UNDERSTANDING INDIVIDUALS' INSECURE BEHAVIOR: FACTORS AFFECTING THE DECISION TO REFUSE THE ADOPTION, USE, OR EXPANDED USE OF PROTECTIVE INFORMATION TECHNOLOGY

Piia Perälä
University of Jyväskylä, Finland

Tiina Koskelainen
University of Jyväskylä, Finland

Mikko Siponen
University of Jyväskylä, Finland

Abstract

In recent years, the need for protecting Internet-connected devices has increased as the number of Internet-connected devices has risen in households. Despite the increased need, some individuals still refuse to run protective information technologies (PIT) for security on their Internet-connected devices. This paper focuses on individuals' insecure behavior and discusses reasons for the refusal of adoption, use, and extended use of PIT. This study identifies 14 factors affecting an individual's decision to refuse. These factors can be linked to individual stages of security behavior, or different stages can share similar kinds of factors. The results of this study provide a deeper understanding of individuals' reasons to refuse PIT in different stages of security behavior and could be utilized in the product development and marketing of information security products in order to improve user engagement.

Keywords: security behavior, information security, Internet security technology, empirical research

JEL code: O33

1. Introduction

The number of Internet-connected devices is continually increasing in households. The diffusion of mobile devices, such as smart phones and tablet computers, has been especially fast in recent years. People are using these Internet-connected devices more and more to handle daily matters, such as banking services, and therefore, there is an increasing need to protect individuals' Internet security in a home context. However, it was found that individuals do not necessarily protect their mobile devices (Han, Wu and Windsor, 2014).

Previous information systems security research has focused mostly on explaining users'

insecure behaviors in an organizational context (Bulgurcu, Cavusoglu and Benbasat, 2010; Dinev and Hu, 2007; Dinev et al., 2009; Johnston and Warkentin, 2010; Lebek et al., 2014; Siponen, 2001; Siponen, Mahmood and Pahnila, 2014; Son, 2011). In recent years, scholars have been increasingly interested in home computer users' security behavior (Anderson and Agarwal, 2010; Claar and Johnson, 2012; Han et al., 2014; Kumar, Mohan and Holowczak, 2008; Liang and Xue, 2009; 2010). However, research concentrating on individuals' security behavior in a home context is still rare compared to research focused on organizational context.

This paper reports the findings from an empirical study that was conducted as part of a research project aimed at understanding individuals' security behavior when they are using different protective information technologies (PIT) in a home context. The study addresses the issue of insecure behavior and provides an understanding of why individuals refuse to adopt, use continuously, or expand the use of PIT for Internet security.

2. Methodology

This empirical study focused on understanding individuals' insecurity behavior. It has identified factors affecting individuals' decisions to refuse the adoption, use, and expanded use of PIT for Internet security (e.g., protection against malware and viruses, etc.) in various devices such as desktops, laptops, tablet computers, and smartphones. The research was supported by a Finnish information security company, which provided the PIT and licenses, and funded by the Finnish Funding Agency for Innovation and the Strategic Center for Science, Technology, and Innovation (SHOK).

A case study theory structure (Eisenhardt, 1989) was selected as the research approach in order to understand the reasons and context for the use of PIT (Myers, 2013). The data was collected by semi-structured interviews following Myers and Newman's (2007) guidelines for qualitative research interviews.

In total, 28 Finnish individuals—18 men and 10 women with a mean age of 41.6 years—participated in this study concerning the use of the technology for Internet security. Simple sampling was used (Patton, 2002, p. 243), as participants were picked randomly from the streets of two cities in Finland between August 2015 and September 2015. All participants had some experience using information security technologies to protect their Internet security, at least in their personal computers.

The study was conducted as a longitudinal study. During the study period, participants used PIT for Internet security for approximately six months. With one license code, the participant obtained access to use the PIT in 10 devices in the household.

During the study, three rounds of interviews were conducted by two researchers. The first interview occurred at the beginning of the study, the second in the middle of the study, and the

last at the end of the study. These interviews aimed to gather knowledge about individuals' previous security behavior, as well as behavior and experiences related to the use of PIT in the study setting. The interviews were done by phone and recorded with the participants' permission. The research data (recorded interviews) were transcribed into text format for data analysis.

The data was analyzed in two ways, and the nature of the analysis was iterative. First, the security behavior of each participant was analyzed as a case. The aim of the case analysis was to get an overall understanding about the individual's security behavior during the time period under consideration, as well as to explore different stages related to the adoption, use, and rejection of the technology during the use of PIT. Next, a data-driven content analysis was performed in order to map constructs to the stages. The transcribed interviews were analyzed by inductive content analysis (Weber, 1990), with the units of analysis concerning the participants' decision to refuse to adopt, use continuously, or expand use of the technology. The data analysis was done in three phases—initial analysis, initial categorization of semantic units, and higher-level categorization—by using ATLAS.ti software.

3. Results

The main result of the study was the identification of factors that can be linked to individuals' security behavior leading to the refusal to adopt, use, or expand use of PIT. Individuals' security behavior is seen as a process comprising three stages: decision to adopt, adoption, and use. During these stages, a person makes decisions about the adoption and continuance of technology use, as well as the expansion of use to other devices in the household. All three stages contain stage-specific processes (Weinstein, Rothman and Sutton, 1998) that the user undergoes. Depending on the stage, the process results in either moving to the next stage or staying at the current stage. Refusal is seen as the end state, as the individual has quit the use of PIT or refused to adopt or expand the use to other devices in the household. Refusal can happen at any of these stages.

In the first stage (decision to adopt), the individual decides whether or not to adopt the PIT. Following that, in the second stage (adoption), the individual gets access to installation, performs the installation, and gets the first impression of the PIT. Finally, in the third stage (use), the individual is actually using and interacting with the PIT. Figure 1 depicts the stages of security behavior.

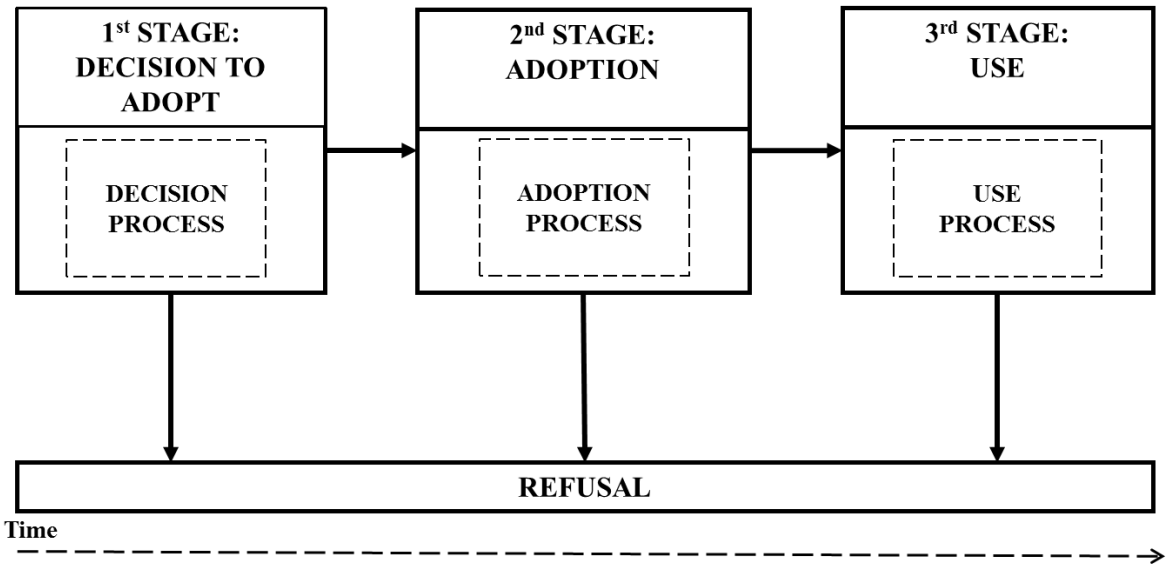

Figure 1. The stages of secure behavior

The study found that refusal can happen in any stage and can be caused by different factors. The refusal of adoption happens in the first stage, whereas the refusal of the continuous or expanded use requires some experience and interaction with the technology, and therefore, refusal also happens in the stages concerning adoption (stage 2) or use of the technology (stage 3). The occurrence of factors affecting refusal can depend on a specific stage (i.e., distinct factors), or different stages can share similar kinds of factors (i.e., shared factors). For example, the refusal of adoption (stage 1) can be caused by stage-dependent factors as well as factors similar to those that cause the refusal of expanded use (stages 2 and 3).

Factor identification revealed the existence of 14 factors—nine shared factors and five distinct factors. Two shared factors were found to cause the refusal of use and expanded use—"negative use experience" and "uselessness." Seven shared factors affected the refusal of adoption and expanded use: "carelessness," "assumed harm," "assumed invulnerability," "device's ownership," "own competence," "OS unsupportiveness," and "threat experience."

Identification of the distinct factors showed that "costs" and "no protection requirement" were factors that caused refusal of adoption. "Prevention of use" was a factor that caused refusal of use. Refusal of expanded use was caused by two distinct factors—"use of another protective information technology" and "others' competence." Definition and examples of shared and distinct factors are presented in Table 1 and Table 2.

Table 1. Shared factors causing the refusal of PIT

Shared factor	**Causing**	**Definition**	**Example**
Negative use experience	Refusal of use and extended use	Individual's negative experience about interaction with the PIT	Individual has faced problems with installation process or use.
Uselessness	Refusal of use and extended use	Individual's experience that use of the PIT is useless	Individual believes in the capability of the device or its operating system to protect itself against security threats.
Carelessness	Refusal of adoption and expanded use	Individual's carelessness about security threats or protection against threats	Individual does not care about security threats or is not motivated to install and use PIT.
Assumed harm	Refusal of adoption and expanded use	Individual's assumption that use of the PIT harms use of the device	Individual assumes that the PIT will slow down the operating speed of the device.
Assumed invulnerability	Refusal of adoption and expanded use	Individual's belief that the user or user's device are not considered a possible target of security threats	Individual believes s/he is invulnerable to security threats because the device, use context, or use purposes are deemed safe.
Device's ownership	Refusal of adoption and expanded use	Individual's relationship to the owner of the device	The device is owned by a partner, or the individual must comply with an employer's security policies that deny the installation of applications to employer-owned devices.
Own competence	Refusal of adoption and expanded use	Individual's competence to control own browsing and Internet use behavior	By controlling browsing behavior, the individual assumes that s/he does not encounter security threats.
OS unsupportiveness	Refusal of adoption and expanded use	Individual's assumption that the device does not support the use of PIT	The operating system does not support the use of certain PIT.
Threat experience	Refusal of adoption and expanded use	Individual's inexperience with security threats	The individual has not faced problems with security threats.

Table 2. Distinct factors causing the refusal of PIT

Distinct factor	**Causing**	**Definition**	**Example**
Prevention of use	Refusal of use	Individual's inability to use the protective technology	Individual has lost his/her device or does not use it anymore.
Costs	Refusal of adoption	Individual's monetary cost for use of the PIT	Individual is not willing to pay for the protection.
No protection requirement	Refusal of adoption	Individual's use of PIT not required by external party	Employer does not require employees to use PIT.
Use of another protective technology	Refusal of expanded use	Individual's use of another PIT on device(s) in the household	Devices in the household run on another PIT.
Others' competence	Refusal of expanded use	Individual's belief that persons in the household do not use devices in a way that causes security threats.	Individual believes that his/her kids are aware about security threats when browsing the Internet.

The secondary result of this study found that the device type can be linked to an individual's security behavior. In the study, every participant had some experience with using technology to protect his or her Internet security, at least on personal computers. However, the study showed that even when the individual has protected a personal computer, s/he has not necessarily protected mobile devices such as tablets or smartphones.

4. Conclusion

Individuals' security behavior can be observed in stages. In these stages, different factors play a role in affecting the individual's insecure behavior concerning the refusal of PIT. These factors are not necessarily similar in different stages of secure behavior. The study found that the nature of the factors affecting the decision to refuse PIT can be stage-specific or shared among different behavioral stages.

Previous research has shown that individuals' awareness and trust are factors that affect behavioral intention to adopt PIT (Dinev and Hu, 2007; Han et al., 2014). However, this study showed, especially in situations of insecure behavior, that the incidence of several factors can affect an individual's decisions concerning security behavior. In addition, the study showed that factors affecting insecure behavior can change over time as the individual moves from one behavioral stage to another.

Based on these results, further research should concentrate on studying the nature and content of factors affecting individuals' security behavior, as well as how the type of device could affect users' security behavior in a home context.

The results of this study can be utilized in the product development and marketing of information security products in order to improve user engagement. For example, product

engagement could be improved by decreasing the occurrence of factors causing refusal of the information security product.

References

Anderson, C. L. and Agarwal, R. (2010) "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, vol. 34, no. 3, pp. 613–643.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, vol. 34, no. 3, pp. 523–548.

Claar, C. L. and Johnson, J. (2012) "Analyzing home PC security adoption behavior", *Journal of Computer Information Systems*, vol. 52, no. 4, pp. 20–29.

Dinev, T. and Hu, Q. (2007) "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the Association for Information Systems*, vol. 8, no. 7, p. 386.

Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009) "User behaviour towards protective information technologies: the role of national cultural differences", *Information Systems Journal*, vol. 19, no. 4, pp. 391–412.

Eisenhardt, K. M. (1989) "Building theories from case study research", *Academy of Management Review*, vol. 14, no. 4, pp. 532–550.

Han, B., Wu, Y. A. and Windsor, J. (2014) "User's adoption of free third-party security apps", *Journal of Computer Information Systems*, vol. 54, no. 3, pp. 77–86.

Johnston, A. C. and Warkentin, M. (2010) "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, pp. 549–566.

Kumar, N., Mohan, K. and Holowczak, R. (2008) "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls", *Decision Support Systems*, vol. 46, no. 1, pp. 254–264.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014) "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, vol. 37, no. 12, pp. 1049–1092.

Liang, H. and Xue, Y. (2009) "Avoidance of information technology threats: a theoretical perspective", *MIS Quarterly*, pp. 71–90.

Liang, H. and Xue, Y. (2010) "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems*, vol. 11, no. 7, p. 394.

Myers, M. D. (2013) *Qualitative research in business and management,* Sage.

Myers, M. D. and Newman, M. (2007) "The qualitative interview in IS research: examining the craft", *Information and Organization*, vol. 17, no. 1, pp. 2–26.

Patton, M. Q. (2002) *Qualitative research and evaluation methods*, Thousand Oaks: Sage.

Siponen, M. T. (2001) "On the role of human mortality in information system security: from the problems of descriptivism to non-descriptive foundations", *Information Resources Management Journal*, vol. 14, no. 4, p. 15.

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, vol. 51, no. 2, pp. 217–224.

Son, J. Y. (2011) "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies", *Information and Management*, vol. 48, no. 7, pp. 296–302.

Weber, R. P. (1990) *Basic content analysis*, (No. 49). Sage.

Weinstein, N. D., Rothman, A. J. and Sutton, S. R. (1998) "Stage theories of health behavior: conceptual and methodological issues", *Health Psychology*, vol. 17, no. 3, p. 290.