International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 01, January - March, 2021, pp 271-273

CYBER CRIME IN INDIA: CURRENT TRENDS

Dr. Nishant Chaudhary*

ABSTRACT

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity[2]. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, spam and so on.

Keywords: *Cyber Crime, Computers or Networks, Phishing, Cyber Terrorism.*

Introduction

The advancement of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet[1]. Internet is used in almost every sphere. With the development of the internet and its related benefits also developed the concept of cyber crimes. Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

Why Cyber Crimes are Rising Exponentially in India

Where the risk is low and rate of return investment is high, people always take the advantage of this type of situation and due to this cyber crime takes shape. Moreover, the invisible nature of crime makes it difficult to find criminal, due to this cyber crime is increasing day by day[3]. In India, there are several factors which are responsible for increasing the rate of cyber crime such as widespread poverty, huge unemployment, eagerness to make quick money among youth, lack of awareness among people, loopholes in laws, lack of trained officials in investigating agencies, etc.

Different Kinds of Cyber Crimes

The different kinds of cyber crimes are:

- **Unauthorized Access and Hacking:** Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network[4]. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer.
- **Web Hijacking:** Web hijacking means taking forceful control of another person's website[5]. In this case the owner of the website loses control over his website and its content.
- **Cyber Stalking**: Cyber Stalking means repeated acts of harassment or threatening behaviour of the cyber criminal towards the victim by using internet services[6]. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.
- **Denial of Service Attack**: This is an attack in which the criminal 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. This kind of attack is designed to bring the network to crash by flooding it with useless traffic.

* Welfare Officer, Government of NCT of Delhi, Delhi, India.

- **Virus Attacks**: Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program[7]. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available. Trojan Horse is a program that acts like something useful but do the things that are quiet damping[8]. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.
- **Software Piracy**: Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original[9]. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.
- **Phishing**: Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft[10]. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.
- **Email Spoofing**: Email spoofing refers to email that appears to originate from one source but actually has been sent from another source[3]. Email spoofing can also cause monetary damage.
- **Cyber Defamation:** When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation[4].
- **Forgery**: Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc[7]. These are made using computers, and high quality scanners and printers.
- **E-commerce/ Investment Frauds**: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities[6]. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.
- **Cyber Terrorism**: Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc[12].

The list of offenses given above is not exhaustive and would also include any other types of offenses that would be committed through a computer or against a computer in the future.

Cyber Laws

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T[11]. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

Cyber Crimes Related Provisions under the IT Act

- Sec.65- Tampering with computer source documents
- Sec.66- Hacking with computer systems, etc.
- Sec.67- Publishing obscene information
- Sec.70- Unauthorised access to protected systems

- Sec.72- Breach of confidentiality and privacy
- Sec.73- Publishing false digital signature certificates

Cyber Crimes under Indian Penal Code (IPC) :

- Sec. 503 IPC- Sending threatening messages b email
- Sec 499 IPC- Sending defamatory messages by email
- Sec 463 IPC- Forgery of electronic goods
- Sec.420 IPC- Bogus websites, cyber frauds, etc.
- Sec.383 IPC- Web-jacking
- Sec.500 IPC- E-mail abuse

How to Prevent Cyber Crimes

With the ever increasing menace of cyber crime in our society, it is imperative to take curbing measures for minimising its impact and reducing the number of victims. Following measures could be taken:

- Social awareness regarding the pros and cons of using internet services should be generated among masses. It would help them to make informed decisions and take precautionary measures.
- Strict implementation of laws and regularly updating the laws would do great advantage in reducing cyber crimes incidence in India.
- Capacity building of investigating agencies by making them familiar with latest technology would not only help in resolving cyber crimes but also act as a deterrent effect on criminals.
- Providing employment, reducing poverty, increasing literacy, etc would help in keeping youth away from engaging in illegal activities.

In a country like India, where a large chunk of population is digitally illiterate, people are prone to fall victim of cyber crime. Therefore, it is of utmost importance to generate awareness among masses and also provide them basic training to deal with cyber crimes. Also, there is a need to update Information Technology Act,2000 as per the new developments and changes in the area of cyber crime to provide stringent punishment to the persons involved in such crimes. All stakeholders like government, people, media, etc should work in tandem to address the challenges of cyber crimes in India and make our country a safe and secure place to live.

References

1. Sankar Sen, 'Human Rights & Law Enforcement', 1st ed., 2002, Concept Publishing Co., New Delhi.
2. Dr. Sub hash Chandra Gupta, 'Information technology Act, 2000 and its Drawbacks', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
3. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi. 1992 U.S. App. LEXIS 9562 (4th May 4, 1992)
4. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
5. R. V. Sean Cropp, Snearesbrook Crown Court, 4th July 1991. (303) B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.
6. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi. Rupam Banerjee, 'The Dark world of Cyber Crime', July 7, 2006 can be viewed at http://articles.sakshay.in/index.php?article=15257
7. Prof. Unni, 'Legal Regulations on Internet Banking', 2007, NALSAR University of Law, Hyderabad.
8. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
9. B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.
10. Prof. V.K Unni, 'Legal strategies for a Robust I.T Infrastructure', 2007, NALSAR University of Law Hyderabad.
11. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi. Sanker Sen, 'Human Rights & Law Enforcement', 1st ed., 2002, Concept Publications, New Delhi.
12. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.