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.
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

<table>
<thead>
<tr>
<th>Shared factor</th>
<th>Causing</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative use experience</td>
<td>Refusal of use and extended use</td>
<td>Individual’s negative experience about interaction with the PIT</td>
<td>Individual has faced problems with installation process or use.</td>
</tr>
<tr>
<td>Uselessness</td>
<td>Refusal of use and extended use</td>
<td>Individual’s experience that use of the PIT is useless</td>
<td>Individual believes in the capability of the device or its operating system to protect itself against security threats.</td>
</tr>
<tr>
<td>Carelessness</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s carelessness about security threats or protection against threats</td>
<td>Individual does not care about security threats or is not motivated to install and use PIT.</td>
</tr>
<tr>
<td>Assumed harm</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s assumption that use of the PIT harms use of the device</td>
<td>Individual assumes that the PIT will slow down the operating speed of the device.</td>
</tr>
<tr>
<td>Assumed invulnerability</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s belief that the user or user’s device are not considered a possible target of security threats</td>
<td>Individual believes s/he is invulnerable to security threats because the device, use context, or use purposes are deemed safe.</td>
</tr>
<tr>
<td>Device’s ownership</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s relationship to the owner of the device</td>
<td>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.</td>
</tr>
<tr>
<td>Own competence</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s competence to control own browsing and Internet use behavior</td>
<td>By controlling browsing behavior, the individual assumes that s/he does not encounter security threats.</td>
</tr>
<tr>
<td>OS unsupportiveness</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s assumption that the device does not support the use of PIT</td>
<td>The operating system does not support the use of certain PIT.</td>
</tr>
<tr>
<td>Threat experience</td>
<td>Refusal of adoption and expanded use</td>
<td>Individual’s inexperience with security threats</td>
<td>The individual has not faced problems with security threats.</td>
</tr>
</tbody>
</table>
### Table 2. Distinct factors causing the refusal of PIT

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

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


