MOBILE SECURITY THREATS AND A SHORT SURVEY ON MOBILE AWARENESS: A REVIEW

Triveni Krishnappa
School of Computing and Digital Media
London Metropolitan University, London
Engalnd, United Kingdom

Abstract— **there is no stop to technology, every day new tools or techniques are emerging, and with the increase in technologies and use of mobile devices, digital crimes are also increasing. Companies are starting to face an enormous amount of data loss. The world is run by technology and networks and it becomes important for everyone to understand that cyber security, company assets, or the individuals data are at risk without the protection added to it. The usage of business applications on mobile devices has become common to keep the production environment active. IT companies use updated technologies to protect their data, but attackers are always enhancing new techniques to break through these technologies. Cyber Security becomes important to make sure the assets, information/data, and personal or financial details are safeguarded and not at risk. This paper aims to review the threats and crimes involving mobile devices and discuss the awareness among people of these crimes based on a short survey.**

Keywords— **Threats, Mobile devices, Security, Cyber, Digital crimes, Attacks**

I. INTRODUCTION

To increase the production of it firms the usage of mobile devices has become common. all the applications and interfaces are available on mobile devices for employees to just go handy at any time. the vulnerabilities in mobile devices and mobile hacking or mobile cybercrimes are also evolving so it becomes important to communicate about mobile security threats and best practices to keep the devices safe. malware attacks are increasing on android based mobile devices. malware entering smartphones try to disable essential functions and spread the virus leading to an information leak. ddos attacks are commonly reported attacks using mobile malware. the harmful codes are added to the application by the hacker using the repacking technique, when the rooting attempt is successful the malware communicates the information saved in mobile (contact lists, sms, public key certificates) to external servers (yoon, 2014). the applications in the play store can be deceiving, the hackers would have added trojans to the applications and uploaded them to the play store. the malware in these applications is executed and the information is scammed every time the user uses the app (vashisht, gupta, singh, & mudgal, 2016).

II. CURRENT AND EMERGING SECURITY THREATS

New security threats are beginning to emerge as technology continues to develop and grow. The increased use of cloud services in the corporate world will face enormous attacks as per the Security Threat Report 2022 by Sophos. With the emergence of attacks on endpoints, mobile devices will be targeted as corporate businesses are moving to cloud services to provide better service to their customers. It is predicted that the attacking methods will be improvised and adapted to Advance Persistent Threats (APTs). It is also predicted that the attackers will make use of Artificial intelligence (AI) to target the victims with more specialized malwares (Sophos, 2021).

III. CYBERCRIMES

Cybercrime is defined by Dr. Latika Kharb as “a criminal activity committed on the internet and is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money” (Kharb, 2017). Cybercrime can take place against persons, property, and the government. Cybercriminals or hackers commit crimes demanding money from the victims.

- Types of Cyber Crimes- Cybercrimes can be committed through the internet by any medium such as computers or smartphones. There are various kinds of cybercrimes, and the few top crimes include (Hakhroo, 2020).

Cyberstalking: Cyberstalking can be defined as a pattern of behavior and acts carried out on the internet or any electronic media to intimidate, alarm, terrify, or harass the victims (Omer Faruqe Jubaer, et al.).

Unethical Hacking: The process of locating vulnerabilities in the system to gain access to the network to obtain the personal or professional data without authorization. Hacking can be considered unethical when hacking infringes at least one ethical value or moral principle (Chiffelle, 2019).

Phishing: Phishing is a type of cybercrime in which victims are contacted via e-mail, phone call, or SMS and tricked into disclosing personal information such as passwords, account information, or card information that can give access to the victims system (Abdul Quadir Md, et al., 2022).

Email and SMS spoofing: The act of creating emails or SMS using a falsified sender address is known as spoofing. In this type of assault, cybercriminals send emails or SMS that have been altered to make them appear to have come from a reliable source (Huseynov, 2021).

Identity theft: Identity theft is taking someone else credentials or personal information and using it to make illicit purchases or conduct financial transactions under a false identity (Nwabineli, Felix, & Aguboshim, 2021).

IV. MOBILE CRIMES

Mobile crimes are the types of offenses where smartphones or mobile devices are involved in committing crimes against victims. These crimes can be targeted at individuals through phone calls, messages, malware, etc. A few types of Mobile crimes are (Narula, 2019):

Bluejacking: It is the process by which an attacker can send an unwanted or malicious message to any device that is Bluetooth enabled (Techslang, 2022).
Vishing: When an attacker calls a victim and requests information over the phone, this is known as "voice phishing". These assaults can be carried out by leveraging caller ID and social media application data collected from millions of users, together with phone numbers and personal information (S. Jones, E. Armstrong, K. Tornblad, & Namin, 2022).

Smishing: Smishing is a type of phishing in which Attackers send communications via text that looks to be from a reliable source and request that recipients click on a link or share their details via SMS messages instead of sending emails (Njuguna, Kamau, & Kaburu, 2022).

Mobile malware: Mobile malware is created expressly to target mobile devices like tablets and smartphones to obtain personal data. Mobile users access unapproved resources to download programs, and the malware present in these sources exposes the user’s private data (Aksakalli, 2019).

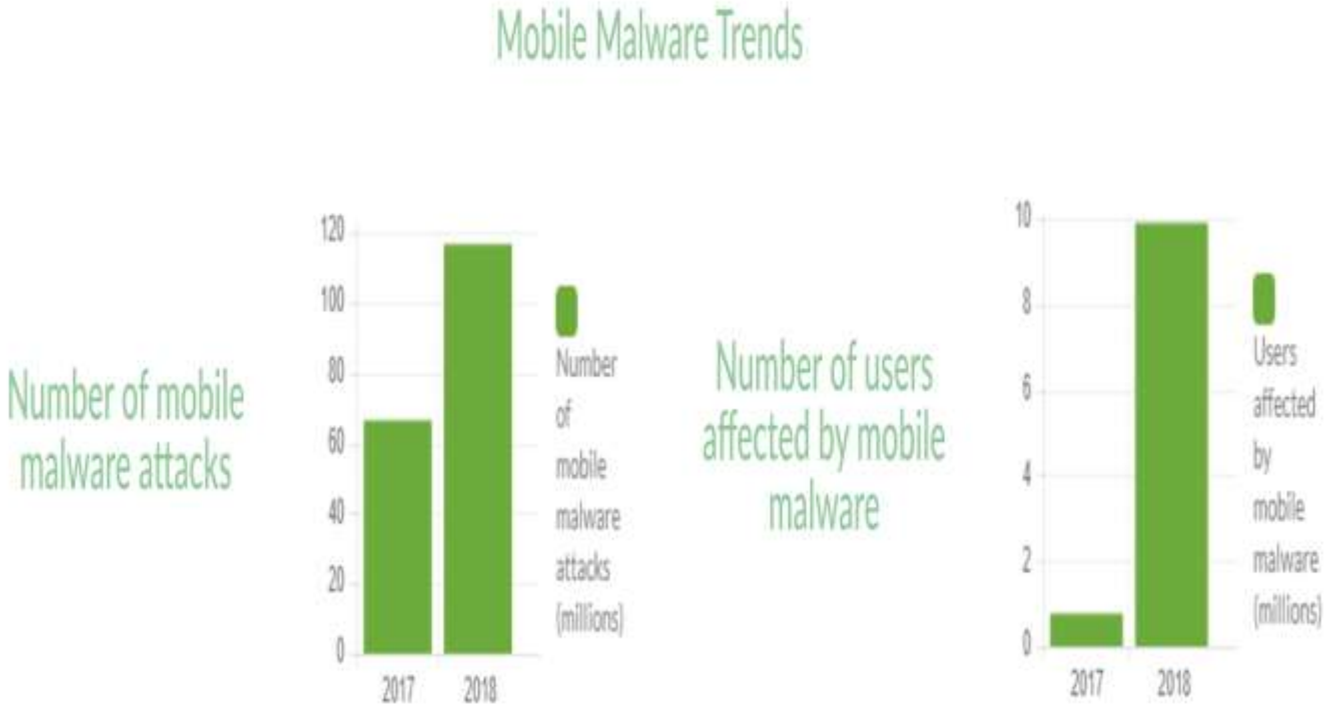


Fig 1: Source- mobility (2022)

V. ATTACKS AND THREATS TO MOBILE DEVICES

Security threats are increasing rapidly. Has the security of the technology is increasing, attackers are becoming innovative in breaking these securities. Bring your device (BYOD) is a huge threat to mobile devices. Mobile phishing and ransomware are other major threats faced by the employees of small companies who fail to maintain and follow the policies of such programs. Ransomware distribution using mobile devices running Google's Android OS is on the rise, according to Stu Sjouwerman (NETWORKWORLD, 2022), a cofounder of security training company KnowBe4 LLC. These risks threaten to exploit individuals online or in private and government organizations. These threats can be classified as:

Application-based threats: Applications downloaded from unlicensed content may cause different mobile device cyber threats. Although "malicious apps" are available on the Play Store, they intend to steal the data. These threats include spyware and malware that steal confidential information without people’s knowledge.

Web-based threats: Smartphones enable users to engage in a variety of online activities and are frequently used to access services provided by the Web. Threats based on the web include Phishing, Browser exploit.

Network-based threats: Local wireless networks (Wi-Fi, Bluetooth) and cellular networks are both frequently used by mobile devices to connect to the internet. By violating the security on the internet malware could be hosted on the devices. These threats include exploiting the network and Wi-Fi sniffing.

VI. MOBILE DEVICES AS EVIDENCE

Mobile phones manage different data like texts and multimedia messages, emails, and location. These facts can be used to connect a criminal with a crime. For instance, based on location information stored on mobile phones forensic technologies during an investigation may identify a person at a crime scene. Digital photos and videos offer reliable evidence that can be used in court. Images and videos also contain metadata that serves as further proof of a crime. When there are issues about a documents legitimacy or the method by which it was made, metadata is important. They can provide information about the creation date, several edits, timing, and type of edits made to a document. The issue of authenticity is the fundamental obstacle to using digital evidence in a way that secures its acceptance in courts. In the court, the information from digital evidence can be used only if its authenticated as per section 29 of the computer misuse Act, and section 7 of the electronic transactions Act (Gilibrays, Matovu, Egwar, & Bongomin, 2022).

VII. PREVENTION OF MOBILE THREATS

It becomes important to be aware of how to protect ourselves from mobile crimes. When selecting features, security must come first. Considering a mobile phone, users must consider password-protected measures to secure data. Security and antiviral Software should be set up on smartphones as well to increase their security. Use only secured with a password wireless network to establish a connection. Devices with Bluetooth support should be turned off so fraudulent users are not permitted to use private information. Avoid clicking and navigating through text or email links. Every time a social networking site is used, remove passwords and crucial data to prevent it from being used by an attacker. Never use a pirated website to download mobile apps always use only official websites. If a user receives a link or form from an unknown source, they should avoid sharing any banking or financial information online. A small group of trustworthy individuals must have access to your mobile phone number; it must not be made public. When not in use, communication interfaces including Bluetooth, and WiFi should not be in function. Accepting requests for personal or device information should be performed with caution. Bluejacking for example can be prevented by Switching off Bluetooth if it is not needed, turning the visibility off while Bluetooth is not actively transferring the file, and protecting your Bluetooth by allowing paring permission, so without pairing no other device can send or receive the files (R. Mistry, Dahiya, & P. Sanghvi, 2013).

VIII. CASE STUDY - AGENT SMITH ATTACK

Agent Smith malware had infected 25 million devices in early 2019, there were around thirty thousand Agent Smith infections in the US and UK. Agent Smith is malware that infected Android devices by replacing the original apps with malicious applications without user knowledge. This malware infected devices around the world including Australia, India, and Pakistan. The malware that spread was a third-party app owned by China. Before April 2019 there was an increase use of the Janus vulnerability to attacks (CVE-2017-13156) (Wu, 2019).

Working of Agent Smith: The victim is lured by the attacker to install the malware-infected app. The app contains encrypted malicious files and is in form of photos, games, or utilities. Once the app is opened, the attacker decrypts and installs the malicious files. The Google Updater was used by malware to disguise its activity (PHILLIPS, 2019). The list of the installed app is created in core malware. In case any app matches the list, it inserts the application with malicious content by updating the app (Rajagopal, 2019).

Prevention: Users were advised to uninstall all the infected apps on their mobile phones. The updates and patches were provided by the mobile solutions and monitoring were done from time to time. Users were recommended to use a multi-layered mobile security solution to prevent unwanted application downloads and adware on their devices.

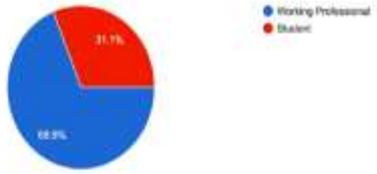
IX. SURVEY

Security Questionnaire for the survey

45 responses

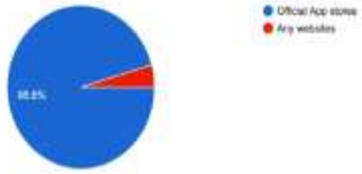
Are you a working professional or a student?

45 responses



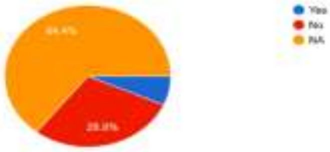
Where do you download your mobile applications from?

45 responses



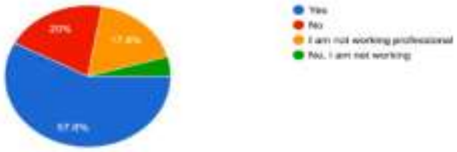
If you have been harassed or cheated online, have you reported it to law enforcement?

45 responses



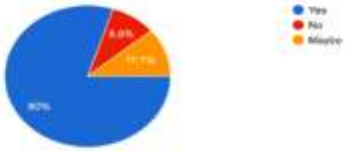
Do you use your mobile phones to manage office related work?

45 responses



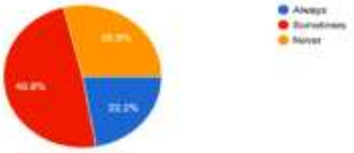
Are you aware of the attacks on mobile devices?

45 responses



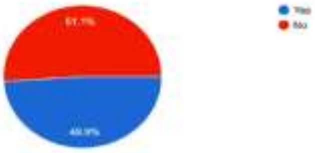
I read all the Terms and Conditions before I install any app/software on my phone?

45 responses



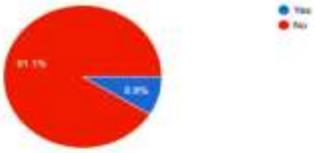
Does your smartphone have anti-virus protection?

45 responses



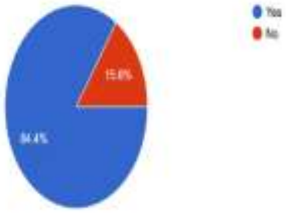
Have you been a victim of cybercrime?

45 responses



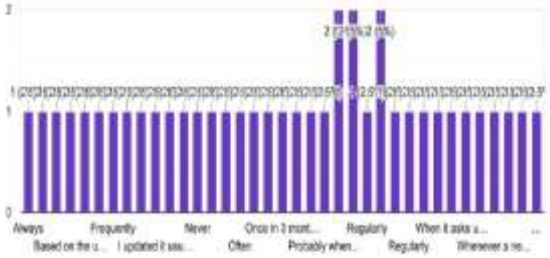
Do you use cloud to backup your data from mobile phone?

45 responses



How often do you update the software of your mobile phones?

40 responses



A survey was conducted among the postgraduate students and working professionals at London Metropolitan University. The purpose of the survey was to discover the awareness among individuals of mobile crimes and security.

The survey was conducted utilizing a questionnaire given to every individual to complete. The questionnaire consisted of 10 questions and it dealt with simple questions on how they are aware of mobile crimes and what actions they take to keep themselves secure from this crime.

From the data collected the most significant observations are as follows. It was seen that 68.9% of the individuals who filled out the survey were working professionals and the rest 31.1% were students. 95.6% of people downloaded their applications from the official app stores which was a positive outcome. When it comes to the usage of anti-virus on mobile phones, 51.1.% of them used the software to keep themselves secure and 48.9% has not been any antivirus. It is seen that 8.9% of people have been victims of cybercrime and have reported time to time to law enforcement. As the usage of mobile phones at the workplace is increasing 80% responded that they use mobile devices to keep productivity going at work. Also, it is seen that 84.4% of people use the cloud to back up their data from mobile devices.

To conclude, it looks like people are not aware of the usage of anti-virus to secure mobile devices. As mobile crimes are increasing at an enterprise level, we also see people making use of mobile devices to work and as cloud usage is also increasing the target on the mobile cloud by attackers will also be rapid in the future.

X. CONCLUSION

Security threats related to mobile devices are the most critical. There are many different kinds of software security hazards, as well as several risks connected to mobile devices with ways to reduce these risks. Security specialists face challenges in defending against mobile threats due to the tremendous growth of mobile threats. Social engineering attacks are one of the biggest security risks that an organization faces. Corporate companies are more prone to insider threats but they deny mentioning or discussing these threats fearing the loss of business. This paper reviewed the kinds of threats in detail and discussed the countermeasures. Looking at the survey we can also conclude that mobile phones are prone to more attacks in the coming days.

XI. REFERENCES

[1] Omer Faruqe Jubaer, M. S., Rumon, A. A., Khan, F. R., Suma, T. A., Dhar, P., & Badhan, P. D. (n.d.). Cyber Stalking is a Cybercrime or not: Hosting a new cybercrime. online Bibliophiles.

[2] Abdul Quadir Md, Dibyanshu Jaiswal, Jay Daftari, Sabireen Haneef, Celestine Iwendi, & Sanjiv Kumar Jain. (2022). Efficient Dynamic Phishing Safeguard System Using Neural Boost Phishing Protection. (A. Gangopadhyay, Ed.) MDPI, 1-17.

[3] Nwabineli, T. C., Felix, C., & Aguboshim, F. (2021). Strategies for Identity Theft Prevention and Countermeasures in Nigeria:A Narrative Study. International Journal of Advances in Engineering and Management (IJAEM), 3(1), 826-832.

[4] Njuguna, D., Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attaks Mitigation Strategies. International Journal of Computer and Information Technology (, 11(1), 9-13.

[5] Gilibrays, G., Matovu, D., Egwar, A. A., & Bongomin, O. (2022). An application-based framework for curbing mobile phone-related crimes: Results of a preliminary study in Eastern Uganda. 1-15.

[6] R. Mistry, N., Dahiya, M., & P. Sanghvi, H. (2013). Preventive Actions to Emerging Threats in Smart Devices Security. The International Journal of FORENSIC COMPUTER SCIENCE, 20-26.

[7] Lemos, R. (2022). DarkReading. Retrieved from https://www.darkreading.com/endpoint/mobile-threats-skyrocket

[8] Vashisht, S., Gupta, S., Singh, D., & Mudgal, A. (2016). EMERGING THREATS IN MOBILE COMMUNICATION SYSTEM. International Conference on Innovation and Challenges in Cyber Security (pp. 41-44). IEEE.

[9] Sophos. (2021). Sophos 2022 Threat Report.

[10] Kharb, L. (2017). Cyber Crimes Becoming Threat to Cyber Security. International Journal of Engineering and Management Research, 7(2), 48-51.

[11] Hakhroo, B. (2020). A STUDY ON TYPES OF CYBER CRIMES AND CYBER ATTACKS IN INDIA. International Journal of Creative Research Thoughts (IJCRT), 8(11), 1257-1260.

[12] Narula, K. (2019). Retrieved Nov 18, 2022, from legitly.in: https://legitly.in/2019/08/mobile-phone-crimes/

[13] Aksakalli, I. K. (2019). Using convolutional neural network for Android malware detection. information and computer technologies, 29-35.

[14] S. Jones, K., E. Armstrong, M., K. Tornblad, M., & Namin, A. S. (2022). How Social Engineers User Persuasion Principles During Vishing Attacks. Information and Computer Security.

[15] Wu, L. (2019). Trendmicro. Retrieved Nov 20, 2022, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/agent-smith-malware-infecting-android-apps-devices-for-adware

[16] PHILLIPS, G. (2019). MUO. Retrieved Nov 20, 2022, from https://www.makeuseof.com/tag/agent-smith-malware/

[17] Rajagopal, A. (2019). Cyber Security Hub. Retrieved Nov 21, 2022, from https://www.cshub.com/malware/articles/incident-of-the-week-malware-infects-25m-android-phones

[18] Legitly. (2019). Retrieved Nov 20, 2022, from https://legitly.in/2019/08/mobile-phone-crimes/

[19] mobliciti. (2022). Retrieved Nov 19, 2022, from https://www.mobliciti.com/the-current-state-of-mobile-malware/

[20] Stacy Collett. (2022). NETWORKWORLD. Retrieved Nov 20, 2022, from https://www.networkworld.com/article/2177072/five-new-threats-to-your-mobile-device-security.html

[21] Yoon, S. (2014). Security Threats Analysis for Android based Mobile Device. ICTC (pp. 775-776). IEEE.

[22] Chiffelle, O. (2019). Ethical and Unethical Hacking. The International Library of Ethics, Law and Technology, 179-203.

[23] Huseynov, F. (2021). A SURVEY STUDY EVALUATING INTERNET USERS' PRONENESS TO FALL PREY TO SOCIAL ENGINEERING ATTACKS. 5th ASIA PACIFIC International Modern Sciences Congress, (pp. 127-132).

[24] Techslang. (2022). Retrieved Nov 19, 2022, from Techslang: https://www.techslang.com/definition/what-is-bluejacking/