International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 2, Mar.-Apr, 2024, Impact Factor: 8.376

Cybercrime Related To Mobile Phones

Aditi Agrawal

Bharati Vidyapeeth (Deemed To Be University) New Law College, Pune

ABSTRACT

The proliferation of mobile technology in India has brought about unprecedented connectivity and convenience, but it has also opened the door to various forms of cybercrime targeting mobile devices. This research paper delves into the landscape of mobile cybercrime in India, analyzing prevalent trends, challenges, and mitigation strategies.

INTRODUCTION

Modern smartphones that incorporate cutting-edge technology similar to personal computers are quite popular. As a consequence of this, communication is now easier to access and more practical, in this dot com era a person is looked at with surprise if he is not a mobile user. Since smartphones are more user-friendly and inexpensive than traditional devices, recent trends indicate that they have surpassed PC sales. Yet, along with many benefits come many drawbacks this is Because of widespread ignorance and comparatively slow security advancements, users are susceptible to cybercrimes. and attackers have been exploiting this expanding market by using old techniques along with new ones.[1]

These simple-to-use gadgets, which are typically based on a particular operating system, allow their users to install apps on their smartphones per their needs. These apps are the main features of smartphones that improve users' daily lives. However, unlike computers, these devices lack security features. At the same time, these applications require users' personal information, such as email addresses, phone numbers, and photos. Many users neglect to activate the security software that comes with their phones merely because they believe that using their phones for surfing the internet is just as safe as using computers.

Advancements in mobile commerce have made it possible for consumers to buy products and apps via wireless networks, use coupons and tickets, bank, process payments at the point of sale, and even make cash register purchases from their smartphones. However, it is very regrettable that whenever a conversation about cybercrime begins, a certain demographic always seems to disappear from the conversation and claim that; Since they rarely utilize computers or the internet for communication, they are not at risk from cybercrime. Individuals try to conceal their ignorance of cybercrimes by staying in places where they cannot fall victim to them, but they are completely unaware of the potential detrimental impacts that cybercrime may have on them, whether consciously or unknowingly. Anyone utilizing the internet, Bluetooth, or even an infrared-capable smartphone is susceptible to becoming entangled in the web of cybercriminals. In light of this, the goal of this research is to evaluate and assess current best practices as well as security risks to mobile applications. therefore, we put forward the following research question:

What are the security threats to mobile applications and what legal measures can we take to mitigate them?

Is a cell phone a computer?

Cybercrime is defined as any crime where a computer is used as a weapon or as a tool, in the broadest sense currently available. A computer is generally understood to be a desktop, laptop, or palm top.

But as per Wikipedia: “A computer is a general-purpose device that can be programmed to carry out the finest set of arithmetic or logical operation[2].” Also as per Section 2(i) of the Information Technology Act, 2000 (hereinafter the IT Act): “Computer means any electronic, magnetic, optical or other high-speed data processing device or system which performs

[1]PandaLabs. “Quarterly Report PandaLabs (January-March 2011).” http://press.pandasecurity.com/wpcontent/uploads/2011/04/PandaLabs-Report-Q1-2011.pdf

[2]https://racolblegal.com/crimes-committed-through-mobile-phones/

logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.[3]" This wide definition includes all of the devices we use daily to make our lives easier when using computers. Mobile phones are only one example of this.

Evolution of mobile technology

The evolution of mobile technology in India has significantly transformed communication, commerce, and social interactions, bringing unprecedented connectivity and convenience to millions. However, alongside its rapid advancement, mobile technology has also become increasingly vulnerable to cybercrime.

Initially, with the introduction of basic voice and text services, cyber threats were limited. But as mobile devices evolved to become powerful computing platforms with internet connectivity, they became lucrative targets for cybercriminals. The proliferation of smartphones and mobile apps expanded the attack surface, providing cybercriminals with numerous entry points to exploit vulnerabilities.

Cybercrime targeting mobile technology in India has had profound impacts on individuals, businesses, and the nation's cybersecurity landscape. Instances of mobile malware, phishing attacks, identity theft, and financial fraud have led to significant financial losses, data breaches, and erosion of trust in digital platforms. Moreover, the interconnected nature of mobile networks has facilitated the rapid spread of cyber threats, posing challenges for law enforcement agencies and cybersecurity professionals in combating these crimes effectively.

As mobile technology continues to evolve, the threat landscape is expected to become more complex, necessitating concerted efforts to strengthen cybersecurity measures, enhance user awareness, and enforce robust regulatory frameworks to safeguard against cyber threats in India's mobile ecosystem.

Security threats to mobile applications

Users have been empowered and influenced by the mobile revolution to shift nearly all of their daily activities into the mobile environment and what are known as mobile applications.

To ensure that our experience is seamless and convenient, developers give software design meticulous consideration. Though few pause to consider the security implications, people happily install mobile apps and divulge personal information. However Numerous cyberthreats and attacks that compromise the privacy of users can target mobile devices and applicationsThese portable electronics, which fit in our pockets, are meant to safeguard and preserve private data. Users are still vulnerable to various forms of attacks even though Google and Apple provide closed, controlled distribution environments. Here are a handful of them:

. To mitigate the risks associated with cyber threats, it is imperative to comprehend their characteristics.
Are as follows:

1. Phishing

This is a term for a category of electronic crime that involves the unlawful collection of private data via online networks, websites, and online payment systems, including passwords, user names, credit card numbers, and electronic signatures. In an attempt to gain access to the victim's account and obtain personal information, the defaulters send emails with attachments and URLs. The progress of technology makes it challenging for the average person to verify the legitimacy of these emails.

The process of phishing is through the illusion of users entering personal data, which is almost identical to the legitimate site with makes recorded use of phishing described in detail in 1987 and the first used in phishing meaning was in 1996[4]

How phishing works?

Phishers use social media, SMS, emails, and other platforms to identify and prey on the uninformed and vulnerable masses. They monitor user searches and subsequently gather fundamental details about the victim's private information, usually via social media sites like Facebook, LinkedIn, and shopping apps. By sending a convincing and alluring fake email to potential victims, the information gathered from these applications aids in their decision-making and helps them cause financial loss.

[3]https://racolblegal.com/crimes-committed-through-mobile-phones/
[4]00_Chapter_OnCyberCrimes_v1_Reference.pdf

Criminal sanctions for phishing

In India, the Information Technology Act, 2000 (**IT Act**) protects against and penalizes cybercrimes[5]. Section 43 of the IT Act proscribes various offenses, including the unauthorized access of a computer resource. Fraudulently and dishonestly committing an offense under Section 43 of the IT Act can lead to imprisonment of up to 3 years or a fine of up to INR 5,00,000. Additionally, the IT Act punishes the fraudulent or dishonest use of an electronic signature, password, or any other unique identification feature, and using a computer resource for cheating, with imprisonment for up to 3 years and a fine of up to INR 1,00,000.[6]

The Indian Penal Code (IPC) permits prosecution of phishing as; (i) forgery; (ii) '*cheating by personation*'; and (iii) cheating and dishonestly inducing the delivery of property.

2. Click-fraud advertising embedded in apps;

The advertisement link is one of the most lucrative illegal ways to obtain user information on smartphones. Since mobile users lack the anti-defence mechanisms found on computers, they are particularly vulnerable to such links. Usually, the defaulters use gaming or shopping applications to target the victim, where the users are either children or a less cognizant mass. they fascinate the victims with alluring deals and freebies while also gathering pertinent information. the cost to advertisers of fraudulently "clicked" ads, according to data published by the World Federation of Advertisers, tops US $19 billion each year.[7]

3. **Malware;**

Any software designed to compromise or damage a device is referred to as malware; The capabilities of smartphones are rapidly catching up to those of PCs, and hackers are motivated by the same things: extortion, fraud, and the theft of private and corporate data. With so many channels for disseminating malware, hackers are ready to strike.

While stealing usernames and passwords from email or bank accounts is the primary goal of a significant percentage of mobile malware, many malicious apps also have intrusive spying features that allow them to record audio and video, track your location, or even erase your content and data. These more sophisticated features are being used by more attacks as mobile malware develops.

There are several ways that malware can infect mobile devices. A typical approach involves the use of malicious apps. Cybercriminals might make phony apps that seem authentic but are actually infected with malware. It's important to only download apps from reliable sources because these apps can be found outside of official app stores. Furthermore, some malicious apps might trick users into downloading them by disguising themselves as helpful or well-liked apps.

Malicious links or attachments in emails, messages, or web pages are another way that malware can infect mobile devices. Malware may install on the device if you click on these links or download infected files. It's crucial to exercise caution and refrain from downloading files from unreliable sources or clicking on dubious links.

4. Spam

Emails or messages that are unsolicited or irrelevant and are sent to a large number of users on the Internet with the intention of advertising, phishing, spreading malware, etc. are referred to as spam.

Spam email is the most common type that is widely recognized. Similar abuses in other media are also referred to by this term, including spam from instant messaging, web search engines, blogs, wikis, online classified ads, mobile phone messaging, internet forums, and social networking. Additionally, the size of a spam email has increased significantly due to the ease with which spammers can enter the system, even after sending emails that prohibit spam.

5. Cyber Stalking;

Lambert Royakkers (Royakkers, 2000) defined stalking crime as follows: "Any person is guilty of the stalking crime who: wilfully, maliciously, trace another person with the intent of placing that person in reasonable fear of death, sexual assault, or great bodily injury to that person, any member of that person's family, or anyone with whom that person has a sexual or intimate relationship".[8]

[5]https://www.studocu.com/in/document/chanakya-national-law-university/business-administration/cyber-2247-final-draft/75197583
[6]https://www.lexology.com/library/detail.aspx?g=a6e35288-c18d-433f-83c1-4525d348d6cf
[7]Mobile_Security_Threats_and_Best_Practices.pdf
[8]00_Chapter_OnCyberCrimes_v1_Reference.pdf

Here are some signs that someone may be a victim of cyberstalking:

- Unwanted and excessive communication: The victim receives a high volume of unwanted messages, emails, or comments, often with a threatening or harassing tone.
- Online surveillance: The cyber stalker monitors the victim's online activities, such as tracking their location, checking their social media posts, or hacking into their accounts.
- Impersonation: The cyber stalker may create fake profiles or impersonate the victim online, spreading false information or engaging in harmful behavior.
- Doxing: This involves the public release of the victim's personal information, such as their address, phone number, or workplace, with the intention of causing harm or encouraging others to harass them.
- Online harassment: The victim experiences consistent and targeted harassment, including offensive comments, threats, or the spreading of rumours.

6. Identity Theft;

More than ever, our smartphones are used to store and access personal information thanks to the growth of social media, online shopping, and mobile banking. This is why it's so important that we recognize the risks and take the appropriate safety measures to keep ourselves safe.

There are several ways that identity theft via mobile devices might occur. Phishing scams are one popular technique. Cybercriminals can trick users into disclosing personal information like usernames, passwords, or credit card numbers by sending them phony emails or messages that seem authentic. It's crucial to exercise caution and confirm the legitimacy of any requests for personal information because these scams can be very convincing.

Via malware or malicious apps is another way. While some apps might contain malware that can steal sensitive data, others might be made to collect personal data from users without their knowledge. It's crucial to update the security software on your device regularly and to only download apps from reputable sources like official app stores.

Furthermore, your personal information may be at risk when using public Wi-Fi networks. Your data, including login credentials and financial information, could be intercepted by hackers when you're connected to an unprotected Wi-Fi network. It's best to stay away from using public Wi-Fi to access sensitive data or conduct financial transactions. Consider utilizing a VPN (Virtual Private Network) to encrypt your data and safeguard your privacy if you must use public Wi-Fi.

Mitigation Strategies

India needs to take a multifaceted approach to mitigate cybercrime pertaining to mobile devices, taking into account socioeconomic, regulatory, and technological factors. The following are some effective strategies to combat cybercrime on mobile devices:

1. Boost Cooperation between Government, Industry, and Civil Society: Fighting mobile cybercrime requires cooperation between government agencies, industry players, and civil society organizations. Public-private partnerships can help with coordinated responses to cyberthreats, information sharing, and cooperative cybersecurity awareness campaigns.
2. **Boost Mobile Device Security:** You can protect mobile devices from malware and other online threats by promoting frequent software updates, applying security patches on time, and utilizing reliable antivirus and anti-malware software. Furthermore, encouraging the use of secure messaging apps and encryption tools can help protect sensitive information sent over mobile devices.
3. **Utilize Emerging Technologies:** Mobile cybersecurity capabilities can be improved by utilizing emerging technologies like blockchain, artificial intelligence (AI), and machine learning (ML). Blockchain technology offers transaction verification and tamper-proof data storage, while AI and ML algorithms can be used for threat, anomaly, and predictive analytics.
4. **Boost penalties and regula to rymeasures:** Strict cyber security rules, data protection legislation, and fines for cybercrime enforcement can discourage bad actors and make them answerable for their deeds. To ensure justice and preserve cyber resilience, law enforcement agencies must be able to better investigate and prosecute cybercriminals.

India can effectively mitigate the risks posed by cybercrime related to mobile devices and create a safer digital ecosystem for all by implementing a comprehensive approach that combines regulatory measures, stakeholder collaboration, technological innovations, and awareness-building initiatives.

CONCLUSION

Security is frequently a matter of balancing risk and reward, defense versus convenience. In this line of thinking, the potential risks and benefits, and their tradeoffs, undoubtedly deserve further and deeper investigation. Security is always an arms race between attackers and deters. Since the mobile application market is growing, at the same time, mobile security will continue to deliver a plethora of issues to face. This paper aims to provide a comprehensive understanding of this phenomenon by analyzing the potential negative events, conditions, and circumstances that may lead to asset loss, as well as the countermeasures designed to mitigate these risks and offer users effective and sufficient protection.