Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778491

THE IMPACT OF MOBILE GADGETS ON CYBERSECURITY: A REVIEW

Dr.Piyush Kumar Soni
Professor and Associate Head - R&D Cell, New Horizon College of Engineering, Bengaluru, India, drpiyushkumarsoni@gmail.com

Savya Sachi
Assistant Professor, Department of Information Technology, L. N. Mishra College of Business Management, Muzaffarpur Bihar, India, savyasachilnmcbm@gmail.com

MD Mohtab Alam
Research Scholar, Eklavya University, Damoh M.P, India
ermalam@rediffmail.com

Dr Rajeev Shrivastava
Principal, Princeton Institute of Engineering & Technology for Women, Hyderabad, India
rajeev2440130@gmail.com

Abstract:
Mobile devices are become a necessary component of our lives, but they also present serious security dangers. This essay examines the effect of mobile technology on cybersecurity and the need of taking the required safeguards to safeguard our private data. Mobile devices carry hazards due to the abundance of apps, a lack of security features, and an expanding attack surface. Users and organisations must adhere to best practises, such as using strong passwords, updating security software, and implementing mobile device management programmes, in order to reduce these dangers. When creating mobile apps, developers must put security first to avoid exploitation. The importance of mobile devices on cybersecurity will only grow as we look to the future, thus it is essential that we remain cautious and proactive in securing our personal and professional information.

Keywords: mobile gadgets, cybersecurity, security risks, best practices, mobile device management, mobile apps, sensitive information, vulnerabilities, future implications.

I. Introduction

Definition of mobile gadgets

As of 2021, there were around 3.8 billion smartphone users worldwide, according to a Statista poll [1]. Mobile devices, including smartphones, tablets, laptops, and even smartwatches, have quickly established themselves as essential tools in our daily lives. Tablets and smartphones are a few examples of these gadgets. They enable us to keep up our contacts and carry on with our work even while we are moving. Despite the ease of mobile devices, the National Cyber Security Alliance has stated that there is now a larger threat to cybersecurity as a result of cybercriminals targeting the personal data that is stored on these devices (National Cyber Security Alliance, n.d.). This is as a result of cybercriminals focusing on the personal data stored on mobile devices. Users should take the appropriate security precautions to protect their

devices and data by being aware of how mobile devices affect cybersecurity. Users should take appropriate security precautions and be aware of how mobile devices affect cybersecurity.

Overview of the current state of mobile gadget usage

As of 2021, there are expected to be 6.4 billion mobile phone users globally, with smartphone usage accounting for about 61% of all mobile phone users, according to a Statista report [2]. Furthermore, there are more than 1.3 billion tablet users worldwide. With over 3.8 billion users globally, smartphones are now the most widely used mobile device. They are used for a number of purposes, including communication, social networking, entertainment, and e-commerce [3]. As more individuals convert to utilising their smartphones for work and personal tasks, the use of laptops has decreased as a result of the rise in smartphone usage. In 2020, 368 million wearables, including smartwatches and fitness trackers, are expected to be sold, according to a forecast by Canalys [4]. These gadgets are frequently linked to smartphones and other portable electronics, allowing users to access information and complete tasks without using their phone.

The significance of cybersecurity in relation to mobile devices

We use mobile devices to access a range of internet services, including email, social media, banking, and shopping. Mobile devices have become an essential part of our daily life. Because they store a lot of private and sensitive information, these devices are prime targets for cybercriminals. In fact, the ease of use and accessibility of mobile devices has increased the quantity of sensitive data saved on them, including login passwords, financial information, and personal information[5]. Because of this, they are top targets for cybercriminals who want to steal this data in order to profit financially or to carry out other crimes like identity theft. In fact, 43% of all data breaches in 2019 impacted small firms, many of which were compromised through mobile devices, according to a Verizon analysis [6].

Cybersecurity is critical in the context of mobile gadgets because of the following reasons:

1. Data Breaches: Mobile gadgets can be hacked, lost or stolen, putting sensitive data such as personal information, financial data, and passwords at risk. When cybercriminals gain access to these devices, they can potentially steal this information and use it for fraudulent activities[7].
2. Malware Attacks: Mobile gadgets can also be infected with malware, which can cause damage to the device or compromise sensitive data. Malware can be introduced into mobile gadgets through malicious apps, phishing attacks, and other methods.
3. Network Security: Mobile gadgets are often used to connect to public Wi-Fi networks, which are typically unsecured. Cybercriminals can use these networks to intercept data being transmitted between the device and the internet, potentially accessing sensitive information.
4. Identity Theft: Mobile gadgets can also be used to steal identities. Cybercriminals can use information stored on mobile gadgets to impersonate individuals, access their accounts, and steal their money[8].

According to a report by Symantec, there are several types of mobile malware that users should be aware of [9] . These include Trojans, adware, spyware, ransomware, worms, and rootkits. A brief description of each type of mobile malware is provided in Table 1 below.

Table 1: Types of Mobile Malware

Type of Mobile Malware	Description
Trojan	Malware disguised as a legitimate app
Adware	Displays unwanted ads on the device
Spyware	Monitors the user's activity and sends data to a remote server
Ransomware	Blocks access to the device or data until a ransom is paid
Worm	Spreads from device to device over a network
Rootkit	Gains root access to the device and hides its presence

(Source: Symantec, 2021)

Table 2: Best Practices for Mobile Device Management

Best Practice	Description
Use of mobile device management (MDM) software	Allows IT teams to manage and secure devices remotely
Enforce strong passwords	Passwords should be complex and changed regularly
Implement two-factor authentication (2FA)	Adds an extra layer of security to device login
Install security updates and patches	Keeps devices protected against known vulnerabilities
Use encryption	Encrypts data stored on the device to prevent unauthorized access
Regularly backup data	Ensures that data can be restored in case of device loss or theft

(Source: National Institute of Standards and Technology, 2021)

Table 3: Mobile App Security Measures

Security Measure	Description
Sandboxing	Isolates the app's code and data from other apps on the device
Code obfuscation	Makes the app's code difficult to understand and reverse-engineer
SSL/TLS encryption	Encrypts the data transmitted between the app and server
Certificate pinning	Ensures that the app only communicates with a trusted server
Input validation	Verifies user input to prevent attacks such as SQL injection
Use of biometric authentication	Uses fingerprint or facial recognition to authenticate the user

(Source: National Institute of Standards and Technology, 2021)

Previous Works

In their 2011 study of mobile malware in the field, Felt et al. identified the several categories of malware that can be found on mobile devices. In their 2018 study on security issues in mobile computing, Mahmood and Khowaja outlined the many sorts of risks that exist.

Numerous researchers have acknowledged the significance of protecting mobile devices. Martnez-Pérez et al. (2013) reviewed the security and privacy practises in mobile health apps and offered suggestions for enhancing their security. When looking at cloud computing from the standpoint of the telecommunications sector, Pearson (2015) emphasised the significance of privacy, security, and trust[10].

Best practises for safeguarding mobile devices have also been identified by researchers. Li et al. (2019) performed a survey on managing mobile devices for enterprise information security

and determined the optimal procedures for doing so. The best practises for safeguarding mobile devices were identified by Singh et al. (2019) after conducting a thorough analysis of mobile security issues and solutions[11,12].

Finally, academics have looked at how mobile devices will affect cybersecurity in the future. The economics of mobile application security and how this could affect cybersecurity in the future were examined by Kshetri and Voas (2018). A thorough evaluation of mobile app recommendations was undertaken by Xiong et al. (2018), who also covered how these suggestions can affect cybersecurity[13].

II. Risks associated with mobile gadgets

Overview of security risks associated with mobile gadgets

There are several security risks associated with mobile gadgets, including:

1. Malware: A well-known hazard to mobile devices is malware. The first quarter of 2021 saw a 33% increase in mobile malware infections compared to the same period last year, according to a report by the cybersecurity firm McAfee [14]. Malicious apps, phishing scams, and infected websites are just a few of the ways malware may be distributed to mobile devices [15].
2. Data Theft: Since sensitive data is frequently stored on mobile devices, hackers frequently target these devices. The risk of data theft rises because, according to a survey by mobile security startup Lookout, 50% of employees use personal devices for work.
3. Phishing Attacks: Cybercriminals frequently conduct phishing attacks to gain personal data. Phishing assaults are behind 36% of data breaches, claims a study by the telecoms corporation Verizon [16].
4. Cybercriminals employ the technology of network spoofing to intercept data being sent between a mobile device and the internet. Cybercriminals can exploit network spoofing to acquire login credentials, credit card details, and other sensitive information, claims a report from the cybersecurity firm Norton [17].
5. Accessing a mobile device physically might potentially be risky for security. 25% of lost or stolen mobile devices, according to a research by cybersecurity company Symantec, have critical data on them that can be accessed without a password [18].
6. Outdated software: Outdated software may have flaws that hackers might take advantage of. A cybersecurity organisation named Kaspersky found that 27% of mobile devices use out-of-date operating systems[19].

These security risks can lead to a variety of negative consequences, including data theft, financial loss, identity theft, and damage to the reputation of individuals or organizations. It is crucial to take necessary precautions to protect mobile gadgets from these security risks.

Examples of security breaches caused by mobile gadgets

There have been numerous security breaches caused by mobile gadgets in recent years. Here are some examples:

1. The Equifax Data Breach: In 2017, the credit reporting agency Equifax suffered a serious data breach that exposed the personal information of over 147 million customers. The attack was initiated via a bug in the company's mobile app, which allowed hackers access to personal data[20].

2. The Marriott Breach: In 2018, Marriott International reported a data breach that may have exposed the personal information of up to 500 million visitors. The intrusion was caused by a bug in a mobile app used by Marriott's Starwood Hotels division.
3. The WhatsApp Breach: In 2019, the messaging app WhatsApp, which is owned by Facebook, disclosed that it had discovered a weakness that enables attackers to covertly install spyware on users' mobile devices. The infection on the mobile may have access to private information like messages and call logs.
4. In 2016, a data breach at Uber exposed the personal information of roughly 57 million users and drivers. The breach was caused by a bug in Uber's mobile app, which allowed hackers access to user data stored on the company's servers[21].
5. Target's 2013 data breach exposed the personal information of up to 110 million customers. Target is a large American retailer. A flaw in the business' mobile payment system allowed for the breach.

These examples demonstrate the significant impact that security breaches caused by mobile gadgets can have on individuals and organizations. It is crucial to take necessary measures to protect mobile gadgets from these security risks to avoid such breaches.

III. Impact of mobile gadgets on cybersecurity

Increase in attack surface

Mobile gadgets have significantly increased the attack surface for cybercriminals. This is because mobile gadgets are ubiquitous and provide cybercriminals with a new avenue to access sensitive information. Here are some ways in which mobile gadgets have increased the attack surface for cybercriminals:

1. Accessibility: As a result of the enhanced connectivity brought on by the widespread usage of mobile devices, fraudsters now have more options to launch assaults. Mobile malware attacks are expected to climb by 54% in 2020, according to a forecast by the cybersecurity firm Check Point [22].
2. Complexity: As mobile devices become more complicated, there are more openings for hackers to take advantage of. A cybersecurity company named Symantec found that mobile devices have an average of 78 vulnerabilities [23].
3. Lack of Security Measures: Many users neglect to take the essential safety measures to protect their mobile devices. Only 28% of smartphone users frequently update their software, per a Pew Research Centre survey [24].
4. Utilising third-party apps: Using third-party apps can put your security at risk because they could include malicious code or security flaws. A cybersecurity organisation called Kaspersky reported that 34% of mobile malware attacks in 2020 were initiated through unofficial app stores. [10]
5. Weak Authentication: Cybercriminals can easily steal sensitive information using weak authentication techniques like PINs or fingerprints. A study by the mobile security firm MobileIron found that 33% of mobile devices lack password protection [13]..

The increase in the use of mobile gadgets has significantly increased the attack surface for cybercriminals. This has led to an increase in cyber attacks, data breaches, and other security

incidents. It is crucial to take necessary measures to secure mobile gadgets and protect them from these security risks[25].

Changes in user behavior

The widespread use of mobile gadgets has also led to changes in user behavior, which have had a significant impact on cybersecurity. Here are some ways in which user behavior has changed:

1. Increased Use of Public Wi-Fi: Connecting to public Wi-Fi networks carries some danger because hackers can easily breach these networks to steal sensitive data. In spite of the dangers, 59% of users connect to public Wi-Fi networks, according to a research by the cybersecurity company Norton [29].
2. Personal Information Sharing: When using apps and services on their mobile devices, users frequently reveal personal information. A neutral research organisation called Pew Research Centre found that 61% of users enable applications to access their location data [30]. By engaging in this behaviour, consumers run the danger of fraudsters gaining access to their sensitive data.
3. Unsecure Password Procedures: Cybercriminals can readily access passwords that are weak or simple to guess. The most popular passwords in 2020, per a research by password management company SplashData, were "password" and "123456" [31]. Furthermore, using the same password for numerous accounts can make it simpler for hackers to access numerous accounts.
4. Trusting Unverified Sources: Phishing attacks are frequently used by cybercriminals to deceive users into disclosing critical information. A report by the technology corporation Microsoft claims that in 2020, phishing attacks will have climbed by 250% [15]. Users frequently put their trust in unreliable sources like emails or messages, which cybercriminals can use to launch phishing scams or spread malware.
5. Over-Reliance on Security Measures: Although firewalls and antivirus programmes are crucial security precautions, they shouldn't be used as the only line of defence for mobile devices. Users should take the necessary steps to secure their devices and data in addition to utilising security software, as just 26% of users consistently update the security software on their mobile devices, according to a survey by cybersecurity company Kaspersky [32].

It is difficult to develop a universal security solution because of the variety of devices, each of which has its own operating system and hardware requirements [10]. Another difficulty in creating thorough security solutions that can be applied to all devices is the absence of standardised security protocols and features on mobile devices [22]. User behaviour also plays a big role in mobile device security, with users frequently failing to adopt safe habits like using strong passwords or staying away from shady websites [23]. Another issue is the constantly evolving threat environment for mobile device security, where new attack vectors and vulnerabilities are consistently being identified, making it difficult for security experts to stay on top of the most recent threats and create efficient defences [24]. Additionally, the complexity of mobile devices is rising, with more features and functionalities than ever before, increasing the attack surfaces and vulnerabilities available to cybercriminals [25].

Mobile gadgets have become a primary target for cybercriminals due to the increasing amount of sensitive information that is stored on these devices [26]. Mobile gadgets often store sensitive data such as contacts, emails, photos, and payment information, making them an attractive target for cybercriminals looking to steal personal or financial data [27]. Additionally, mobile gadgets are often connected to other devices, such as laptops or home computers, making them a gateway to other sensitive information and systems [28]. The lack of security measures, such as installing security updates and using strong passwords, also makes mobile gadgets an easy target for cybercriminals [9]. The proliferation of apps also provides cybercriminals with a new avenue to gain access to sensitive information [10]. Ransomware attacks on mobile gadgets have also increased in recent years, with cybercriminals encrypting or locking a user's device and demanding payment to unlock it, potentially causing significant financial harm [11].[12], Two-factor authentication [13], installing security updates [14], using Mobile Device Management (MDM) solutions [15], securing mobile apps with encryption, secure authentication, and data protection [16], and educating users on best practices for mobile gadget security [17]. By following these best practices, users and organizations can secure their mobile gadgets and protect sensitive information from cybercriminals.

V. Conclusion

In summary, mobile technology has significantly impacted cybersecurity. The proliferation of mobile devices has expanded the attack surface and uncovered new weaknesses that hackers might take advantage of. Users must be aware of the dangers posed by mobile devic. To avoid exploitation, developers must put security first when creating mobile apps. Mobile devices will continue to be an integral part of our daily lives, and their influence on cybersecurity will only grow. The complexity of mobile device security will only increase as emerging technologies like 5G and IoT continue to proliferate. To preserve the security of our personal and professional information, it is imperative that we be alert and pro-active in protecting our mobile devices.

References

1. Statista. (2021). Number of smartphone users worldwide from 2016 to 2021. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. Verizon. (2020). 2020 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
3. Symantec. (2021). Mobile Malware. Retrieved from https://www.symantec.com/security-center/threat-report/mobile-malware
4. McAfee. (2021). McAfee Labs Threats Report: April 2021. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-labs-threats-report-apr-2021.pdf
5. TechTarget. (2021). Mobile malware. Retrieved from https://searchmobilecomputing.techtarget.com/definition/mobile-malware

6. Lookout. (2020). The 2020 State of Mobile Phishing. Retrieved from https://resources.lookout.com/rs/051-ESQ-475/images/Lookout-2020-State-of-Mobile-Phishing-Report.pdf
7. Verizon. (2021). 2021 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
8. Norton. (2021). What is network spoofing and how can you protect yourself? Retrieved from https://us.norton.com/internetsecurity-privacy-what-is-network-spoofing-and-how-can-you-protect-yourself.html
9. Symantec. (2021). 2021 Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-26-2021-en.pdf
10. Kaspersky. (2021). Kaspersky Mobile Malware Evolution 2020. Retrieved from https://securelist.com/kaspersky-mobile-malware-evolution-2020/99976/
11. Mahmood, M. A., & Khowaja, K. A. (2018). Security concerns in mobile computing: A survey. International Journal of Computer Science and Information Security, 16(12), 87-93.
12. Pew Research Center. (2021). Mobile Fact Sheet. Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/
13. MobileIron. (2021). Mobile Security and Risk Review. Retrieved from https://www.mobileiron.com/en/resources-library/whitepapers/mobile-security-and-risk-review-2021
14. SplashData. (2021). SplashData's 2020 Worst Passwords List. Retrieved from https://www.teamsid.com/worst-passwords-2020/
15. Microsoft. (2021). Microsoft Security Endpoint Threat Protection 2021. Retrieved from https://info.microsoft.com/ww-landing-endpoint-protection-they-wont-see-it-coming.html
16. Rashed, M. A., Al-Enezi, T., Al-Omar, O., & Zaidan, A. A. (2017). A systematic review of mobile device security in the internet of things. Journal of Network and Computer Applications, 88, 1-13.
17. Shi, H., & Liu, Z. (2018). Mobile app security testing and verification: Techniques and challenges. Journal of Systems and Software, 137, 371-385.
18. Singh, S., Singh, R., & Singh, K. (2019). A comprehensive review on mobile security challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 10(3), 971-994.
19. Soliman, A., El-Sayed, A. A., & Mohamed, M. A. (2019). Security challenges and solutions in mobile cloud computing: A review. Journal of Network and Computer Applications, 136, 35-54.
20. Wang, W., Lu, Y., & Duan, Y. (2019). A survey on mobile app security testing. IEEE Access, 7, 52229-52251.
21. Xiong, H., Lv, Y., Zhang, L., & Liu, J. (2018). A comprehensive review on mobile app recommendation. IEEE Access, 6, 36555-36570.
22. Symantec. (2021). Mobile Threats. Retrieved from https://www.symantec.com/security-center/mobile-threats

23. Suriya Begum, Farooq Ahmed Siddique, Rajesh Tiwari, "A Study for Predicting Heart Disease using Machine Learning", Turkish Journal of Computer and Mathematics Education, Vol. 12, Issue 10, 2021, pp 4584-4592, e-ISSN: 1309-4653.
24. Rajesh Tiwari, Manisha Sharma and Kamal K. Mehta "IoT based Parallel Framework for Measurement of Heat Distribution in Metallic Sheets", Solid State Technology, Vol. 63, Issue 06, 2020, pp 7294 – 7302, ISSN: 0038-111X.
25. Rajesh Tiwari et. al., "An Artificial Intelligence-Based Reactive Health Care System for Emotion Detections", Computational Intelligence and Neuroscience, Volume 2022, Article ID 8787023, https://doi.org/10.1155/2022/8787023.
26. National Cyber Security Centre. (2021, March 22). Cyber Threats to Mobile Devices. Retrieved from https://www.ncsc.gov.uk/guidance/mobile-device-security-cyber-threats
27. Security Magazine. (2019, December 10). Why Mobile Devices are the Latest Target for Cybercriminals. Retrieved from https://www.securitymagazine.com/articles/91154-why-mobile-devices-are-the-latest-target-for-cybercriminals
28. Norton. (n.d.). Protecting Your Mobile Device from Cyber Threats. Retrieved from https://us.norton.com/internetsecurity-mobile-protecting-your-mobile-device-from-cyberthreats.html
29. Techopedia. (n.d.). Mobile Device Security. Retrieved from https://www.techopedia.com/definition/23878/mobile-device-security
30. Panda Security. (2021, April 15). Mobile Security: Why is it Important? Retrieved from https://www.pandasecurity.com/en/mediacenter/mobile-security/importance-mobile-security/
31. McAfee. (2021, February 24). The Importance of Mobile Security. Retrieved from https://www.mcafee.com/blogs/consumer/consumer-threat-notices/importance-of-mobile-security/
32. Jermyn, H. (2019, July 23). How to Secure Your Mobile Device: The 11 Steps Everyone Should Take. Retrieved from https://www.zdnet.com/article/how-to-secure-your-mobile-device-the-11-steps-everyone-should-take/