ORIGINAL RESEARCH PAPER | Information Technology | Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

Awareness and strategy to prevent Cybercrimes: An Indian perspective

KEYWORDS: Cybercrimes , Awareness

MS. ANISHA

RESEARCH SCHOLAR ITTR, BPSMV KHANPUR KALAN

ABSTRACT The use of internet in India is increasing quickly.It has given rise to new opportunity in every field like –entertainment, industry, sports, education etc. It is universally true that every coin has 2 sides, same for the internet, it uses has both advantage and disadvantage, and one of the most disadvantage is Cyber-crime . Every crime has its impact specifically on society, nation and the world to the great extent. By the surveillance of cybercrime and its phenomenon it is exposed that similar to former crimes it has badly affected social life of humans. To understand the influence of cybercrime, it is necessary to look into the impact of two things computer technology and internet on people as cybercrime is no doubt originating out of these. There are inherent challenges to the field of IT security and services through individuals and critical infrastructure. Socially, people are now more open to communicate and interrelate with others compared to past which widen the objectives from the personal relations to the professional ones. Today, there is no single reason for the people to interact through internet but thousands.. Technological innovation is an evolutionary process. This paper focus on critical infrastructure scenario in India, facts around usage of internet and exploration of cybercrimes under diverse heads across India.

INTRODUCTION

cyber-crime is any illegal activity which is committed using a computer network (especially the internet). Also, cyber-crime involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software. In India most of cyber-crime cases are committed by educated person (some cyber – crime requires skills). So, it is required the deep knowledge about the cyber –crime and it prevention. Also, in India most of the cases found where, crimes are committed due to lack of knowledge or by mistake.. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet.

The common types of cyber crimes may be discussed under the following:-

1. Hacking - A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an attack in to the privacy of data.

2. Cyber Stalking - This crime involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.

3. Spamming - Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates .negative impact on consumer attitudes towards Internet Service Provider.

4. Cyber Pornography - Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such funs. Later they are sexually exploited for gains.

5. Phishing - It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

6. Software Piracy - It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies.

7. Corporate Espionage - It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.

8. Money Laundering - It means moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. eg. Transport cash to a country having less stringent banking regulations and move it back by way of loans the interest of which can rededucted from his taxes. This is possible prior to computer and internet technology, electronic transfers have made it easier and more successful.

9. Password Sniffers - Password sniffers are programmes that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.

10. Spoofing - It is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted. Spoofing was used to access valuable information stored in a computer belonging to security expert *Tsutomu Shimomura.*

11. Credit Card Fraud - In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases.

12. Web Jacking - The term refers to forceful taking of control of a web site by cracking the password.

13. Cyber terrorism - The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country.

14. E mail bombing: this is a serious crime in which a person sends a numbers of emails to the inbox of the target system/person. Mail

Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

bombs will usually fill the allotted space on an e-mail server for the users e-mail and can result in crashing the e-mail server.

15. Spreading computer virus: It is a set of instruction which is able to perform some malicious operations. Viruses stop the normal function of the system programs and also to the whole computer system. They can also ruin/mess up your system and render it unusable without reinstallation of the operating system A computer viruses can be spread through—Emails, Cds, Pendrives (secondary storage),Multimedia, Internet.

16. Internet fraud: Internet fraud can occur in chat rooms, email, message boards or on websites. In internet fraud criminal can send fake info to the victim in cases like online purchasing, real estate, pay BAL, Work-at-home donation processing etc.

17. Cyber warfare: It is Internet- based conflict involving politically motivated attacks on information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities.

18. SMS Spoofing: SMS Spoofing allows changing the name or number text messages appear to come from.

19. Voice Phishing: The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

Cyber crime can be recognized in two ways :

I. The Computer as a Target:-using a computer to attack other computers. Ex:. Hacking, Virus/Worm attacks, DOS attack etc.
II. The computer as a weapon:-using a computer to commit real world crimes. Ex:. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cybercrime Prevention Strategies:

a) There is only a partial awareness among the general users about the cyber crimes and government agency should take care of creating more awareness on this type of crimes to general public which as dangerous or even more dangerous than gold chain snatching.

b) The cyber café/center owners have done appreciable work by adopting the system of asking for address proofs and identity of the cyber users. This system has been adopted after the enforcement agency made it compulsory from the year 2010 to have the login time and logout time of every user with their identity to identify incase of cyber crime takes place. But the enforcement agency should have a follow-up action to see whether their records are maintained properly or not by each internet centers in city for preventing the city users from cyber crimes.

c) The children may become addict to games and visiting unscrupulous and objectionable sites not suited to their age. Parents, teachers, responsible citizens, cyber café owners and enforcement officers should take some action in this regard to protect the psychological health of future generation of India.

d) The social networking is being visited by youth and also by adolescent children and they are used to share all sort of information and mostly about films and film personalities. This is grossly wasting the time and energy of our youth for this type of most uncreative browsing. This all is the area of attention and concern for all in the society.

e) The internet users should be taught to protect their password and importance of protecting the password. This should be done by the internet café/ center's (owners) supervisors and teachers of school and colleges.

f) Susceptible for this type of crimes when give away their personal details like name, address, email and email address and other passwords to the sites while making purchases or e-money transfers on internet without taking proper precaution.

g) The survey reveal a need of educating all users about the types of cyber crimes and their consequences and importance of protecting one's password/ bank pin number and email address while using internet.

h) Install or update your antivirus software—Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without the users' knowledge. Most types of antivirus software can be set up to update automatically.

i) Turn off your computer—With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

j) Prevention of cyber crimes and training requirement of enforcement authorities -

through years of research which would be of help for government and all other stake holders in the process and especially to the benefit of the society in creating fearless environment where they will have happy surfing, e-banking, e-shopping and e-mailing internet experiences for their lifetime.

CONCLUSION

Roots of cybercrime are lies in technology and critical infrastructure. Number of internet users is continuously increasing and with this growth risk of several types of crimes is also amplified. Cybercrimes are varying in its nature due to enhancement in technologies. Technology-based crimes have been developing with the passage of every day and they need to be solved with utmost priority. These crimes never restricted to computers but other electronic devices are made like financial transaction machines, tele-communication equipments etc. Due to diversified nature it is difficult to identify the cyber security problems which leads to unawareness on security issues. we can arrange workshops, free advertisements, public interest with the help of government & NGO'S . The process of acknowledgment about cyber world crimes and cyber illiteracy should be start from grassroots level; institutes, computer centers, schools & individuals. Yet India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time.

REFERENCES

1. A comparative analysis of cybersecurity initiatives worldwide, international telecommunication union, Geneva, 28 June -1 July 2005.
2. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.
3. Cybercrime classification,[Online],Available: http:// shodhganga. inflibnet.ac.in/ bitstream /10603/7829/12/12_chapter%203.pdf [29 September 2013]
4. Cybercrime system requirements in India: Most necessary thing inIndia, [Online],Available: http://www.cyberlawsindia.net/ requires. html [13 May 2012].
5. Cybercrime, [Online], Available: http://www.britannica.com [5 March 2012].
6. e-Infrastructure, [Online], Available: http://deity.gov.in [24 August 2013]
7. Federal Bureau of Investigation's 2010 statistics, [Online], Available: www.fbi.gov [16 July 2013].
8. Godbole, N., Belapure, S. (2011) Cyber Security, 'Understanding Cybercrimes', Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd., (1st ed.), ISBN: 978-81-265-2179-1
9. Incidence of Cases Registered under Cyber Crimes in States/UTs, [Online], Available: http://www.ncrb.org [10 June 2013]
10. Industry & Sectors, [Online], Available: http://indiainbusiness.nic.in [16 June 2013]
11. IT Infrastructure in India, [Online], Available: http://business.mapsofindia.com/ indiabudget/infrastructure/it.html [16 June 2013]
12. Lum Wai Seng, Dave Junia, Berenice Wong, Yeo Kai Zhen, Mabel, Tan Chien Ying, Jolin,

Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

Woo Nicholas. (2012) 'Responsibility of National Security and the Indian Government: A Case Study on Cyber Terrorism in India', National University of Singapore.
13. Muthukumaran, B. (2008) 'Cybercrime scenario in India', criminal investigation department review, Chief Consultant, Gemini Communication Ltd., p. 17.
14. Nagpal, R. (2008) Evolutions of Cybercrimes, Asian School of Cyber laws.
15. Pillai, (2008). 'Govt. framing norms for social infrastructure in SEZs', The Economic Times, [Online], Available: http://articles.economictimes.indiatimes.com/2008-06-20/news/28488069
16. Sanjay K Singh, 'Information Technology in India: Present Status and Future Prospects for Economic Development'
17. Srivastava, B., Abhichandani, T., Biswas, A., Thakare, M. 2011, Report on Internet in India (I-Cube), Internet & Mobile Association of India (IAMAI), p. 3.
18. State wise Internet Users in India Census 2011, [Online], Available: http://updateox.com [25 April 2012].