WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Overview of Cyber Crimes and Cyber Law's in India

Gaurav Jain

Assistant Professor Dept. of CSE , AKTU University U.P.

ABSTRACT :

Internet, the worldwide connection of loosely held networks, has made the flow of data and information between different networks easier. With data and information being transferred between networks at distant locations, security issues have become a major concern from the past few years. The internet has also been used by few people for criminal activities like unauthorized access to others networks, scams, etc. These criminal activities related to the internet are termed as Cyber Crimes. With the increasing popularity of online activities like online banking, online shopping, etc., it is a term that we often hear in the news now-a-days. Therefore, in order to stop and punish the cyber criminals, "Cyber Law" was introduced. Cyber Law can be defined as law of the web, i.e., it is a part of the legal systems that deals with the Internet, Cyberspace and with other legal issues like online security or online privacy.

Therefore, keeping the objectives in mind, this chapter is divided into different sections in order to provide a brief overview of what is cyber crime, the perpetrators of cyber crime-hackers and crackers, different types of cyber crimes and the evolution of cyber laws in India. The chapter further throws light on how these laws work and the various preventive measures which can be used to combat this "hi-tech" crime in India.

Key Words : Internet, Cyber Crime, Cyber Law, Cyberspace, Online security, Online privacy, Hi-Tech Crime, Hackers, Crackers, Unauthorized access.

Introduction

A computer can be defined as the machine that stores and processes information that are instructed by the user. Cyberspace, i.e., the Internet, has made the flow of data and information between different networks easier and more effective. The internet technology is used for various purposes ranging from online dealing to online transactions. Since decades majority computer users are utilizing the computer, either for their personal benefits or for other benefits. Therefore, security related issues have become a major concern for the administrators. This has given birth to "Cyber Crimes". Cyber Crime can thus, be defined as the crimes committed by using computer or computer network and usually take place over the cyberspace especially, the Internet. In simple terms, cybercrimes are the offences that take place over electronic communications or information systems. A Cybercriminal may use a device to have access to users' personal information, confidential business information, and government information or to disable a device. Selling any private data or information without the consent of the owner also falls under cybercrime. Criminals performing such activities are often referred to as hackers. Therefore, cybercrimes are also known as electronic crimes or e-crimes, computer-related crimes, high-tech crime, digital crime and the new age crime.

Today, Cybercrime has caused a lot of damages to individuals, organizations and even the Government. Several laws and methods have been introduced in order to stop crimes related to the Internet. "Cyber Law" was introduced in India with an objective to cover the part of the legal systems that deals with the Cyberspace and legal issues, online security or online privacy, etc. In other words, Cyber Law can be defined as the laws that govern the Cyberspace cybercrimes, digital and electronic signatures, data protections and privacy, etc., and comprehended by the cyber law. The UN's General Assembly recommended the first Information Technology (IT) Act of India in 2000. This Act was passed on the "United Nations Model Law on Electronic Commerce (UNCITRAL) Model".

Classification of Cyber Crimes

Cyber crimes can be classified in to 4 major categories as the following:

(1) Cyber crime against Individual

(2) Cyber crime Against Property

(3) Cyber crime Against Organization

(4) Cyber crime Against Society

(1) Against Individuals

(i) Email spoofing : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

(ii) Spamming : Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

(iii) Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

(iv) Harassment & Cyber stalking : Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

(2) Against Property

(i) Credit Card Fraud : As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

(ii) Intellectual Property crimes : These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

(iii) Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

(3) Against Organisations

(i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms:

a) Changing/deleting data: Unauthorized changing of data.

b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack : When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse : This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

(4) Against Society

(i) Forgery :Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism :Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) Web Jacking :Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money

Prevention of Cyber Crimes:

Since the Information Technology Act, 2000 did not covered all the aspects of cybercrimes committed; amendments were done in the Rajya Sabha on 23rd December, 2008, renaming the Act as the Information Technology (Amendment) Act, 2008 and was referred to as ITAA, 2008. Eight new Cyber Offences were added to ITAA, 2008 under the following sections:

Sr. No.	Sections under the Information Technology (Amendment) Act, 2008	Punishment
1.	**Section 66A:** Cyber Stalking, i.e., sending offensive messages through any communication services like a computer or mobile phone	Imprisonment up to 3 years long with a fine.
2.	**Section 66B:**Receiving stolen computer's resources or communication device dishonestly	Imprisonment which may extend up to 3 years, or with a fine of rupee 1 lakh or both.
3.	**Section 66C:**Identity Theft	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
4.	**Section 66D:**Phishing, i.e., punishment for cheating by personation by the use of computer's resources	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.

5.	**Section 66E:**Voyeurism, i.e. punishment for violating privacy of an individual	Imprisonment for 3 years along with a fine which may be extended up to 2 lakh rupees or both.
6.	**Section 66F:**Cyber Terrorism	Life imprisonment.
7.	**Section 67A:**Publishing/ or transmitting material in electronic form containing sexually explicit contents	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first convict; and imprisonment can be extended up to 7 years with fine of 20 lakh rupees in the second convict.
8.	**Section 67B:**Child pornography	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first conviction; and imprisonment can be extended up to 7 years with an extended fine of 10 lakh rupees in the second conviction.

CONCLUSION:

To conclude, we can say that the advent computer networking and newly developed technologies have given rise to cybercrimes in the past few years. This has created great threats to mankind because the victim is known to the attacker and he/she with malicious intentions like causing harm to the computer system, stealing or erasing data saved in the system, changing password, hacking credit card details, and bank account number, etc., commits such crimes. Different types of cybercrimes like cyber stalking, cyber terrorism, cyber pornography, morphing, forgery, email spoofing, identity theft, etc., have serious impacts over the society. The cybercriminal gains unauthorized access to computer resources or any other personal information of the victim by hacking their account. It is, therefore, very important for every individual to be aware of these crimes and remain alert and active to avoid any personal or professional loss.

REFERENCES:

1. Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning
2. Bar Association of India (2015). Anti-Bullying Laws in India. Retrieved from https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-india.pdf
3. Brenner, W. Susan (2010). Cybercrime: Criminal threats from cyber space. Green Wood Publishing Group, Westport.
4. Chinov, Mike (2000). Aid Workers Decry Growing Child Sex Trade in Cambodia. CNN.com Retrieved from http://archives.cnn.com/2000/asianow/southeast/09/18/cambodia.pedophile/index.html
5. Staff Author, CNN (2001). Sex Slavery: The Growing Trade. CNN.com Retrieved fromhttps://archives.cnn.com/2001/world/europe/03/08/women.trafficking/
6. Flemming, P. and Stohl, M. (2000). Myths and Realities of Cyber terrorism. International Conference on Countering Terrorism through Enhanced International Cooperation, Page No. 22-24, September, Italy.
7. Hafele, D. M. (2004). Three different shades of Ethical Hacking: Black, White and Grey. February 23, 2004.
8. Higgins, George (2010). Cybercrime: An Introduction to an Emerging Phenomenon. Mc Graw Hill Publishing, New York.
9. Holt, Thomas J. (2011). Crime Online: Correlates Causes and Contexts. Caroline Academic press, USA.
10. International Journal of Social Science and Humanities Research (2016). A Sociological Study of Different Types Of Cyber Crimes. Vol.4, Oct-Dec 2016. Retrieved fromhttp://www.researchpublish.com/journal/IJSSHR/Issue-4-October-2016-December-2016/0
11. Singh, Talwant (2011). Cyber Law and Information technology. New Delhi, India.
12. Wall, David S. (2001). Crime and the Internet. Routledge, London.
13. www.tigweb.org/actiontools/projects/download/4926.docx
14.http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp#21/4/201
15.https://www.tutorialspoint.com/information_security_cyber_law/introduvtion.htm
16. https://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india
17.http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_C YBER_LAW
18. http://deity.gov.in/sites/upload_files/di/files/downoads/itact2000/itbill2000.pdf
19. http://www.lawyersclubindia.com/articles/Classifiaction_Of_CyberCrimes_1484.asp
20. http://vikaspedia.in/education/Digital%20Literacy/information-security/cyber-laws
21. https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V518-0156.pdf
22. https://indiankanoon.org/doc/1439440/
23.http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20%202008%20%28amendment%29.pdf
24. https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/

Author Profile:

Mr. Gaurav Jain Pursed Bachelor of Computer Science and Engineering from LNCT Group of Collage , RJPV Bhopal in the Year 2014 and Masters in Cyber Security from Madhav Institute of Technology and Science in the year 2017. He has published Several Research Papers in Reputed international journals including IEEE and UGC approved Journals. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, Image Processing, Deep Learning or AI or ML based education. He has 3 years of Research Experience or 5 Years Industrial Experience and almost 1 year Experience in Teaching.