MOBILE CELL PHONES AND CYBER CRIMES IN INDIA: HOW SAFE ARE WE?

Mr. Nikhil A. Gupta*

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 May 2012 there were 929.37 million mobile users in India. 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 Even our morning alarm clocks are been replaced by the mobile cell phones.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. Mobile cell phones have now become new personal laptops and desktops which are having capacity to store as much data as our laptops and desktops are and in additional they are providing flexibility and portability. Internet enabled smart phones, tablets etc...are performing the functions of our computer, but one vital feature is missing and that is security. Rapid growth in the use of internet enabled mobile cell phones allows us to use manage our banking transaction, official and institutional transactions, rapid communication through email or social networks, and many more. Virtually we can perform the task of a computer on our mobile; this means alike our computer our mobile phone is also vulnerable to the risk of fraud, theft of financial information and identity theft etc.

Cell Phones: An Open Door for Cyber Criminals

Recent reports have suggested that with the advancement of the telecommunication technology there is increase in cyber crime in the

* Civil Judge Junior Division & Judicial Magistrate First class, Newasa, District Ahmednagar.

nation. 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 cyber crime ignites, a particular class of the people escapes the discussion saying that; they neither use computers nor they use internet for communication and therefore cyber crime is not a threat for them. People try to hide their ignorance about cyber crimes on the ground that cannot become its victim, but they have absolutely no idea that knowingly or unknowingly they can be adversely affected by cyber crime. 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 cyber crime 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." 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 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." This broad definition encompasses every gadget we are using in our day to day life to make our life simpler as a computer. Mobile cell phones are just one of it.

Common Cyber Crimes Associated with Cell Phones

1. **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

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. In Bluesnarfing the hacker can commit theft of all the data and information in your mobile phone using his laptop.

2. **Vishing:** This is a tool for committing financial crime by using mobile. 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.

3. **Malware:** This 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 service 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.

Mobile Cell Phones and the Information Technology Act, 2000

As per definition of term "computers", as provided by Section 2(i) of the IT Act, mobile phones are encompassed in the definition of a computer. Mobile phones are been used for exchange of information. As per Section 2(r) of the IT Act, "electronic form", with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.... . Thus any information shared on the mobile phone though it may be talks, text or entry of information they are encompassed in the purview of the IT Act.

Section 66A of The IT Act, provides for punishment for sending offensive messages through communication service etc. This provision of law is parallel provision to Sections 294, 504, 506, 507 and 509 of Indian Penal Code, 1860 only difference is that in this provisions of law the criminal uses his cell phone or computer to express the offensive feeling. The punishment prescribed under this section is imprisonment for a term which may extend to three years and with fine. This section is embedded with an explanation which states that for the purpose of this section, terms electronic mail and electronic mail message means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message. This explanation widens the scope of this section and assures that the criminal cannot escape his liability.

Newly added provision in the IT Act in the form of Section 67(A) provides for punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form. This is most important for teenagers. The trends of sharing pornography material on cell phones are on increase. The incident of indecent MMS is not unknown to anyone. This provision of law books those who publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct. This provision of law is analogous to provisions of Sections 292 and 292A of the Indian Penal Code, 1860. It provides for a punishment on first conviction for imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees. In the even to second or subsequent conviction for imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

This provision of law elaborates Section 67 which provides for punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Conclusion

A mobile phone is just like a match stick. A match stick can ignite a lamp and can also ablaze a house. Choice is of the person having it. Alike is with mobile technology you can use it to make you life simpler, or for satisfying you selfish gain by misusing it. As we are careful while using match stick in home, and keep it in safe place out of the reach of children. A mobile phone also should be used with caution. Your ignorance can bring you in trouble. People must be vigilant and educated towards the game of dirty business played on mobile phones. A certain class of people is exploiting the technology. All the glitters is never gold must be remembered by mobile users. People must be sensitive towards suspicious or malicious information received on their mobile phones. They shall forthwith report against it. This will ensure not only their security but security of others too. Care also should be taken when we are shopping online; know as much as you can about the site, its policies and procedures. Never share our personal information with stranger on mobile phones. Also no secret information like passwords, PIN, credit card details etc., must be stored on the mobile phone. Precaution is the only means to stay secured in this e-world. In this e-world one must never forget the words of Fransis Bacon that knowledge is power, because in the world of computers, more you know about computers, the more you will know that you don't know! Thus with following tips for securing your cell phone I end up this article.

Tips for Securing Cell Phones

- Turn on Bluetooth or enable internet only when required.
- Do turn off the wireless connections when not needed.
- Regularly update the cell phone software.
- Install latest anti-virus software, and keep it updated.

- Use strong passwords to lock your cell phone.
- Never share personal information with stranger.
- Never store personal banking details in cell phones.
- Be suspicious while entertaining strangers on social networking website.
- Consider disabling the geo-tagging feature on your phone.
- If you are connected to a public WiFi, don't access sites where you need to enter your password, credit card information etc.
- While banking and shopping online, ensure the sites are *https* or *shttp*.
- Always keep in mind that you cell phone is a device that contains a lot of your personal information. Keep it safe and secure.