Examining Current Safety Measures and Awareness of Cyber Threats to Mobile Devices: A Literary Review

Samantha Brewer

BACKGROUND

- The use of mobile devices, particularly smartphones, has skyrocketed in the past few years, resulting in a surge in cyber threats for phone users.[7,10]
- Mobile devices are fundamentally different in functionality to desktop PCs and other computers, which can make mobile users more vulnerable.[5]
- Most studies have focused on the technical models of resolving cyber threats with advanced techniques, with minimal consideration for end-users' usability.[11]

PURPOSE

Our project focuses on the specific cyber dangers present for mobile devices and phones, with the goal of raising awareness and presenting safer ways for using said devices.

Through a literary review, we hope to find up-to-date cyber threats to mobile devices and methods of communicating this information to the public in an accessible way.

METHOD

Databases: Google Scholar, IEEE, MDPI

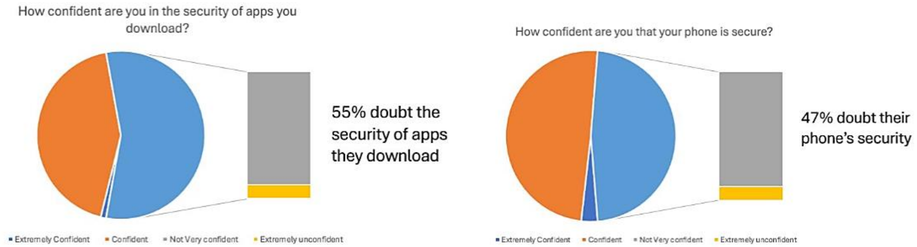
Keywords: mobile devices, cybersecurity, threats, cybersecurity education, smartphones, mobile apps, education app, mobile network security

Number of Articles: 28 initial identified articles, 10 identified as presenting a problem and potential solution(s) for Public Awareness or a new Cyber Threat.

Analysis: Reading through the 10 included sources, we identified potential ways mobile device users could be vulnerable to cyber-attacks and existing efforts to raise awareness about such risks.

Inclusion Criteria: The studies incorporated in this analysis addressed cyber threat concerns and provided viable solutions to mitigate their effects.

FIGURE 1: PERCEPTIONS ON PHONE AND APP SECURITY



Note. These models and their data was produced by Williams(11) summarizing the attitudes of respondents to his surveys. Copyright 2022 by ProComm

FIGURE 2: PROBLEM/SOLUTION SUMMARY OF EVERY ARTICLE ADDRESSING POTENTIAL MOBILE DEVICE THREATS

Authors	Problem/Vulnerability	Potential Solutions
Alsunaidi & Almuhaideb, 2019[1]	Just as virtual attacks on smartphones have increased with general use, so have **physical threats like theft**, where the thief could directly bypass virtual security.	There are many possible solutions that can help **locate and/or lock down** lost phones. IMEIs are unique identifiers generated for every phone and can be blacklisted if a user reports theirs stolen.
Ashawa & Morris, 2021[2]	Malicious attackers can **use permissions** granted on installation for benign-seeming apps for background programs the main app runs, which can **access more** than the user consented to.	Correlations were found between **specific permission types,** where if one was requested, others in the cluster may also be included, which can be used to **determine the risk factor** of apps.
N. Chen & B. Chen, 2022[4]	When **malware** takes over a mobile device's OS, the lower-level antiviruses in the **kernel can be hijacke**d, removing any way to fight the malware.	The writers developed mobiDOM, an **antivirus** that runs in the FTL layer **in flash storage.** If malware is detected, it can halt deletion processes, remove the malware, and restore the data.
Goel & Jain, 2017[5]	Mobile users are three times as **vulnerable to phishing** as desktop users, which is when attackers attempt to steal personal information.	Given that phishing tends to start from user inputting passwords or logins into unsecure sites or imitations of familiar apps, **awareness needs to be raised.**

RAISING AWARENESS VIA EDUCATIONAL APPS

- Several of the articles[6,8,9] found that developing apps were the best way to quickly teach about cyber safety.
- By gamifying tasks, including creating tasks to complete, quizzes to take, and scores based on how well they did can engage the user compared to less interactive means of learning such as lectures.[6]
- It was found that the respondents were aware of theft as a threat, but the more virtual threats such as malware and spyware were less familiar to respondents.
- Users were also only familiar with the more basic security measures like a pin password compared to a VPN.[8]
- After using the apps, users were found to have improved understanding on how to identify malware.[9]

IMPACT

As more and more potential modes of attack are developed for mobile devices, the public awareness of the danger has lagged far behind.

Creating ways to teach people about the risks specific to the most commonly-used technology today is necessary.

As mobile devices are replacing credit cards, carry important personal data, and can even control the appliances in a smart home, the public needs to understand how to stay safe when using their smartphones.

By creating apps that can teach cyber safety in an understandable way, it can bridge the gap between cybersecurity professionals discovering new vulnerabilities and the average user who is most at risk.

REFERENCES

1. Alsunaidi, Shikah J., and Abdullah M. Almuhaideb. 'Security Methods against Potential Physical Attacks on Smartphones'. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS.*
2. Ashawa, Moses, and Sarah Morris. 'Modeling Correlation between Android Permissions Based on Threat and Protection Level Using Exploratory Factor Plane Analysis'. *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, MDPI AG, Nov. 2021, pp. 704–743.
3. Bubukayr, Maryam Abdulaziz Saad, and Mohammed Amin Almaiah. 'Cybersecurity Concerns in Smart-Phones and Applications: A Survey'. *2021 International Conference on Information Technology (ICIT)*.
4. Chen, Niusen, and Bo Chen. 'Defending against OS-Level Malware in Mobile Devices via Real-Time Malware Detection and Storage Restoration'. *Journal of Cybersecurity and Privacy*, vol. 2, no. 2, MDPI AG, May 2022, pp. 311–328.
5. Goel, D., and A. K. Jain. 'Mobile Phishing Attacks and Defense Mechanisms: State of Art and Open Research Challenges'. *Computers & Security*, vol. 73, 2018, pp. 519–544.
6. Jawad, Hadeel Mohammed, and Samir Tout. 'Introducing a Mobile App to Increase Cybersecurity Awareness in MENA'. *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*.
7. Kappelman, Leon, et al. 'The 2018 SIM IT Issues and Trends Study1'. *MIS Quarterly Executive*, vol. 18, no. 1, Association for Information Systems.
8. Markelj, Blaž, and Igor Bernik. 'Safe Use of Mobile Devices Arises from Knowing the Threats'. *Journal of Information Security and Applications*, vol. 20, Elsevier BV, Feb. 2015, pp. 84–89.
9. Podila, Laxmi M., et al. 'Practice-Oriented Smartphone Security Exercises for Developing Cybersecurity Mindset in High School Students'. *2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*.
10. Rodriguez, Eva, et al. 'A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks'. *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, Institute of Electrical and Electronics Engineers (IEEE), 2021, pp. 1920–1955.
11. Williams, Sean D. 'Exploring the User Experience Design of Commercially Available Cybersecurity Products for Personal Mobile Devices'. *2022 IEEE International Professional Communication Conference (ProComm)*.

FUNDING & THANKS

The author is thankful for help on this poster from her mentor Blessing Akinrotimi.

The author is also grateful for funding from the Griffiss Institute under contract No. SA10012021MM0336.