ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #37257

An analysis of differences in behaviors and practices of security-conscious users and regular users on mobile devices.

Stephen Mujeye

Dr. Stephen Mujeye an Assistant Professor of Computer Systems Technology at Illinois State University, Normal, Illinois. He earned a bachelor's degree with a double major in Business Management and Business Systems Support Specialist from Siena Heights University, Adrian, Michigan. He has a master's degree in Information Resource Management from Central Michigan University, Mt. Pleasant, Michigan. He completed his Ph.D. in Information Systems from Nova Southeastern University. His Ph.D. dissertation was titled "An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity." He holds several industry certifications, including A+, Network+, CCNA, and CCNA Security. His areas of research interest are authentication methods, cyber security, mobile and network security.

An analysis of differences in behaviors and practices of security-conscious users and regular users on mobile devices.

[Research in Progress]

Abstract

Mobile devices are widespread worldwide; individuals increasingly use their mobile devices to check emails, online banking, social media, etc. Previous studies have shown, however, that mobile devices have specific weaknesses and vulnerabilities to security. Security attacks for mobile users have also been on the increase. In this work-in-progress study, we seek to investigate the differences in security-conscious and regular users' behaviors and practices on mobile devices. A descriptive research methodology will be developed, utilizing two groups of participants (security-conscious and regular users) to address the study's objective. Participants will be selected from students at Illinois State University. The data will be analyzed using the multivariate analysis of variance. The analysis will reveal if differences are present in the behaviors and practices of security-conscious users and regular users. The results will help in recommending the best behaviors and practices for mobile device users, thereby increasing mobile device security.

Keywords: mobile devices, mobile security, security-conscious, ransomware, cybersecurity

Introduction

The use of mobile devices has been on the increase over the years (Fernando, 2019). Mobile devices are used for various activities, including checking emails, online banking, schoolwork, and work activities. Chin et al. (2020) pointed out that 266 million people used smartphones in the US in 2019. Meanwhile, 70% percent of the world's population used mobile devices in 2019. As mobile devices have become powerful and pervasive computing tools, they have become preferred over desktop computers. Mobile devices comprise cell phones and tablets, while desktop computers include laptops. Mobile devices are preferred over desktop computers because of their accessibility and convenience. Figure 1 shows a comparison of global mobile device users and desktop users.

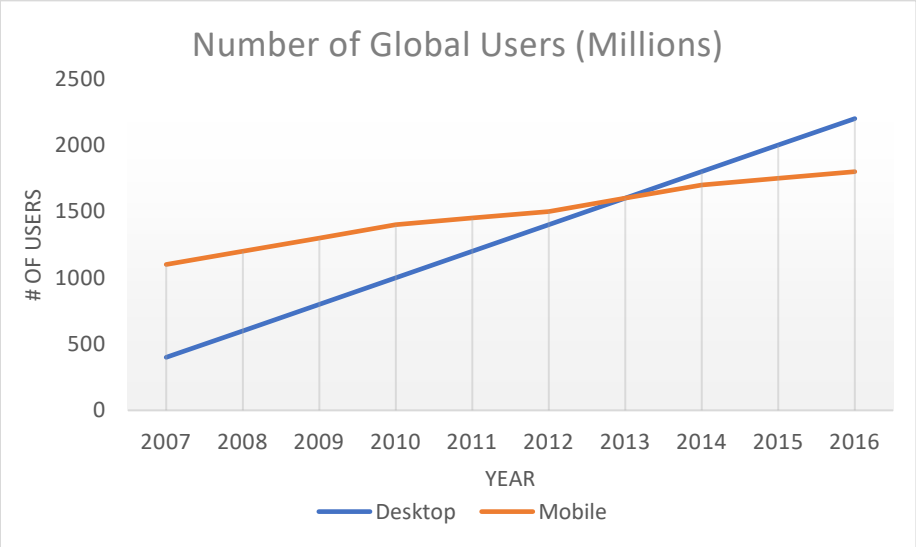

Figure 1. Desktop and mobile user comparison.

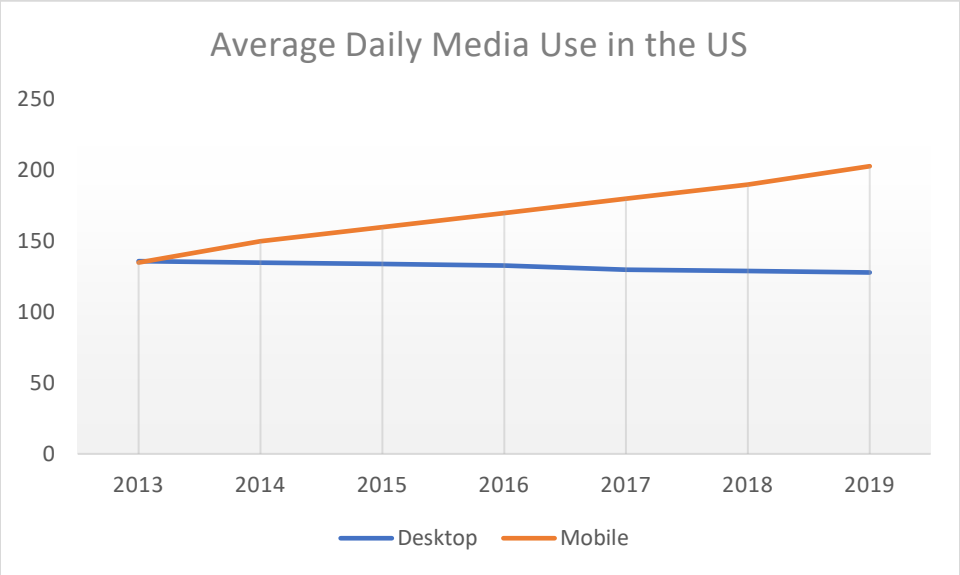

Figure 2. Average daily media use in the US.

On the other hand, Figure 2 shows the average daily media usage on desktop/laptop computers compared to mobile devices in the US.

Giwah (2019) pointed out that mobile devices continue to change and transform how people conduct business. While they are convenient for users, mobile devices, and ultimately mobile users, they face data theft and other breaches. The breaches are greatly attributed to the user's failure to conform to the best mobile device security policies and practices. The user's behavior is therefore incredibly connected to the security of mobile users. Mobile devices are considered to have more risk when compared to other computing systems; mobile device size makes it convenient for users to carry around, which further exposes the devices to risk and breaches. Ransomware, which comes as a piece of malware that seeks a ransom from users for profit after locking the device or encrypting the data, has been on the rise on mobile devices (Hu, 2020). In 2017, it was estimated that 48 million apps were downloaded per day, and ransomware cybercriminals are shifting their attack efforts towards mobile device users (Lachtar, 2019). Crespo (2020) pointed out that security threats are not going away, they are ever-pervasive, and they are an ongoing problem. The number of personal computers and mobile computers with publicly available applications continues to rise (Carstens, Mahlman, Miller & Shaffer, 2019). It is estimated that $48 billion was lost in 2018 due to security breaches and incidents (Wang, Yang, & Wan, 2020).

Previous research studies investigated how users view mobile security. Wolf, Kuber, Aviv (2018) conducted an explorative qualitative study to understand the motivations and practices of highly security-conscious users as they access their mobile devices. The study targeted one group of users only and focused on accessing the devices. The results revealed that highly security-conscious users were concerned with the usability of mobile devices and their identity while using the devices.

McGill and Thompson (2017) performed a study in which they analyzed users' security perceptions and behaviors on both home computers and mobile devices. The study indicated that users' behaviors on mobile devices put them at more risks when compared to the home computer. They propose the need for users' perceptions of security threat severity on mobile devices to shift.

McDonough (2018) developed some recommendations for mobile users to protect their devices from 'bad actors.' Some suggestions about good decisions and behaviors regarding protecting users and their data on mobile devices are suggested.

While prior studies have attempted to address mobile device security, none have compared the behaviors and practices of security-conscious users and regular users on mobile devices. Therefore, the goal of this study is to gain a better insight into the differences in behaviors and practices of users with different experiences on mobile devices.

Objectives

This research investigates the differences in behaviors and practices of security-conscious users and regular users on mobile devices. Based on prior research and the author's ongoing work in this area, the following hypotheses will guide this study (noted in null layout):

H1 There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices

H1a There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age

H1b There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender

H2 There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices

H2a There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age

H2b There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender

H3 There will be no significant differences in *data backup and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices

H3a There will be no significant differences in *data backup and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age

H3b There will be no significant differences in *data backup and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender

H4 There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices

H4a There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age

H4b There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender

Methodology

A survey will be used to investigate the differences in behaviors and practices of security-conscious users and regular users on mobile devices.

Participants

The first step will be identifying two groups of mobile users from the Illinois State University student body. The students will be used as the sample in this study. The first group (group A) will be made up of security-conscious students. To qualify for the security-conscious group, the users will be expected to have some computer security or mobile security training. One hundred students will be randomly selected from Illinois State University students who have completed at least TEC 383 or IT 250. These two courses were selected because of their focus on computing security concepts. Contacts have been made with instructors who teach these courses. Instructors who teach classes in which these two courses are prerequisites have also been contacted, and they have agreed to assist with administering the survey.

The second group (Group B) will be made up of regular mobile device users. One hundred students in this group will be randomly selected from students in different degree programs at Illinois State University. Classes in Criminal Justice Sciences, Family and Consumer Sciences, Health Sciences, and Kinesiology and Recreation have been identified. Instructors from those departments have also been contacted and asked to administer the surveys in their courses.

The sample for the two groups will be selected because of their generalizability. Generalizability refers to the degree that study conclusions are valid for members of the population not included in the study sample (Trochim & Donnelly, 2008). Group A students represent the security-conscious population, while Group B represents the regular mobile device users.

Instrumentation and Measurements

The survey included in Appendix A will be administered to Group A and Group B. The first part of the survey asked for demographic information. There will be two control variables in this study; they are age and gender. Sekeran (2003) noted that demographic information helps describe the information of a sample and the general population.

The next part of the survey includes four general security practices, protection practices, data backup and disaster recovery, and perception of security. These four constructs were selected based on Jones and Heinrichs (2012) broad questions relating to security practices. The questions were based on three approaches: avoiding harmful behaviors and activities, providing protection through phone settings and add-on utilities, and preparing for disaster and recovery. The questions were used as a starting point, and adjustments were made. Below is a further explanation of the four constructs:

General security practices. Participants will be asked to give their responses to general security questions. The questions include opening and downloading attachments received in a text message or email from unknown sources. They will answer with a yes, no, or not sure response.

Protection practices. Participants will rate their practices and views on mobile device protection. The questions include installing antivirus and encryption software, password/passcode to access their device, enabling lock/timeout, and remote wipe. The rating will be on a 5-point scale ranging from 1(strongly agree) to 5 (strongly disagree).

Data backup and disaster recovery. Participants will rate how they deal with data backup and disaster recovery. The questions include having a backup plan for data and Apps, the insurance of mobile devices, and the ability to restore data and Apps in the event of a failure. The rating will be on a 5-point scale ranging from 1(strongly agree) to 5 (strongly disagree)

Perception of security. Participants will rate how they perceive mobile device security. The questions include their perception of the importance of mobile device security in general, how they perceive threats, and the importance of having antivirus software on their device. The rating will be on a 5-point scale ranging from 1(strongly agree) to 5 (strongly disagree).

Each of the constructs has some dependent variables (DV) that will be measured. Once the data about the variables is collected, it will be tested for reliability using SPSS's Mahalanobis Distance. A summary measure of each construct will then be calculated for each response as the average responses to the items for that construct.

Two identical surveys will be created using Qualtrics. One link will be distributed to Group A, and the other will be distributed to Group B. The links will be shared with the identified instructors who will assist with administering the survey. The survey will be issued to the targeted students during the Fall 2021 semester, as outlined in Figure 3. There will be no incentives for students to complete the survey.

External and Construct Validity

There are different types of validity, including external and construct validity. As Sekeran (2003) pointed out, external validity addresses how the results can be generalized to other settings or populations. The questions to be asked include what populations, settings, and measurement variables can be generalized. The study participants in this study will come from students with some special security training. They will also come from different degree programs as well as different academic levels. The sample size will be homogeneous, thereby providing additional validity for the measured effect. The construct validity asks whether the intended measure was measured (Trochim & Donnelly, 2008). The constructs in this study measure the differences in behaviors and practices of security-conscious users and regular users on mobile devices.

Pre-Analysis and Data Analysis

After the surveys have been completed, a pre-analysis data screening will be performed. Pre-analysis will help to increase the validity and accuracy of the results. SPSS Mahalanobis Distance analysis will be used to identify any outliers in the data. The survey results from the two groups will then be analyzed using the multivariate analysis of variance (MANOVA). The MANOVA test will be used in analyzing the hypotheses H1a through H4b. MANOVA will be used because of its ability to assess group differences.

The data collected will help find the differences in behaviors and practices between security-conscious and regular users on mobile devices. A summary of the hypothesis analysis, accepted or rejected based on the results, is shown below.

Hypothesis Analysis		
H1	There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices	The MANOVA test will be used to check for general security practices statistical differences between groups A and B. The data will be analyzed

		using the SPSS statistical software.
H1a	There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age	MANOVA test will be used to compare the effects of age on general security practices between the groups. The data will be analyzed using the SPSS statistical software.
H1b	There will be no significant differences in *general security practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender	MANOVA test will be used to compare the effects of gender on general security practices between the groups. The data will be analyzed using the SPSS statistical software.
H2	There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices	The MANOVA test will be used to check for protection practices statistical differences between groups A and B. The data will be analyzed using the SPSS statistical software.
H2a	There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age	MANOVA test will be used to compare the effects of age on protection practices between the groups. The data will be analyzed using the SPSS statistical software.
H2b	There will be no significant differences in *protection practices* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender	MANOVA test will be used to compare the effects of gender on protection practices between the groups. The data will be analyzed using the SPSS statistical software.
H3	There will be no significant differences in *data backup and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices	The MANOVA test will be used to check for data backup and disaster recovery statistical differences between groups A and B. The data will be analyzed using the SPSS statistical software.

H3a	There will be no significant differences in *data backup and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age	MANOVA test will be used to compare the effects of age on data backup and disaster recovery between the groups. The data will be analyzed using the SPSS statistical software.
H3b	There will be no significant differences in *security and disaster recovery* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender	MANOVA test will be used to compare the effects of gender on data backup and disaster recovery between the groups. The data will be analyzed using the SPSS statistical software.
H4	There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices	The MANOVA test will be used to check for the perception of security statistical differences between groups A and B. The data will be analyzed using the SPSS statistical software.
H4a	There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for age	MANOVA test will be used to compare the effects of age on perception of security between the groups. The data will be analyzed using the SPSS statistical software.
H4b	There will be no significant differences in *perception of security* between the security-conscious users (group A) and regular users (group B) on mobiles devices when controlling for gender	MANOVA test will be used to compare the effects of gender on the perception of security between the groups. The data will be analyzed using the SPSS statistical software.

Table 1. Summary of Hypothesis Analysis

Given the widespread use of mobile devices and the ever-increasing breaches on these devices, it is essential to increase mobile device security. The research in this proposal will shed light on the differences between security-conscious users and regular users. The best behaviors and practices will be highlighted in order to improve mobile device security.

Conclusion

This work-in-progress research outlines a study to investigate the differences in behaviors and practices of security-conscious and regular users on mobile devices. The study was proposed to include two groups: the security-conscious users (group A) and regular users (group B). Both Group A and Group B will be given a survey with questions about mobile device behaviors and practices. The behaviors and practices are grouped into four categories: general security practices in protection practices, data backup, and disaster recovery, and perception of security. The results of this study should demonstrate the differences in behaviors and practices of security-conscious users and regular users on mobile devices. Since the results from group A and group B will be recorded, it is hypothesized differences will occur in behaviors and practices between the two groups. Furthermore, the results will be further analyzed when controlling for gender and age. After the study is completed, the findings related to the hypotheses will be examined and published.

References

Carstens, D., Mahlman, J., Miller, J., & Shaffer, M. (2019). Mobile Device Espionage. *Journal of Management & Engineering Integration*, *12*(2), 86–94.

Chin, A. G., Little, P., & Jones, B. H. (2020). An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University. *International Journal of Education & Development Using Information & Communication Technology*, *16*(1), 44–61.

Crespo, M. (2020). let's collaborate! cyber security. *Technology & Engineering Teacher*, *80*(2), 20–21.
Fernando, L. (2019). Computing with Nearby Mobile Devices: A Work Sharing Algorithm for Mobile Edge-Clouds. *IEEE Transactions on Cloud Computing*, *7*(2), 329–343.

Giwah, W. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, *ahead-of-print*(ahead-of-print).

Hu, Z. (2020). Research on Android Ransomware Protection Technology. *Journal of Physics. Conference Series*, *1584*(1), 12004–. https://doi.org/10.1088/1742-6596/1584/1/012004

Jones, B., & Heinrichs, L. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53*(2), 22–30.

Lachtar, I. (2019). The Case for Native Instructions in the Detection of Mobile Ransomware. *IEEE Letters of the Computer Society*, *2*(2), 16–19. https://doi.org/10.1109/LOCS.2019.2918091

McDonough, B. (2018). Protecting Your Mobile Devices. In *Cyber Smart* (pp. 203–216). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119559658.ch18

McGill, T., & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology*, *36*(11), 1111–1124

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). New York: John Wiley & Sons, Inc.

Trochim, W., & Donnelly, J. (2008). *The research methods knowledge base* (3rd ed.). Mason: Cengage Learning.

Wang, L., Yang, J., & Wan, P.-J. (2020). Educational modules and research surveys on critical cybersecurity topics. *International Journal of Distributed Sensor Networks*, *16*(9), 1–18.

Wolf, F., Kuber, R., & Aviv, A. J. (2018). An empirical study examining the perceptions and behaviours of security conscious users of mobile authentication. *Behaviour & Information Technology*, *37*(4), 320–334.