Gurukul International Multidisciplinary Research Journal (GIMRJ)*with*
International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0019

e-ISSN No. 2394-8426
Special Issue on
Cyber Crime and Social Media
Issue–III(II), Volume–XIII

# Impact of Mobile Malware and Mobile Hacking Cases in India

**Dr. Kavita Kanholkar**
Orange City College of Social Work,
Nagpur
Kavita10kanholkar@gmail.com

## Introduction

Telecommunication was introduced in India long back in the year 1882. There was a mushroom growth of telecommunication after the advent of internet and mobile technology in India. It was on August 15, 1995 when the first mobile telephone service started on a non-commercial basis in India. On the same day internet was also introduced in this nation. After the liberation and privatization in this area India didn't look back; telecommunication conquered life of citizens of India and in no time India's telecommunication network became the second largest in the world. In this dot com era, a person is looked with surprise if he is not a mobile user. Impact of Cell Phones on Human Life Communication technology has left no aspect of human life untouched. Even our morning alarm clocks are been replaced by the mobile cell phones. Technology is constantly bringing advancement in our mobile cell phones. The technological advancement provided opportunities to the miscreants in the society, who are using technology for their selfish gains. There are cases where hackers have breached in Nokia's Symbian, Apple's iOS and Google's android operating system. Thus, to be safe we must be vigilant. But it is really unfortunate that whenever a discussion about cybercrime ignites, a particular class of the people escapes the discussion saying that; they neither use computers nor they use internet for communication and therefore cybercrime is not a threat for them. On the ground that cannot become its victim, but they have absolutely no idea that knowingly or unknowingly they can be adversely affected by cybercrime. Every person using an internet, blue tooth or even an infra-red enabled cell phone can easily be fished in the web of cyber criminals. Is Cell Phone a computer? The broadest definition of cybercrime that is available is-any crime where computer is used either as a tool or weapon. In common parlance computer is understood to be a desktop, laptop or a palm top. But as per Wikipedia: "A computer in a general-purpose device that can be programmed to carry out a finest set of arithmetic or logical operation."

Common Cyber Crimes Associated with Cell Phones Bluebugging: As the name suggests this is the attack on the mobile cell phone through Bluetooth. Bluetooth is not a stranger term today. Almost every mobile cell phone is embedded with Bluetooth technology. We use Bluetooth for sharing photos, audio or video files etc. Bluebugging allows the hacker to take over complete control over your mobile phone. The victim cannot even realize that his mobile cell phone is attacked, because even if the Bluetooth device is disabled or turned off the mobile cell phone can be victim of this attack. Bluebugging allows the hacker to read the information in your mobile cell phone, he can access Published in Articles section of www.manupatra.com Bharati Law Review, April – June, 2014 20 calendar, address book etc., he can make calls and even send messages. The hacker can even listen to the conversation of your mobile phone. Every time you receive a call on your infected mobile cell phone the call is also forwarded to the hacker and he can listen the conversation.

Use of mobile making is increased on the mobile phones. Mobile phones are now used for online shopping and managing banking transactions. This has made mobile cell phone an easy victim of Vishing. Motive of the hacker is to get easy money. These attacks are similar to phishing attacks. It includes identity theft like credit cards numbers and other secret information. Scammer calls the victim and by use of his voice tries to extract the confidential information of the victim. Therefore, every mobile user must be vigilant towards these fooling calls. We should not be carried away by the lucrative offers or scheme the scammer offers us.

**Mobile Malware**

Mobile malware refers to malicious software specifically designed to exploit vulnerabilities in mobile devices and operating systems. It can encompass a wide range of threats, including viruses, worms, Trojans, adware, and spyware. As mobile devices become more sophisticated and technologically advanced, so does the complexity and proliferation of mobile malware Malware is one of the biggest threats to mobile cell phones. It is a program (software) designed to perform malicious activities in the device infected. Malware enters the mobile cell phone of victim through SMS, file transfer, downloading programs from internet etc. Malware enters and functions in the victim are mobile without his knowledge and perform several malicious activities like usage of talk time, etc. 4. Smishing: In this e-age the term “SMS” do not need any introduction.

It signifies Short Message Service. It is a common term for sharing messages on mobile phone. This service is the one of the most used services on mobile phones. Hence criminals are targeting it as a tool to satisfy their greed. Smishing is a security attack in which the user is sent an SMS posing as a lucrative service that indulges them into exposing their personal information which is later misused. This is also used for introducing a malware in the cell phone of the user. These are alike Phishing and Vishing attacks in which personal confidential information is gained and later misused. In these attacks the criminal obtains the internet banking passwords, credit card details, email ID and password etc.

**Types of Mobile Malware**

**Viruses:** These are malicious programs that can replicate and spread from device to device. They can cause damage to files, applications, and the overall system.

**Worms:** Similar to viruses, worms can replicate themselves, but they do not require a host file. They can spread rapidly across networks and devices.**Trojans:** These are disguised as legitimate applications or files but are designed to perform malicious activities. They can steal personal data, create a backdoor for attackers, or even take control of the device.

**Adware:** Adware displays intrusive advertisements on the device, often redirecting users to unwanted websites or prompting them to install other malicious applications.

**Spyware:** This type of malware silently gathers sensitive information from the device, such as passwords, banking details, session cookies, and browsing habits, without the user’s consent.

Cybercriminals are constantly innovating and developing new forms of malware to stay one step ahead of security measures, although when looking at recaptured logs in the Spy Cloud database we primarily see data that was exfiltrated by one or more mobile Trojans – commonly referred to as “RATs,” or remote access Trojans. Notably, we’re seeing Trojan malware campaigns largely target banking and financial service providers to perpetuate fraud, with the number of observed mobile banking Trojans doubling last year.

**The Impact of Mobile Malware on Organizations**

The impact of mobile malware extends beyond individual users and can also have significant consequences for businesses and organizations. A successful mobile malware attack can compromise sensitive corporate data, disrupt operations, and damage a company’s reputation.

If sensitive or proprietary data stored on smartphones and tablets, or data transmitted over mobile networks, is compromised by an attacker, it can lead to a data breach, potentially resulting in regulatory fines, lawsuits, and reputational damage. The loss of intellectual property or customer information can be particularly damaging.

Mobile malware infections can also disrupt business operations. For example, if mobile devices used for work become infected, employees may be unable to perform their duties, resulting in productivity losses.

**How Mobile Malware Spreads**

Understanding how mobile malware spreads is a critical piece of the puzzle for both individuals and organizations.

Malicious Apps and Downloads:

As mentioned above, one common method used for spreading mobile malware is through malicious applications or downloads. Malware-infected apps can be disguised as legitimate software, making it challenging for users to distinguish between genuine and malicious ones. In some cases, infected applications may ask the user to grant the app certain permissions, which then allow the attacker to perform malicious actions like stealing banking credentials.Phishing and Social Engineering:

Phishing attacks are also prevalent in the mobile ecosystem, and it’s been reported that 82% of phishing sites now target mobile users. Cybercriminals may use social engineering techniques like sending fraudulent messages or emails to deceive users into revealing sensitive information, clicking on a malicious link, or downloading a malicious app. Supply Chain:

Recently, there have also been campaigns to spread mobile malware via the supply chain. As seen with the Bad box and Peach Pit Trojans, some knock-off Android devices are being sold to mobile users with malware pre-installed on the device, capitalizing on consumers looking for a good deal on a new phone.

**Role of Operating Systems in Mobile Malware**

Android and iOS are the two dominant operating systems in the mobile market, each with its strengths and vulnerabilities when it comes to malware. Android, due to its open nature, is particularly susceptible to malware attacks, especially when users download apps from unofficial sources. In a recent research study, mobile malware was found on 1 out of 20 Android devices in 2022.

Mobile malware poses plenty of risks and implications for users and organizations. For users, though, the impacts are generally personal data loss, stolen credentials, and financial fraud.

**Preventing and Combating Mobile Malware**

To combat the growing threat of mobile malware, smartphones have various security measures built in. These include regular software updates and app store security checks, but user education around safe browsing and downloading practices remains a key component of attack prevention.

**User Education Countermeasures**

Education and training for mobile users advising them to exercise caution while clicking on links or providing confidential data, even if it appears to come from a trusted source, is a standard part of a prevention strategy. It is crucial for individuals to be aware of the risks and take necessary precautions to protect their personal data and financial security. Some best practices to share with users for mobile security include:

- □Only download apps from official and trusted sources like Google Play Store or Apple App Store.
- □Regularly update the device's operating system and security software.
- □Avoid clicking on suspicious links or opening attachments from unknown sources.
- □Enable strong passwords or biometric authentication for device lock screens.
- □Be cautious while sharing personal information online or with unrecognized apps. Ask yourself if the app you’ve just installed really needs the permissions it's asking for. For example, does an app for a flashlight really need permissions to access your contact list or send texts and make calls?

**Technology Countermeasures**

Human error will always be part of the equation, but there are an increasing number of technology solutions that can help security teams swing the odds in their favour.

**Défense mechanisms against mobile malware**

Defending against mobile malware can be done by many ways, such as the use of antivirus and anti-malware solutions, mobile device management technologies, secure coding practices for app development, and user awareness and education.

**Antivirus and Anti-malware Solutions**

Antivirus and anti-malware are tools used for protecting mobile devices against malware. These tools scan devices for known malware signatures and behaviour patterns, detecting and removing malicious software before it can cause harm. These tools often include features such as real-time scanning, which monitors device activity for signs of malware infection, and automatic updates, which ensure that the software is always up-to date with the latest malware definitions.

**Mobile Device Management Technologies**

Mobile device management (MDM) systems play a critical role in securing the corporate network.

MDM can be used for the purpose of security procedures, such as using strong passwords or data encryption. These tools can also remotely wipe devices that are lost or stolen, ensuring that sensitive information does not fall into the wrong hands. Additionally, MDM technologies can provide visibility into device activity, helping organizations detect and respond to potential security threats.

**Secure Coding Practices for App Development**

Developers can help prevent mobile malware by following secure coding practices when developing apps. This includes using secure APIs for accessing sensitive data, validating input to prevent injection attacks, and encrypting sensitive data stored on devices. Additionally, developers should regularly update their apps to address known vulnerabilities and follow best practices for secure app distribution.

### User Awareness and Education

User awareness and education are crucial for mobile malware defence. Users should be educated about the risks of mobile malware and how to recognize suspicious activity. This includes avoiding clicking on links or downloading attachments from unknown sources, keeping their devices upto-date, and using strong, unique passwords for their accounts. Users should be encouraged to report any suspicious activity to their organization's IT department.

## Conclusion

•□Mobile malware is a growing problem that can cause big issues for people, businesses, and society.

•□It has looked at how mobile malware has changed over time, the damage it can do, and ways to protect against it.

•□We talked about different types of mobile malware like viruses, worms, Trojans, spyware, ransomware, adware, and rootkits. We also discussed how these harmful programs can affect devices through things like fake apps, dangerous websites, phishing texts, and sneaky software kits. We explored how mobile malware can harm individuals, businesses, and society by stealing personal information, causing financial loss, and disrupting everyday life.

## REFERENCES:

▪□Bharati Law Review, April – June, 2014 18 MOBILE CELL PHONES AND CYBER CRIMES
IN INDIA: HOW SAFE ARE WE? Mr. Nikhil A. Gupta

▪□Civil Judge Junior Division & Judicial Magistrate First class, Newasa, District
Ahmednagar. Published in Articles section of www.manupatra.com Bharati Law Review,
April – June, 2014 19

▪□International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal) e-ISSN: 2582-5208
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.comwww.irjmets.com
@International Research Journal of Modernization in Engineering, Technology and
Science [2844]

▪□International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal) e-ISSN: 2582-5208
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com www.irjmets.com
@International Research Journal of Modernization in Engineering, Technology and
Science [2845]

▪□Ahammed Muntazir M*1, Dr. Rengarajan*2

▪□*1Student of MCA, Dept. Of CS & IT, Jain (Deemed-To-Be-University), Bengaluru, India.
*2Professor, Dept. Of CS & IT, Jain (Deemed-To-Be-University), Bengaluru, India. DOI:

https://www.doi.org/10.56726/IRJMETS56358

▪□K. Kaspersky, "Cabir – the first network worm for mobile phones," Securelist, 2004. [Online]. Available:
https://securelist.com/cabir-the-first-network-worm-for-mobilephones/36138/.

▪□A. Zhou et al., "The state of malicious Android applications: a static analysis approach," in Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 1-10.

▪□A. Abu-El-Haija et al., "Mobile phishing: A review of the literature and future directions," in Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 2017, pp. 95-106.

▪□S. Chakraborty et al., "The impact of mobile device usage characteristics on the security of mobile devices," in Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2015, pp. 567-578.

▪□E. Kaspersky, "The Evolution of Mobile Malware and the Ways to Counter It," Mobile Information Systems, vol. 2017, Article ID 7820456, 2017.