International Journal of Research and Review
www.gkpublication.in ISSN: 2349-9788

Review Article

Cyber Crime through Mobile Phone in India and Preventive Methods

Avneet Kaur Bajaj[1], Chander Jyoti[2]

[1]Department of Biotechnology, [2]Department of Bioinformatics,
GGDSD College, Sector 32 B, Chandigarh, India.

Corresponding author: Avneet Kaur Bajaj

Received: 25/02/2015 *Revised: 11/03/2015* *Accepted: 16/03/2015*

ABSTRACT

Technology has made human life easier. Though there are many benefits of the technology but we are also facing a serious threat of cyber crime. One of the examples of technology is mobile phone. Cell phone advancement in terms of various applications like networking mobile, computing wireless network is one of the major achievements of the technology. India is second largest user of mobile phone after China and according to telephone regulatory of India on 31st March 2014, there are around 933 billion mobile users in India but 50 percent of mobile users in India do not use mobile security solution resulting in increase mobile cyber threat. Various types of the cyber crime through mobile and their preventive methods have been discussed in this article.

Keywords: Cyber crime, Prevention of cyber crime, Vishing, Smishing.

INTRODUCTION

Cyber crime is a criminal activity through computer and internet. The first recorded cyber crime took place in the year 1820. Communication technology has touched each and every aspect of human life. [1] Different types of mobile are introduced in market with better and advanced technology. But due to the misuse of same technology, cyber crime is increasing heuristically which is affecting our society at large extent. Mobile phones provide users mobile access to email, the internet, GPS navigation, and many other applications. However, Mobile phone security is not at pace with computer security. There are various cyber threats due to mobile like blue bugging, SIM card cloning, cyber stalking, vishing, smishing and trojan attack.

Bluebugging: Bluebugging is attack on the mobile cell phone through Bluetooth. Every mobile phone has embedded Bluetooth which allows the hacker to take over complete access of user mobile feature like listing the call, forwarding the call, sending the text message. The victim is ignorant of the attack even if the bluetooth device is disabled or turned off. [2]

Vishing: Vishing originate from two words voice and phishing. User banking account information is gained by criminal through voice email and voice over internet protocol. Vishing attack is common nowadays due to increased mobile banking and online transactions by mobile user. Main motive of

the hacker is to get money by access of user bank account. [3]

Smishing: Smishing is type of phishing which uses short messaging services or text messages on the mobile phones. SMS service is the one of the most used service on mobile phone and an easy tool for hacker to full fill their greed. Smishing is a security attack in which the user is sent a very lucrative SMS that compels the user to expose their personal information like internet banking passwords, credit card detail etc. Recently these SMS also include false online dating subscriptions and job offers. [4]

Cyber stalking: Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. It involves following the victim online, making harassing call, leaving written messages and tracking the various activity. There are ways of cyber stalking like E-mail stalking, Internet Stalking and Computer Stalking. [5]

SMS spoofing: One of the major problem with SMS based banking are SMS Spoofing which is an attack where malicious user sends out SMS message which appears to be sent by original sender. End-to-end encryption of the SMS message is not available. SMS spoofing is when the identity of the sender is taken over by a hacker. SMS messages are sent for free by the hacker whilst the victim is charged for sending this fraudulent traffic. [6]

Trojan horse: "Trojan horse" name originate in the past from Greek mythology indicating a large horse built for gaining entrance into Troy city during Trojan War. But now-a-days it is synonym for non-replicating malicious programs that perform actions of deleting, blocking, modifying and copying data that have not been authorised by the user. It can be used to steal other's information by network attacker. [7]

On the basis of action performed it is being classified as:

Backdoor: Gained access to infected computer, can delete, display and able to launch any unwanted program

Trojan-Banker: It has the ability to disable online banking security and steals password, username and account information.

Trojan-Spy: Like a spy, it tracks all the activities being performed on infected computer taking screen shots and sending it to the hackers.

Trojan-SMS: This Trojan can send premium SMS from an android mobile phone user and leave account balance to zero.

MOBILE CYBER CRIME CASE REPORTS

1. State of Tamil Nadu Vs Suhas Katti. This case is related to posting of obscene, defamatory and annoying message to divorcee woman in the yahoo message group by the accused through a false email account. The accused start pressurizing her to marry her and on her reluctance to marry him, the accused took up the harassment through the Internet. Eventually marriage ended in divorce and conviction of the accused. The court relied upon the expert witnesses and other evidences (cyber café owner statement) produced before it. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India. [8]

2. Cyber Stalking Case: Ritu Kohali case was the first case in India dealing with cyber stalking. Victim was stalked by Munish Kutharia. As a result she received around forty obscene telephone calls at odd hours for consecutive three days. She lodged a complained to Delhi Police and police traced IP address and Kutharia was arrested. Delhi police registered the case under section of 509 of Indian Penal Code. [9]

3. SMS Spoofing Case: There are several cases of people losing money through SMS spoofing. One such case is of 52 year old graduate women of Mylapur that she has won a cash prize in Indian currency. She had to deposit token money to get the prize. She didn't get any amount but lost Rs. 57 lakh. [10] Another case is of 400 million SMS scan in Mumbai in which two bother in Mumbai took the help of SMS technology and messages on random number and asked the people to earn ten thousand per month. It was advertised that each interested people need to deposit five hundred. [11]

Law Against Mobile Cyber Threat In India

Today use of internet through mobile is very common but criminal activities through mobile are also increasing day by day. To stop such type of activity strict law should be implemented. Cyber law is constantly being evolved as new challenges are surfacing every day. [12] Earlier cyber stalking is not covered under section of 509. Ritu Kohli case was an alarm to Government to make the law against cyber mobile threat. Cyber law has introduced to various sectors to deal with mobile threaten.

1. Section 66A deals with sending offensive messages through communication services. Imprisonment of three year jail is given as punishment under this attack.
2. Section 67 deals with publishing or transmitting obscene material in electronic form. Corrupt person is punished for five year jail and fine of ten lakh rupee is imposed.

This section has historical importance as landmark judgment was given in famous case of "State of Tamil Nadu vs Sushas Katti" on 5 November 2004 under this act.

3. Section 67A deals with publishing or transmitting material containing sexually explicit act in electronic form. [13]

Preventive Measurements: No matter cyber threat is increasing; the remedy lies in our hand. Small steps in this regard will help to protect cyber crime which is as follows.

Awareness: People should be aware regarding different threat of cyber mobile threat through TV, internet, magazine etc. [14]

Strong Antivirus Software: Mobile devices should always be updated with strong antivirus which prevent from viruses, malware, Trojan horses and unwanted software. [15]

Be Careful while using social site: Posting photograph to various social networking site people should be careful as one can save those picture and can post those picture for wrong deeds.

Strong Password: One should choose strong password using special character, upper and lower case.

Hiding Personal Information: People usually received many mail and messages to give their account number so that sender can send money of cash prize to their account. Never respond to such type of messages and mail. Avoid frequent use of online shopping and banking.

REFERENCES

1. Hemraj Saini, Yerra Shankar Rao, T.C.Panda, "Cyber-Crimes and their Impacts: A Review", vol. 2, March-April 2012, pp.202-209.
2. Nikhil A. Gupta, "Mobile Cell Phones and Cyber Crimes in India How Safe are we?" vol. 4, February 2014, pp. 427-429.
3. Ezer Osei Yeboah-Boateng, Priscilla Mateko Amanor, "Phishing, Smishing & Vishing: An Assessment of Threats against Mobile Devices", vol. 5, April 2014, pp.297-307.
4. Nilay Mistry, H. P. Sanghvi, Dr. M. S. Dahiya. Dr. J. M. Vyas, "Preventive Actions to Emerging Threat in Smart

Devices Security", vol. 1, May 2013, pp. 20-26.
5. Anju Thapa and Dr. Raj Kumar, "Cyber Stalking: Crime and Challenge at the Cyberspace", vol. 2, 2011, pp. 2229-6166.
6. Manoj V, Bramhe, "SMS Based Secure Mobile Banking", vol. 3, 2011, pp. 472-479.
7. Daniel Petri "An Introduction to Trojan Horse VIRUS", unpublished.
8. Dr. A. Prasanna, "Cyber Crime: Law and Practice,"unpublished.
9. Ashwani Tanwar, "Legal Perspective of Cyber Crimes in India," vol. 3, Feb 2012, pp. 35-36.
10. K.N. Basha, "Seminar and Workshop on Detection of Cyber Crime and Investigation,"unpublished.
11. "Audit of Fraud, Fraud Detcetion Technique& Forensic Audit, Case Study on Cyber Crimes. Indian Audit & Accounts Departments", *unpublished.*
12. Taraq Hussain Sheakh, "Cyber Law: Provisions and Anticipation", vol 53, Sep, 2012, pp. 10-12.
13. www.cyberlawsindia.net
14. Vinay Kumar D., "Cyber Crime Prevention and Role of Libraries", vol 3, pp 222-224.
15. Vineet Kandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention in India," vol 2, 2013, pp. 150-156.

How to cite this article: Bajaj AK, Jyoti C. Cyber crime through mobile phone in India and preventive methods. Int J Res Rev. 2015; 2(3):110-113.

****