Review Article

Mobile Phone Crimes: A Threat, Laws, and Prevention

DevaseelanS[a] , Bhat VJ[b], Vajagathali M[c]

Abstract

The Internet is one of the essentials for survival in today's modern society. Internet use has increased drastically worldwide. Mobile and the Internet enabling, speed up and efficiency of communications. All information is accessible via smartphones. A straightforward fingertip availability of information has enhanced the use and popularity of this information. While the technology is known to a more significant number of people, they are not aware of the risks and impacts.The Internet is one of the essentials for survival in today's modern society. Internet use has increased drastically worldwide. Mobile and the Internet enabling, speed up and efficiency of communications. All information is accessible via smartphones. A straightforward fingertip availability of information has enhanced the use and popularity of this information. While the technology is known to a more significant number of people, they are not aware of the risks and impacts. In this systematic review, we provide a detailed analysis of current state-of-the-art mobile forensic procedures and propose preventive possibilities that must be investigated in order to enable more efficient future solutions.

Keywords: Internet;smartphones; technology; mobile forensic

Introduction:

In certain circumstances, mobile devices are the primary way of communicating and participating in the digital world, allowing for ubiquitous access to information. However, after years of sustained and stable market growth, mobile device shipments have slowed down for the first time, indicating that worldwide device saturation has reached unprecedented levels.[1] Nevertheless, as per the industry analysts' prediction, smartphone usage and network traffic accounted for most of all Internet traffic by 2020. [2] The increasing capabilities of mobile and otherelectronic devices facilitated the creation, transfer, and storage of large amounts of personal and often sensitive information on the device itself. To obtain this data, cybercriminals constantly find ways to utilize or exploit these devices by engaging in unlawful activities.[3] This information and the associated metadata are a valuable source of digital forensic evidence in corporate, civil, criminal, and military investigations.[4] For example, a crime can be committed online via standard communication features or social networking apps, but device storage can contain vital incriminating evidence such as device location history.[5]Alternatively, a device owner might be a victim of cybercrime, including malicious software and other assaults; mobile devices are vulnerable to a wide range of threats covering various layers, including apps, communication routes, and local resources, but the device itself provides a great deal of information about the assault.[6]There are many different data collection methodologies and evidence

[a]Assistant Professor, Department of Forensic Science, Srinivas University, Mangalore-574146, India, [b]Professor& Head, Department of Forensic Medicine, Srinivas Institute of Medical Sciences and Research Centre, Mangalore, [c]School of Social Work, RoshniNilaya, Mangalore-575002, India

Correspondence:Devaseelan S
Email. devaseelan.s3@gmail.com

Received on 22.02.2021	Accepted on 28.05.2021

extraction process frameworks and recommendations available today. However, this heterogeneity adds to the forensic investigative process's complexity when combined with the continually changing technological world. We provide a detailed analysis of current state-of-the-art mobile forensic procedures and propose preventive possibilities that must be investigated to enable more efficient future solutions.

Types of mobile phone crimes

Mobile Hacking

In layman's terms, hacking is unauthorized access to a computer system and network.Cracking is a phrase that is similar to hacking. Hacking is defined as any action used to gain access to a mobile phone, communication device, computer, or network. To attack the target computer, mobile device, or communication device, hackers develop or employ ready-made computer programs.

Mobile Cyber Defamation

This kind of crime has become widely prevalent across the world today. Criminals use their mobile phones and other communication devices to send insulting, humiliating, and vulgar SMS or email to slander people and damage their reputation in the eyes of people who respect them.

Mobile Pornography

Abusers use the Internet extensively to reach and sexually abuse youngsters across the world. The Internet is quickly becoming a standard home item. As more houses gain internet connection, more children will use mobile phones, communications devices, and the Internet, increasing their risk of falling prey to pedophiles. Section 67B of the modified Indian Information Technology Act 2000 might bring mobile pornography into the scope of the law. The abovementioned act is a criminal punishable by imprisonment of any kind for up to five years and a fine of up to ten lakh rupees.

Identity Theft

Identity theft is carried out through mobile phones, and thieves employ numerous communication devices to perform crimes such as subscription fraud.

Cloning or Re-Chapping of Mobile

A clone is an analog mobile phone that has been configured to imitate a valid subscriber's phone by utilizing its ESN and phone number (these numbers are commonly obtained via intercepting using a scanner radio, stealing a dealer's or service provider's data, or straight from the impersonated phone). New varieties of cloned phones are making their way to the UK from the United States and Hong Kong: 'tumbling' phones look for identity from a pre-programmed list, while the latest 'magic' phones function as their scanners, duplicating identities from adjacent phones in use.

Mobile Cyber Stalking

Cyber-stalking is described as a cyber-repeated criminal's acts of harassment or threatening behavior directed at a victim using mobile internet services. Stalking is described as the systematic acts of harassment directed at a target, such as following them, making harassing phone calls, murdering the victim's pet, vandalizing the victim's property, and leaving written messages or items. Stalking can lead to significant violent activities against the target, like bodily injury, and must be recognized and considered as such. Everything is contingent on the stalker's actions.

Denial of Service Attack

This is an act by the criminal, who floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

Mobile Software Piracy

Theft of mobile software by unauthorized copying of authentic apps or counterfeiting and marketing items that imitate the original.

Mobile Phishing

This refers to the practice of sending phishing emails that usually come from mobile service providers to mobile phone subscribers.

Bluejacking and Bluesnarfing

Bluejacking means that messages are

transmitted from a Bluetooth to some other Bluetooth connection. Manufacturers of products or companies generally use this technique to market their brand by transferring texts, emails, or pictures.

In Blue Snarfing, the hacker attempts via Bluetooth to steal information and data.

Both operations are benign; even so, you cannot join your mobile device's confidentiality and look at the data.

Blue Bugging

In these crimes, the Hacker controls the victim's telephone entirely and can do everything, like access to the phone directory, contact list, sending text messages, and trying to call. It means that the victim's phone will be fully controlled.

Mobile Forensics

As a result of significant diversity among electronic devices, digital forensics has evolved into several distinct areas or subdisciplines comprising computer forensics, network forensics, malware forensics, database forensics, and mobile forensics. The NIST defines mobile forensics as "the study of recovering forensic evidence from a mobile device utilizing established procedure under forensically sound conditions".[7] Mobile forensics is inherently multidisciplinary and challenging because of the increasing heterogeneity of mobile device technologies and the features these devices support, which are usually far beyond basic voice calls and text messaging. At the same time, the various features supported enable the extraction of large amounts of valuable evidence not only from the device itself but also from other linked sources. Although a significant amount of evidence can be found on a device, the user workstations with which the device connects for synchronization and backup purposes and the telecommunications carrier can be considered additional evidence sources, especially for retrospective examination and analysis. In addition to legacy phones with essential features and smartphones, the field of mobile forensics also includes data acquired from a wide range of digital electronic devices, including personal digital assistants (PDAs), tablet devices, satellite phones, and navigation devices.[8] The literature describing the early stages (pre-2007) is generally scarce and focuses on building up the recognition of cell phones as valuable potential sources of digital evidence. The majority of techniques presented focused on devices that utilize the Global System for Mobile Communications (GSM) standard and data acquisition through subscriber identity modules, commonly known as SIM cards.[9]The 2007 to 2010 period was characterized by strict conformance to the original guidelines developed by NIST and the Association of Chief Police Officers (ACPO) in 2007. These guidelines prescribed the need to acquire a device data image that fully corresponds to the original device state before the acquisition.[10]

Mobile crime laws

Section 66A

This section states that "whoever sends the offensive message through communication services will get imprisonment of three years."

Section 67

In this section, it is given that "whoever publishes or transmits obscene material in electronic form will get rigorous imprisonment for five years and a fine of ten lakh rupees." This section was used in a landmark judgment in the case of State of Tamil Nandu Vs. SuhasKatti.

Section 67A

This section deals with publishing or transmitting material containing sexually explicit acts in electronic form.

Prevention

Keep software and operating system updated

Maintaining system and applications up-to-date ensure to acquire the latest security corrections to secure computer.

Use antivirus software and keep it updated

Antivirus software is an intelligent strategy for keeping PC safe from attacks and a

comprehensive Internet security solution such as Kaspersky Total Security.

Antivirus software scans detect and eliminate threats before they become a problem. This protection keeps computers and data safe from cybercriminals, giving peace of mind.

If you use antivirus software, keep it updated to get the best level of protection.

Use strong passwords

Use strong passwords that no one can guess, and write them down anywhere. To make things easier, use a reliable password manager to generate secure passwords at random.

Never open attachments in spam emails

Spam emails with attachments are frequent for computers to be infected with malware and other forms of crimes. Never open an attachment from a sender you do not recognize.

Do not click on links in spam emails or untrusted websites

Clicking on a link in spam letters and other communications or on unknown websites is yet another method to become victims of cybercrime. Avoid doing so in order to be secure online.

Do not give out personal information unless secure

Do not offer personal information over the phone or email if sure of a secure line or email.

Conclusion

In this review, we take advantage of crime's temporal and spatial properties to establish the empirical connection between mobile communication and our society's number of crimes. It is clear that technology improvements and the digitization of things have made life easier, but technological improvements have also increased the number of crimes, which must be prevented through strict legislation. People should be aware of these crimes and be attentive to them. The general public should not use unsecured Internet sites to prevent such fake calls. One should install strong antivirus and prevent one's phone and laptops from unwanted data which can harm them. People should keep themselves updated and aware of different and new ways of cybercrime. An individual should install strong antiviruses and avoid unwanted data on their phone and laptops. People should keep up to date and be aware of new and different ways of cybercrime.

References

1) Gartner Says Worldwide Smartphone Sales to Slow in 2016," Gartner Group, 7 June 2016; www.gartner.com /newsroom/id/3339019.
2) "The Zettabyte Era—Trends and Analysis," Cisco, 7 June 2017; www.cisco.com/c/en/us/solutions/collateral /service-provider/visual-networking-index-vni/vni -hyperconnectivity-wp.html.
3) Q. Do, B. Martini, and K.K.R. Choo, "A Cloud-Focused Mobile Forensics Methodology," IEEE Cloud Computing, vol. 2, no. 4, 2015, pp. 60–65.
4) W.B. Glisson, T. Storer, and J. Buchanan-Wollaston, "An Empirical Comparison of Data Recovered from Mobile Forensic Toolkits," Digital Investigation, vol. 10, no. 1, 2013, pp. 44–55.
5) T.B. Tajuddin and A.A. Manaf, "Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone," Proc. World Congress on Internet Security (WorldCat), 2015, pp. 132–138.
6) Y. Wang, K. Streff, and S. Raman, "Smartphone Security Challenges," Computer, vol. 45, no. 12, 2012, pp. 52–58.
7) R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101, 2014.
8) K. Barmpatsalou et al., "A Critical Review of 7 Years of Mobile Device Forensics," Digital Investigation, vol. 10, no. 4, 2013, pp. 323–349.
9) Azfar, K.K.R. Choo, and L. Liu, "An Android Communication App Forensic Taxonomy," J. Forensic Sciences, vol. 61, no. 5, 2016, pp. 1337–1350.
10) Baggili et al., "Watch What You Wear: Preliminary Forensic Analysis of Smart Watches," Proc. 10th Int'l Conf. Availability, Reliability and Security (ARES 15), 2015, pp. 303–311.