eISSN: 2349-5715 pISSN: 2349-5707
Volume: 10, Issue 09, Sep-2023 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980

NEGATIVE IMPACT OF MOBILE APPLICATIONS ON NATIONAL SECURITY

Homidov Mamirjon Maxammadjonovich

Abstract. This study aims to identify how mobile users perceive the security of different mobile apps and the extent to which different apps affect such perceptions. This study also investigates mobile user preferences for the places where they can access apps and their perceptions of risk at marketplaces vs. websites. This study is based on a qualitative research in which interviews were conducted with 32 university students. The study found that mobile users do not feel secure when installing mobile apps, and that concerns about hacking personal and private information are pervasive.

Key words: app type, mobile applications, security, user perception, a significant contribution.

Introduction. Users expressed more security concerns regarding entertainment passus as games and communication rather than financial apps, such as banking. The study also found that users prefer installing apps from app stores. The findings of this research contribute a greater understanding of how mobile users perceive mobile app security and offer insights that will help developers adjust their security policies to ensure users 'security. In recent years, numerous fascinating mobile technologies have been unveiled and have made a significant contribution to our normal lifestyles. Mobile technology is among the most pervasive and innovative technologies ever invented, one that offers cellular communication across the globe. In line with the growth of mobile technology, mobile app stores have experienced booming business. Although app stores were introduced to enhance customers' security and trust in mobile apps, there are still some who doubt the protection offered by the same app stores. Convincing users that the apps they download are secure continues to be a big challenge for app stores. Mobile apps can be categorized as content delivery mode and transaction mode. Mobile apps are used in the content delivery mode to notify and report messages such as sport, financial news, games, and social media. Users will only provide their personal information on these apps if they feel secure. On the other hand, in transaction mode, apps are used to conduct transactions. Several apps can be used to purchase online products. However, concerns about the security of these apps are still the main reason many users avoid them. Users always have to decide where to get their apps – from app stores or from other websites. Few studies have investigated users' perceptions regarding the downloading of mobile apps from app store vs. websites. Argued that most people prefer to download their apps from app stores. However, others have argued that more people install their apps from any given source than app stores apps users. As the security of mobile application marketplaces is a relatively new area for research, this study chose a qualitative approach using interviews to gain a deeper understanding of user perceptions of the security of mobile apps marketplaces. The exploratory nature of this study is the main reason for adopting a qualitative approach. The study used the qualitative approach mainly to explore user perceptions of the security of mobile apps marketplaces, an issue on which there has been scant research. Thirty-two qualitative interviews were conducted individually to obtain a good understanding of how mobile users perceive the security of mobile apps. Interviews questions focused on users' mobile phone and apps use, their perceptions regarding the main reason of app stores, their perceptions regarding the security of mobile apps and whether this differ by the app type and finally users' preference to download apps from app stores vs. websites. A selection criterion for participants was previous experience using mobile phone apps. Before the data collection process, an email explaining the purpose of the study and its importance, and indicating the confidentiality of the research, was sent to all students

eISSN: 2349-5715 pISSN: 2349-5707
Volume: 10, Issue 09, Sep-2023 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980

requesting their cooperation. Students were offered a five-point extra credit on one of their courses if they chose to complete the interview, and an alternative extra credit assignment was made available if students chose not to participate. Each participant's interview was recorded with a voice recorder. At the beginning of each interview, respondents were notified that all interviews were being recorded. Before the interview, the participants were asked if they had any questions. They were also asked to provide as much data as they could. The researcher preferred to transcribe the interviews to ensure familiarity with the data before the analysis process started. Interviews were transcribed in detail to ensure that the richness of information generated during the interviews was fully captured. Smartphones include sensitive data about users, such as addresses, photos, phone numbers, emails, and credit card information. Disclosure of these data may result in hackers invading the privacy of users and putting them at risk of financial loss. Research findings reveal that security concerns are the main barrier to users adopting certain technology. Lack of mobile apps security is a main concern for mobile users, as revealed by the study findings. This study corroborates prior research, which illustrates that most mobile users don't feel secure using mobile apps, as malware and viruses can be used to steal their private information for fraudulent purposes. Based on the current study and previous research it is clear that the majority of mobile users have not embraced mobile commerce because they don't trust the credibility and security of numerous apps that are used in online business transactions. In their research regarding the security of health apps concluded that sensitive data included in health apps lack sufficient security because app developers do not give enough priority to security during app development. In addition, the findings suggest that users feel more secure downloading mobile apps only from app stores. The participants in this study highlighted that although downloading mobile apps from app stores is not fully secure, they are still more secure than unknown websites. This supports a study by who reported that the main reason mobile users prefer using an app store is because app stores verify the credibility of app sources before availing them to the users. Installing an app from unknown or unsafe sources is very risky for mobile users. As reported by the research results, app stores are considered more secure than any other websites since users can review the download rankings of apps before installing them. Users can use this information to distinguish between malicious and benign apps. Availability was also highlighted as a main reason for users' preference for downloading apps from an app store instead of a website, as reported by the research findings. When one needs a particular app, an app store is easily accessible, unlike websites where one haste search and sometimes be redirected to other sites filled with adverts before reaching the exact app. The research findings provide a rich basis for further theory development in this area. With the increased use of tablets and smartphones for accessing and saving users' personal and financial information, mobile security calls for far greater attention to protect users from security risks. The findings highlight that there are still great concerns amongst mobile users regarding the security of mobile apps. The widespread nature of the mobile marketplaces and the proliferation of apps contribute to users' sense of insecurity while downloading mobile apps, particularly entertainment and games apps. To promote better mobile app security perceptions, the developers of mobile apps should bear the responsibility of the security of mobile users. Ensuring that consumers are protected against any attack through the services of apps stores is very important if these stores wish to retain customer loyalty. If app stores prioritize security, they will gain the confidence and loyalty of their customers. Results indicate that mobile users feel less secure downloading free apps. Initiatives to make the marketplace more secure in downloading apps should include free apps as well as paid ones. Moreover, as accepting all permissions while downloading mobile applies becoming a default step for users which increasing the risk to the security and privacy of mobile users. In this study, the sample profile of respondents was university students. This sample

eISSN: 2349-5715 pISSN: 2349-5707
Volume: 10, Issue 09, Sep-2023 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980

profile minimized the chances of generalizing the results to different profiles. Despite these concerns, this group serves as a good sample of mobile users. This category is familiar with mobile apps and the security concerns involved in downloading these apps. However, it is suggested that future research should be conducted with different samples, using respondents who have different demographic characteristics or mobile usage patterns. In addition, the findings of the current study reveal that the perceptions of mobile users towards the security of their mobile apps are limited. Adopting suitable security technologies can play a significant role in enhancing users' security perceptions. However, as the qualitative nature of this study design could be considered one of its main limitations, it is recommended for exploratory research, such as the current one.

Conclusion. The main objective of this study was to explore mobile users' perceptions of the security of mobile apps. It was necessary to have direct interaction with mobile users to gain a deep understanding of the security of mobile apps from their perspectives. Losing sensitive data, such as client information and login passwords, typically stem from inadequate mobile app security, which hackers leverage to obtain access to sensitive information.

References

7. Androulidakis, I. I. (2016). A multinational survey on users' practices, perceptions, and awareness regarding mobile phone security. In Mobile Phone Security and Forensics (pp. 15–28). Springer.
8. Bao, P., Pierce,J., Whittaker, S., & Zhai, S. (2011). Smart phone use by non-mobile business users. In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (pp. 445-454). Academic Press.
9. Gasimov, A., Tan, C., Phang, C., & Sutanto, J. (2010). Visiting Mobile Application Development: What, How and Where. In Proceedings of the 2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR) (pp. 74-81).
10. Dulaney, K., Cosgrove, T., Erensen,J.,Jones, N., McIntyre, A., & Reynolds, M. (2015). Predicts 2016: Mobile and Wireless. Gartner. Retrieved from https://www.gartnerinfo.com/ipg/predicts_2016_mobile_and_wir_273934.pdf
11. Fife, E., & Orjuela, J. (2012). The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security. International Journal of Engineering Business Management, 4, 4–11. doi:10.5772/51645
12. Gupta, K., Kumar, R., & Loothra, S. (2014). Smartphone security and contact synchronization. In Proceedings of the 2014 Fourth International Conference on Communication Systems and Network Technologies (pp. 621- 625). Academic Press. doi:10.1109/CSNT.2014.130