 (2018) 32–44

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

The impact of information security threat awareness on privacy-protective behaviors

Stanislav Mamonov [a, *], Raquel Benbunan-Fich [b]

[a] Montclair State University, Department of Information Management and Business Analytics, Feliciano School of Business, 1 University Ave, Montclair, NJ 07043, USA

[b] Baruch College, CUNY, Information Systems and Statistics Department, Zicklin School of Business, One Bernard Baruch Way, Box B11-220, New York, NY 10010, USA

ARTICLE INFO

Article history:

Keywords:
Security
Privacy
Protective behaviors
Passwords
Self-disclosure

ABSTRACT

In this study, we examine how to motivate computer users to protect themselves from potential security and privacy threats. We draw on the Information Processing framework which posits that threat mitigation commonly occurs before full cognitive threat assessment and we conduct an empirical study to evaluate the effects of an exposure to general information security threats on the strength of passwords and the disclosure of personal information. Through an online experiment, we compare immediate computer user reactions to potential non-individually specific security and privacy threats in an extra-organizational context. We find evidence consistent with automatic security and privacy protective actions in response to these threats. Computer users exposed to news stories about corporate security breaches limit the disclosure of sensitive personal information and choose stronger passwords. The study complements the existing behavior modification research in information security by providing the theoretical and empirical foundation for the exploration of automatic security and privacy threat mitigation strategies across different contexts.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

Continued integration of technology into everyday life exposes technology users to growing security and privacy risks. According to a survey of Chief Information Officers by PricewaterhouseCoopers, 42.8 million security incidents were detected in 2016, showing a 48% increase over the previous year (PricewaterhouseCoopers, 2017). The economic impact of the security breaches is estimated at nearly half a trillion dollars globally (Ponemon Institute, 2017). Password breaches are one of the most common information security failures. Although there is a considerable body of research on the best practices in secure computing (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013; Yang & Tate, 2012; Zeng, Wang, Deng, Cao, & Khundker, 2012), companies continue to struggle with preventing password breaches. In 2015, the Central Intelligence Agency discovered that 47 government agencies, including the Department of Homeland Security, were compromised, giving the hackers access to over 21 million government employee accounts (Hirschfield Davi, 2015). Equifax, one of the three largest credit agencies, recently reported that it suffered a breach that affected 143 million consumers (McMillan & Knutson, 2017) and Yahoo announced that over three billion user accounts were impacted in the previously reported breach (Andriotis & McMillan, 2017). These events indicate that secure password selection and protection remains a problematic area of practice that merits further research.

News of security breaches feeds a parallel trend in modern society because they exacerbate concerns about potential privacy violations. Increased reliance on technology to store and communicate personally identifiable information exposes technology users to ever-growing privacy risks. Yet, researchers have found that, seemingly in contradiction to increasing privacy concerns, people continue to disclose ever-growing volume of personal information online (Barnes, 2006) and this trend shows no signs of slowing down. Recent social media statistics show that Facebook users share over 300 million images through the social network platform every day (Zephoria Digital Marketing, 2017). The growing frequency of security incidents along with the mounting volume of

* Corresponding author.
E-mail addresses: stanislav.mamonov@montclair.edu (S. Mamonov), rbfich@baruch.cuny.edu (R. Benbunan-Fich).

https://doi.org/10.1016/j.chb.2018.01.028
0747-5632/© 2018 Elsevier Ltd. All rights reserved.

technology-mediated information disclosure raises the question of how to motivate technology users to protect themselves.

Interdisciplinary research has established that people have two alternative information processing systems: automatic (fast) and effortful cognitive (slow) (Kahneman, 2011). The cognitive approach to motivating employee compliance with organizational security policies has been a central theme in Information System search (Sommestad, Karlzén, & Hallberg, 2015). However, little is known about the *automatic* reactions of technology users to immediate perceived privacy and security threats. We draw on the Information Processing (IP) framework (Beck & Clark, 1997), which emphasizes automatic threat mitigation in response to threatening stimuli and we conduct an experimental study to evaluate the effects of an exposure to information security threats on the strength of passwords and disclosure of personal information. We manipulate the exposure to information security threats by showing the participants different types of news stories. The control group is exposed to general technology-related news, while the treatment group is exposed to computer security breach related stories. For these two conditions, we evaluate the differences in two behavioral variables: the strength of passwords chosen by participants to protect their responses and the degree of refusal to answer personal questions in a self-disclosure survey.

2. Theoretical background and hypotheses

The focus of our study is on the automatic computer user reactions to potential security and privacy threats. We draw on the IP framework as the theoretical foundation for our study. The IP framework posits that threat mitigation often precedes full cognitive threat assessment (Beck & Clark, 1997). Before we discuss the automatic threat mitigation, we will review the established stream of research which has focused on a related question of how to motivate employee compliance with organizational security policies through cognitive persuasion. This stream of research evolved from the observation that organizational insiders are often responsible for the organizational security breaches (Zadelhoff, 2016). Promoting organizational security policy compliance is seen as a key factor in corporate security breach prevention.

Protection motivation theory (PMT), which was initially developed in health-related behavior modification research (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986; Rogers, 1975), has served as the focal theoretical foundation for the stream of research examining ways to persuade employees to adhere to organizational security policies (Sommestad et al., 2015). PMT research on health-related topics provided evidence that exposure to "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" can be effective in motivating behavior modification, e.g. in motivating people to quit smoking (Witte, 1992). PMT posits that perceived threat severity, perceived vulnerability, self-efficacy and response efficacy are the key factors that affect individual behavioral intentions (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986). Applying PMT to the organizational security policy compliance contexts, prior research has shown that fear appeals and threats of personal responsibility can have a positive effect on employee intention to follow organizational policies (Ifinedo, 2014; Johnston & Warkentin, 2015). However, the results have not been consistent across the studies. For example, a study of employee intention to comply with organizational security policies in the United States showed no significant effects of perceived threat severity or perceived threat susceptibility after considering the effects of perceived security policy legitimacy and organizational value congruence (Son, 2014). A recent study by Boss et al (Boss, Galletta, Lowry, Moody, & Polak, 2015). involving student reactions to malware threats similarly found no significant direct effects for perceived threat severity and perceived susceptibility on the behavioral intention. Contrary to the predictions of the PMT, Boss et al. (2015) also documented a negative effect of self-efficacy on the behavioral intention. Individually-relevant fear appeals are at the core of PMT because fear is believed to be the core emotion that motivates changes in attitudes and behavioral intentions (Floyd, Prentice-Dunn, & Rogers, 2000; Johnston, Warkentin, & Siponen, 2015). Recent neuroimaging studies have further challenged PMT assumptions in information security research by showing that computer security-related warnings commonly fail to produce activation in the brain regions associated with fear (Warkentin, Johnston, Walden, & Straub, 2016).

In addition to the inconsistencies concerning the effects of the core PMT constructs in information security research, there has also been very little work on examining actual user behaviors using objective security-related behavior measures. The majority of studies applying PMT to examine organizational security policy compliance have been limited to measuring respondents' intentions (Sommestad et al., 2015). The studies that did measure security policy compliance have generally relied on self-reports. The only study which measured PMT constructs and actual behaviors did so measuring behaviors first and PMT constructs second, thus undermining the interpretation of the results on the effects of PMT constructs in motivating the behaviors (Boss et al., 2015). A summary of security policy compliance studies that include compliance behavior measures is presented in Appendix A1. Prior research has shown that self-reports can be unreliable in security (Sonnenschein, Loske, & Buxmann, 2016) and privacy-related (Barnes, 2006) contexts. Hence, the question of whether fear appeals can be effective in promoting actual user compliance with the organizational security policies remains open. Technology-mediated personal information disclosure also exposes the users to privacy risks. Self-disclosure has similarly been extensively studied in Information Systems, yet the vast majority of studies have relied on self-reports to assess individual self-disclosure. Li, Lin, and Wang (2015) exemplify a parallel approach to evaluating self-disclosure which relies on the analysis of secondary data, e.g. information that people share in social networking sites. There has been little in the way of experimental evidence on factors that may affect self-disclosure. A summary of recent studies involving evaluation of different factors that affect self-disclosure is provided in Appendix A2. In the present study, we seek to address the relative lack of knowledge about actual security and privacy-related user behaviors by examining automatic responses that occur following the exposure to information about the potential threats. To this end, we apply the IP framework proposed by Beck and Clark (1997) to lay the theoretical foundation for our study. The IP framework posits that the behavioral response to a threat often precedes cognitive assessment of the potential hazard. These predictions have been confirmed in individual psychology (Zajonc, 1980) and in marketing (Obermiller & Spangenberg, 1989). This framework is suitable to evaluate users' actions from a pragmatic perspective. Due to the time pressures of modern life, people are often motivated to make split-second decisions that simply do not leave much room for cognitive evaluation. This may occur, for example, when a user is requested to specify a new password or is prompted with a request for personal information online.

The IP framework posits that threat-related information processing consists of three stages: automatic threat detection, focusing of attentional resources towards goal-directed activities,

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات