Research Project: Final Draft

An assessment of smartphone security, vulnerabilities, and the importance of spreading education and awareness.

JORAEL JAMISON

Columbia Basin College

CSIA-450: Cyber Security Capstone

Professor Boehnke

June 1, 2023

Abstract

The widespread adoption of mobile devices has revolutionized the way we communicate, access information, and go about our daily lives. Smartphones offer unparalleled access to sharing and receiving information, however, along with the convenience and functionality they offer, smartphones also pose significant security risks. This project aims to assess smartphone security vulnerabilities and the importance of user education and awareness. By investigating common security weaknesses and incorporating statistics and recommendations from scholarly articles, the project seeks to provide valuable insights into the risks associated with smartphone usage and proposes effective strategies to mitigate these threats.

Introduction

This report presents an assessment of the smartphone security vulnerabilities. With the increasing usage of smartphones, this project aims to educate individuals and promote awareness of the risks and vulnerabilities associated with mobile devices. The scope of the project involves a research-based approach to investigate various aspects of smartphone security, including data leaks, weak passwords, unsecure networks, and malicious applications. Additionally, the report highlights the importance of carefully examining which permissions are requested by applications and offers guidance on limiting the sharing of location services on social media platforms and its associated risks. The project also addresses phishing methods, spam identification, and safe browsing practices. Finally, this project will explore several scholarly sources to provide additional insight to understand how users interact with and perceive the importance of smartphone security and offer guidance to mitigate risks.

Problem Statement

Mobile devices contain a multitude of personal and sensitive data making them attractive targets for attackers seeking to exploit this information. As articulated by Ruggiero and Foote in the article *Cyber Threats to Mobile Phones*, the number and sophistication of attacks on mobile devices are increasing faster than countermeasures can catch up, making it essential to address their security vulnerabilities. Additionally, the lack of technical security measures and the potential exploitation of seemingly legitimate applications highlight the need for mobile device strategies and to spread education and awareness (Ruggiero, P. & Foote, J., 2011).

The rapid growth of smartphone usage has exposed users to a multitude of security threats. Weak passwords, unsecure networks, and malicious applications requiring unnecessary permissions, can lead compromising user privacy, data leaks, and unauthorized access to personal information. Furthermore, phishing methods through text and email have become increasingly sophisticated, making it crucial for users to understand the importance of how to identify spam and avoid clicking on malicious links. Finally, sharing location services or oversharing personal information on social media can lead to not only being tracked for ad purposes, but anyone who can view your posts may be able to find you in person. This leaves you vulnerable to people with malicious intent, like stalkers or threat actor, finding your exact location or using your personal information against you in a phishing campaign to further their objective.

The problems outlined above are becoming increasingly more prevalent and to address these challenges, this project aims to educate individuals on smartphone security, enabling them to make informed decisions and protect themselves against cyber threats.

Results

i. Assessment of smartphone security and vulnerabilities.

The following assessment will discuss several key security vulnerabilities identified through research for mobile devices, including, data leaks due to weak passwords, connecting to unsecure networks, and downloading malicious applications or granting unnecessary permissions to personal information, leading to privacy violations. In addition to discussing the importance of not oversharing location services or personal information on social media, and identifying the risks associated with unsafe browsing techniques, and identifying phishing methods in order to avoid being a victim to identity theft and financial loss. In summary, to mitigate these risks, this project emphasizes the importance of implementing strong passwords, avoiding unsecure networks, downloading applications only from trusted sources, carefully considering permissions, limiting location services and the over-sharing of personal information on social media platforms, and finally, developing the ability to practice safe browsing techniques and to identify and avoid phishing attempts.

a. Potential risk of weak passwords on mobile devices.

Weak passwords provide an easy avenue for cybercriminals to exploit. Users often choose easily guessable passwords or reuse them across multiple accounts, this practice is unsafe and makes their data vulnerable to breaches. Weak passwords can allow an attacker to access things like your bank account or social media accounts by utilizing the “email/password” reset or “forgot my password” features. Ensuring your passwords are secure should be across the board on all devices and platforms. Your mobile devices are just as vulnerable if not more as they contain a compact and portable means to access all your

accounts via the web or downloaded applications. Mobile devices are easily lost or stolen and failure to implement strong authentication measures for accessing your device can leave you vulnerable to anyone who finds your device having access to your personal and sensitive information.

Let's discuss some ways to mitigate these risks and better protect your mobile devices from such a scenario. First, ensure your device is secured by a strong authentication method, such as a strong password/PIN, biometrics, or facial recognition. Although, facial recognition leaves the possibility of a relative or someone with similar facial features getting past this step. A strong PIN should consist of numbers that do not resemble a pattern, a date, or any repetition of numbers that would make it easily guessed. It would be advised to increase from a four to 6 digit PIN, so long as you follow the steps above to not make it strong.

In addition to accessing your device, the next step is ensuring your applications and web browser are secure. Say an attacker by-passed the first authentication measure and now gained access to your device, by implementing the following suggestions will slow them down and limit the amount of access they will be able to obtain. Starting with the browser, it is not good practice to rely on storing your username and password credentials directly on the web browser. Doing so can allow anyone to open the browser, navigate to your bank and they will be prompted to select your stored password – gaining access your account. The best practice would be to use a secure password storage manager like Lastpass, Dashlane, Nordpass and many others. Another important step is implementing multi-factor authentication or MFA when offered. This allows for

an additional step when logging into your account to verify your identity, such as a text message or email with a code. One other key suggestion is to ensure you are fully logged out of the website after each browser session.

Finally, let's discuss ways to better secure downloaded applications on your device. This coincides with the advice above about ensuring you are logged out after each session. Particularly, with any application holding sensitive and confidential information such as personal banking. Although it may be convenient to always remain logged in to an account, you have to weigh the risk if your mobile device were to be compromised, what would you not want an attacker to see.

b. Potential risk of connecting to unsecure networks.

With the mobility of smartphones and seemingly endless wireless networks to connect to in your travels, you may think you are safe connecting to your local coffee shop network, or other public Wi-FI. This is not the case, public or unsecured networks make it much easier for a cybercriminal to get a hold of your web traffic and use if for nefarious purposes, like Man in the Middle or MITM attacks. This attack is where an attacker will position himself between the conversation of the user and application in order to capture login credentials or other vital information being transmitted to further their attack. If you do find yourself in need of connecting to an unsecured network ensure you consider the following advice, do not transmit any sensitive personal data or access personal bank accounts. Do not leave your smartphone unattended in a public place.

Your best defense with securing your internet traffic while connected to an unsecure network is using a Virtual Private Network or VPN. There are many out there, such as NordVPN, Norton, and ExpressVPN. A VPN adds an additional layer of protection by encrypting and re-routing your traffic so anyone trying to snoop would have a very difficult time. This is our overall objective right, to slow down the attacker and make it as difficult as possible. It is important to understand we can never fully prevent attacks; we can only do our best effort in mitigating the risks. Some other quick advice to better protect yourself with unsecured networks is to use your own hotspot, disable auto-connecting to wireless networks, browse using HTTPS sites, and ensure you are connecting to the correct wireless access point. Attackers can be nearby a coffee shop for instance with their own access point being broadcast with a similar name, also known as an evil-twin attack. The attacker hopes you will connect to their network versus the legitimate one.

c. Potential risk of downloading from unknown sources.

The app store on your device is designed to provide users with applications that work seamlessly with their devices, however this is not always the case. Among the millions of free and paid applications, many have not been fully tested for security vulnerabilities. Any developer could potentially pay a small fee to have their mobile application placed in the app store. And there is a good chance some users will download an application before Google or Apple catches the malicious content. As such, it is best to stay away from third-part app stores or downloading applications from web pages. Downloading from unknown sources increases the risk of malware

infections and data compromise. Some risks associated with malware infections are adware, spyware, and phishing, in addition to apps from unknown sources may have compatibility and performance issues.

d. Potential risk of granting unnecessary permissions to mobile device.

The next crucial step once you have an application downloaded on your device is to ensure they do not require unnecessary permissions to be granted. By unnecessary I mean, a gaming app should not need access to your SMS text messages or access to your camera or camera roll. You would be surprised just how many applications require a multitude of unnecessary permissions for their app to be used. Often times a user will just skip through the long list of permissions and blindly accept the terms and conditions. As expressed in the article by Unisex, users tend to grant permissions more than they deny them and the microphone was the most often denied permission, followed by calendar, contacts, and camera (unisex, 2021). Failing to properly grant or deny permissions obviously opens the door to significant risk of their device being compromised. If an application does need permissions to areas like your camera it is best to select that it is only allowed while using the app. Make sure you fully exit out the app each time you are complete. You can always review your current app permissions under settings. For Apple choose System Preferences, Security & Privacy, then open the Privacy tab. Android users will need to open Settings, Apps, tap the app they want to view and tap Permissions.

e. Potential risk of utilizing location services and over-sharing information on social media.

Location services on your mobile devices offer a big advantage to allowing first responders from being able to find you during an emergency, they can relay real-time information, such as traffic updates or weather reports, and allow you to utilize GPS maps while traveling. While at the same time, utilizing location services has its potential risks. Caution should be used when openly allowing location services on mobile applications, such as social media and over-sharing information on social media. When you make a post on social media, some geolocation tags may list the exact address of your location, this means that anyone who can view your post may be able to find you in person. This is a significant security risk as say a person wanted to stalk you or a criminal wanted to break into your residence, they would know you are not home.

Oversharing information is also risky as the more personal information you share on the internet, the easier it is for a cybercriminal to have ammunition while conducting phishing attacks, stealing your identity, tracking your daily routine, or gaining access to your personal accounts. The settings for changing app location services can be found on your device's settings, and if necessary, should be set to "Allowed only while in use." This will prevent unwanted background tracking of your location.

f. Potential risk of practicing unsafe browsing techniques and clicking on untrusted links.

Safe browsing techniques are necessary to ensure you are better protected while using your mobile device. First, let's discuss clicking on unknown links. By clicking on unknown links from SMS messages, social media posts, websites, or

email could potentially re-direct you to a phishing website designed to steal your personal information, such as your login credentials. If you are not completely sure a link is from a trusted source, do not click. If you receive an email to click on a link to log in, always avoid that and directly log in from the official website. You can always hover over the link or right click and save the link URL and run it through an application like VirusTotal. This is free tool used to analyze suspicious files and URLS to detect types of malware and other malicious content.

Other safe browsing techniques include implementing an internet security tool such as Bitdefender or other tool to actively monitor and protect you from navigating to unsecure websites. It is important to note that you should not fully rely on your browser or anti-virus settings you protect you, they can warn you but not stop you from accessing the site. Avoid visiting unsecure or risky websites that you are not certain are legitimate, have a valid certificate, or are not HTTPS. Visiting an unsecure website can result in viruses, spyware, or worse. Some safe practices include never trusting free content, free movies, music, and other content often contain viruses and malware. Use caution what links are clicked while using a search engine, often times a hacker will use legitimate topics or enticing offers to get you to click.

g. Potential risk and ways to identify phishing methods.

Phishing is the practice of sending emails or other messages that appear to be from reputable companies in order to have individuals click on links or reveal personal information, such as passwords and credit card information. Successful phishing attacks can cause financial loss for victims and put them at a greater risk

of their personal information being compromised. One method of phishing attacks is via email and there are many red flags to look out for when analyzing the legitimacy of a message. Although phishing attacks are becoming more legitimate in appearance and sophisticated, they still may contain things such as generic greetings, miss-spelled words, unofficial email address, and misleading hyperlinks navigating to a strange URL. Other phishing methods can be done through text message or phone call. The aim is to have you navigate to a website, click on a link to download malicious software, or to have you disclose personal and confidential information. If you receive a suspicious phone call, always veer on the side of caution, and tell them you will call them back directly at their official number found online. Never freely disclose personal or confidential information to random callers impersonating to be a legitimate source.

ii. Annotated Bibliography

The following is an annotated bibliography that will outline key findings from each of the scholarly sources referenced and how they are relevant in this project.

Patten, K.P. & Harris, M.A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education (JISE).* https://jise.org/Volume24/n1/JISEv24n1p41.pdf

This article focuses on the critical need, at the time of writing in 2013, for higher education to implement a curriculum to undergraduate IT students concerning the global security issues of mobile device security. The article did an excellent job expressing points on why this was a growing concern, and how it would greatly benefit IT students

to better address these issues, as they become professionals in their field of work. Although this article was written a decade ago, I do find the following points relevant in my research. I could utilize the statistics of mobile device users, organizations and the threat "BYOD" and even corporate issued mobile devices pose for IT professionals, to compare how things have changed. At the time, it was said 68 percent of IT professionals were unable to identify known mobile device issues on their networks, because either no controls in place or employees ignored usage policies. As my project involves teaching and training to offer a better overall awareness to mobile device security threats, I believe this article will assist in obtaining useful information, as it points out education as being one solution toward understanding the threats and offers guidance for organizations to follow in order to develop proper mobile device policies and device management systems. Additionally, the article goes into the business needs for mobile device security and depicts the growing concern and vulnerabilities with the two leading operating systems – Google's Android and Apple's IOS. This article is scholarly and is published in a peer-reviewed journal.

Ruggiero, P. & Foote, J. (2011). Cyber Threats to Mobile Phones. *CISA.* https://www.cisa.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf

This article expresses the growing popularity of smartphone use and how their lax security has made them attractive targets for attackers seeking sensitive data and personal information. It mentions how the number and sophistication of attacks on mobile devices are increasing faster than the rate of countermeasures – which stays relevant today. Mobile devices account for a large percentage of digital fraud and phishing attacks.

Although, some aspects of the article are dated, such as the mention of technical security measures being uncommon on mobile devices, such as, firewalls, antivirus, encryption, and updates. Security surrounding smartphones has really improved over the years. Some points I found interesting are how mobile devices are much easier to be lost or stolen than a PC and given time an attacker can defeat most security features and gain access to sensitive information on a device. In addition, the article goes into how many applications, even those seemingly legitimate, can be malicious, and describes methods attackers use to exploit a device through phishing. Finally, the article depicts steps that can be taken to better protect your mobile phone from threat and actions to take if your mobile phone is stolen. I found this article interesting, and feel it correlates well with my project. This article is scholarly and is published in scholarly journals.

Souppaya, M. & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST.* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

The purpose of this article provides strategies for organizations to manage and secure mobile devices against a variety of threats in order to achieve the three security objectives: confidentiality, integrity, and availability. The information in this article is relevant to my project as it discusses recommendations for centralized management technologies and security concerns specifically inherent in mobile devices. This information is crucial for those responsible for planning, implementing, and maintaining mobile device security. In addition, this article discusses high-level threats and vulnerabilities, lack of physical security controls, and use of mobile devices on untrusted

networks and the risk of utilizing untrusted applications and location services. All of which are beneficial to my research pertaining to my project. This article by NIST is scholarly and is published in scholarly journals.

Cao, W., Xia, C., Peddinti, S., Lie, D., Taft, N. & Austin, L. (2021). A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. *USENIX*. https://www.usenix.org/conference/usenixsecurity21/presentation/cao-weicheng

The article "A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions" studies user behavior, expectations, and engagement with Android permissions. A large-scale study across 10 countries and regions was conducted to understand how users interact with their Android phones and better understand their expectations and rationale in granting and denying permissions. Conclusions from the study revealed that users are less likely to deny permissions when explanations are presented or are less educated. This article coincides with the purpose of this project to spread awareness and educate users about the implications and risks associated with mobile devices and in this scenario, granting unnecessary permissions for applications. This article by USENIX is scholarly and is published in scholarly journals.

Conclusion

In conclusion, this report highlights the increasing security risks associate with the widespread use of smartphones and emphasizes the importance of user education and awareness in mitigating these threats. An assessment of the most common smartphone security vulnerabilities revealed weaknesses, such as utilizing weak passwords, accessing unsecured

networks, downloading from unsecure sources, granting unnecessary permissions, sharing location services, and oversharing information on social media, practicing unsafe browsing techniques, and falling victim to phishing attempts. To address these risks, the report provides practical recommendations and best practices to mitigate these risks, in addition to incorporating insight from scholarly sources empowers users to make informed decisions about how to safety utilize their mobile devices, safeguard their personal information, and to not fall victim to attacks.

References

Patten, K.P. & Harris, M.A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education (JISE).* https://jise.org/Volume24/n1/JISEv24n1p41.pdf

Ruggiero, P. & Foote, J. (2011). Cyber Threats to Mobile Phones. *CISA.* https://www.cisa.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf

Souppaya, M. & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST.* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

Cao, W., Xia, C., Peddinti, S., Lie, D., Taft, N. & Austin, L. (2021). A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. *USENIX*. https://www.usenix.org/conference/usenixsecurity21/presentation/cao-weicheng