2013

Are You Annoyed? The Effects of Mobile Device User Interface and Intrusiveness of Security Notifications on User Security Perceptions

Gregory Moody
University of Nevada, Las Vegas, gregory.moody@unlv.edu

Dezhi Wu
Southern Utah University, wu@suu.edu

Are You Annoyed? The Effects of Mobile Device User Interface and Intrusiveness of Security Notifications on User Security Perceptions

Gregory D. Moody
Management, Entrepreneurship & Technology Department
University of Nevada, Las Vegas
gregory.moody@unlv.edu

Dezhi Wu
Computer Science & Information Systems Dept.
Southern Utah University
wu@suu.edu

ABSTRACT

Research on the behavioral-based security of information systems within organizations and for personal use has been common over the last decade, however little is known regarding how individuals perceive the security of their mobile devices. This study seeks to explore how the security notifications within a mobile application environment alter adoption and security-related beliefs concerning their device. We proposed a theoretical model based on the technology adoption and psychological theories, and conducted a set of controlled experiments with 351 subjects in six US universities. A structural equation modeling technique was utilized to examine the overall research model. The data analysis results demonstrate that the majority of our proposed hypotheses were significant. We find that disruptive mobile security notifications cause user irritation, which negatively impacts user perception about mobile security. Mobile device user interface also has compounding effects on users' perceived usefulness and security with mobile devices.

Keywords

Mobile Security, Mobile Interface Design, Security Notifications, User Irritation, Security Awareness, HCI.

BACKGROUND

The adoption of mobile devices continues at an unprecedented rate throughout the world. Only recently has researched begun to focus on the security awareness of users in regards to their devices. Research has shown that users are unaware of the risks that these devices pose to their own personal information. **T**herefore, mobile devices have become a new target for security attacks, which pose serious threats to the security of such devices (Distefano et al. 2010), to individual users (Oberheide and Jahanian 2010), and to organizations when used and transported outside of their physical organizational boundaries (Halpert 2004).

At the individual user level, mobile user experiences are increasingly enriched by various mobile applications customized for different mobile devices. However, mobile applications can be a double-edged sword, which can cause serious security risks and threats to individual users. Research (Oberheide and Jahanian 2010) points out that users are not fully aware of the potential damage to their personal assets and private information saved in their mobile devices as they may be conditioned to the process of installing malicious mobile application. It is unclear how much users are aware of their mobile security settings, and how they should take proper actions to effectively protect their assets saved in mobile devices. Therefore, this research focuses primarily on the security awareness of mobile users as an initial project to explore how to increase the security of mobile devices through the use of security notifications to increased perceived perceptions of privacy and security. More specifically, we focus on mobile usability issues associated with mobile devices to examine users' awareness and ability to respond to various mobile security notifications.

RESEARCH HYPOTHESES

We begin by building on the Apple Usability Guidelines and the technology adoption model to propose how the interface of a mobile device impacts users' intentions to continue to use the device. Next, we explore how security notifications pushed to the user due to application of device operations may interrupt the cognitive processing of the individual and cause a sense of irritation. This builds upon the work by McCoy et al. (2008) by extending their web-based premises and manipulations to the mobile operating system context.

The initial hypotheses are an extension of the Technology Adoption Model (Davis 1989) to mobile devices, which has been previously validated (Cyr et al. 2006). As the users' main interactions with a mobile device are based on the graphical interface of the device (Hoehle 2013), it becomes the predominant antecedent of the ease-of-use for the device. We thus replicate prior research and propose:

H1: The mobile device user interface consisting of mobile application graphics, user interface input, output and structure will be positively related to the perceived usefulness / ease-of-use of the device.

H2: The perceived usefulness / ease-of-use of the mobile device will be positively related to the intention to continue to use the device.

Unlike computer operating systems and environments, mobile devices do not have built in security applications that provide dashboards regarding the relative security of the device. Rather, users are notified regarding any changes or requests by applications relative to private or secure information through the means of notifications. How these notifications are delivered to the user is determined by the interface of the mobile device. We thus posit that the awareness of the device's mobile security is primarily engendered through such notifications as afforded through the interface of the mobile device.

H3: Devices that are perceived as having superior user interfaces will be positively related to higher perceptions of mobile device security.

We propose that within application notifications are similar to pop-up and in-line ads present on the websites. We thus extend the work of McCoy et al. (2008) that when such notifications are perceived to be more repetitive will have the potential of being perceived as being more intrusive. Constant repetition of the same information, or same type of notification is likely to disrupt the cognitive flow of information that an individual requires when focusing on a task. We thus extend this prior line of reasoning and research to the context of mobile security notifications and propose:

H4: The perceived intrusiveness of notifications will be positively related to the perceived irritation afforded by such notifications.

Building on psychological theories of attitude change, we pose that as negative emotions regarding the mobile device are increased, that intentions or perceptions regarding the device will also be negatively impacted (Petty and Wegener 1998). Specifically, as the user becomes irritated with the security notifications, it is likely that these feelings will negatively impact the perceptions of the ease-of-use and usefulness of the device, which will negatively impact the intention of the user to continue to use the device. However, the engenderment of irritation will potentially positively impact perceptions of security. Irritation will likely raise the salience of cues regarding the security of the device, and provide the user with a sense of control over their data and their device, and thus increase the perceptions of security. We thus propose that feelings of irritation caused by the security notifications will produce the following outcomes:

H5: Feelings of irritation caused by the security notifications will negatively impact the perceptions of usefulness/ease-of-use, the intention to continue to use, and security perceptions of the mobile device.

Finally, although practitioners have long proposed that security is at odds with the general day-to-day usage of an application, we formally test this assumption. Thus, we propose:

H6: As the perceived security of the mobile device increases that the user will have weaker intentions to continue to use the device.

RESEARCH METHODOLOGY

Study Design

We intend to assess our hypotheses through the means of a 2 (high vs. low threatening conditions) x 3 (highly disruptive, moderately disruptive and no notifications treatment groups) randomized experiment with mobile phones. In the highly disruptive treatment condition, users would be exposed to push notifications during the process of the experiment that alerts them to security violations. The user would be unable to perform any other task until they first read through the entire violation and then approve or disapprove of such an action. They would then be returned to the screen that they had been using. In the moderate disruptive notification, the user would receive a push notification that is minimally inserted into their view, but does not obstruct or interfere with the tasks that the user is currently working on. Rather it would simply notify of the violation, and not require any interaction on the part of the user. In the no disruption condition, we would allow the user to complete tasks as specified by the experiment, and they would never receive any notification of any security violation. This would serve as the control condition to ascertain how much variation in our model is simply caused by the notification process.

In order to examine our research, we designed and implemented a mobile security notification system that can be run in various mobile phones.

Data Collection

We were able to recruit 351 users from six universities in the United States. The incentive for participating in this study was to earn 5 extra points for a particular course. The whole experiment took users about 15-20 minutes. After the users completed the experiment using a mobile smartphone, they were asked to fill out an online questionnaire that assesses common demographic controls and items to assess the constructs of interest in this study.

Measures

After investigating possible validated constructs from existing theoretical and empirical literature, we were able to obtain the reliable measurement items based on scales in prior literature (Hoehle 2013, Venkatesh et al. 2003, Anderson and Agarwal 2010, McCoy et al. 2008). All construct items were measured reflectively with multiple items on seven-point Likert scales.

PRELIMINARY DATA ANALYSIS RESULTS

We did some preliminary frequency and factor analyses on the data we collected. We also tested discriminant validity and reliability, which reached satisfactory levels. The majority of hypotheses were significantly supported. Some confounding effects were found and are briefly discussed in the next section.

DISCUSSIONS

Mobile devices are becoming a way of life around the globe. While the development of more applications, and the adoption by more users increases the incentives for users to also adopt, there is little research exploring how users can be made aware of the potential security issues and problems inherent in such devices. Whereas most users are aware of virus, malware and other such dangerous software on their personal computers and laptops, very few are aware of similar threats on their mobile devices.

This is an initial study that examines an adoption-based theoretical model to explore how the interface notifications impact the perceptions of security, and the intention to continue to use the device. We conducted a laboratory experiment, using mobile device users on their own devices, in which they were exposed to differing levels of security-related notifications and varying levels of security-related threats. Our current data results indicate that mobile user interface significantly impacts user perception of security and perceived usefulness. Among four key mobile interface components including graphics, input, output and structure, it turns out mobile user interface structure plays a key role of affecting user perception on mobile application usefulness and perceived security. This finding further indicates the importance of a good overall interface structure in mobile devices. Another important interface element significantly impacts user perception about security is mobile interface input. We found that user interface input has a significant positive impact on perceived security with mobile devices. More importantly, through our controlled experiment, we found that disruptive mobile security notifications can cause user irritation, which has a significant negative effect on perceived security. Therefore, our study informs more challenges how to increase users' mobile security awareness with proper user interface design and reduce user irritation while interacting with their mobile devices.

Since we just performed preliminary data analysis to test research hypotheses, more in-depth data analyses are needed to further explore how exactly different levels of security notifications affect user security perceptions and what we can do to improve mobile user interfaces in order to increase individual users' mobile security awareness.

We propose several important contributions for research in practice, with the most important being a call to focus on mobile-based security research. This area of security in regards to information technology is lacking, which is an appalling condition given the lack of awareness that exists in the general populace. We also note that this would be the first study to explore how the interface of the mobile device is able to impact perceptions of security, and likewise how the perceptions of security on the device impact the user's intention to continue to use the device.

REFERENCES

1. Anderson, C. L., and Agarwal, R. (2010) A multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, 34, 3, 613-643.
2. Cyr, D., Head, M., and Ivanov, A. (2006) Design aesthetics leading to m-Loyalty in mobile commerce, *Information & Management*, 43,8, 950-963.
3. Davis, F. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13, 3, 319-340.
4. Distefano, A., Grillo, A., Lentini, A., and Italiano, G.F. (2010) SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle, *In the CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 27, 1-4.
5. Halpert, B. (2004) Mobile device security, *Proceedings of InfoSecCD Conference*, Kennesaw, GA.
6. Hoehle, H. (2013) Mobile application usability: Conceptualization and instrument development, *MIS Quarterly*, in press.
7. McCoy, S., Everard, A., Polak, P., and Galletta, D.F. (2008) An experimental study of antecedents and consequences of online ad intrusiveness, *International Journal of Human-Computer Interaction*, 24, 7, 672-699.
8. Oberheide, J. Jahanian, F. (2010) When mobile is harder than fixed (and vice versa): Demystifying security challenges in Mobile Environments," *Proceedings of the Eleventh International Workshop on Mobile Computing Systems and Applications*, February 22, 2010, Annapolis, MD, USA.
9. Petty, R.E., Wegener, D.T. (1998) Attitude change: Multiple roles for persuasion variables, In: Gilbert, D.T., Fiske, E. Lindzey, G. (eds.), *The Handbook of Social Psychology*, Volume 1, McGraw-Hill, New York, NY: USA, 323-390.
10. Venkatesh, V., Morris, M., Davis, G., and Davis, F. (2003) User acceptance of information technology: Toward a unified view," *MIS Quarterly*, 27, 3, 425-478.