Crimes and Laws Related to Internet users: An Overview

AdilRasool
Govt. College Jammu

Abstract

The internet has become need of current world. It provides wide and extensive range of facilities including access to the global stores of Information. The Internet access allows instant access to both current and historical sources of information that results saving of time, which is more precious than gold at present time. Looking towards the other side of the same coin, there are few shortcomings while adopting Internet usage. Which is wrong usage of Internet i.e. for unethical means? In present Internet world, such means are known as Cyber-crimes. To highlight such activities, present study was conducted with main focus to raise awareness regarding suchcrime activities; further the present study also mentioned the penalties for committing such activities as per cyber laws and I.T Act.

Key Words: *Cyber Crime, Cyber law and I.T Act*

I. INTRODUCTION

According to Naoh Feldman, "Cyber war takes place largely in secret, unknown to the general public on both sides"

A crime committed or facilitated via the Internet is a cybercrime. 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.

Internet connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices.

II. TYPES OF CYBER CRIMES

- Harassment via e-mails: it is very common type of harassment through sending letters, attachments of files and folders i.e. through e-mails. At present harassment is common as usage of social sites i.e. facebook, Twitter etc. increasing day by day
- 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 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.
- E-mail Spoofing: A spoofed email is said to be that, which misrepresents its origin. It shows its origin to be different from which it originally originates.
- Cyber-Stalking: it means expressed or implied a physical threat that creates fear through the use of computer technology such as internet, e-mail, phones, text messages and webcam.
- Hacking: among the all types of cybercrime it is the most dangerous and serous thread to the internet and e-commerce. Hacking simply refers to the breaking into the computer system and steals valuable information (data) from the system without any permission. Hacking is done by hackers now the question arises who are hackers; hackers are in b/w client & server and able to spoof the data/info. Duplication the IP address illegally.
- Cracking: it is amongst the gravest cyber known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and permission, and has tempered vital, confidential data and information.
- 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.
- Child Pornography: it involves the use of computer networks to create, distribute, access materials that sexually exploit underage children.

- 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.

- Defamation: it is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails using vulgar language to known and unknown persons.
- Intellectual property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software privacy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc
- Cyber Squatting: it means where two persons claim for the same domain name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. E.g. two similar names like www.yahoo.com and www.yaahoo.com
- Cyber Vandalism: Vandalism means deliberately destroying and damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include any kind of physical harm done to the computer. Such act may take the form of theft of computer, some parts of computer or a peripheral attached to the computer.
- Internet Time Thefts: basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet data/hours paid for by another person. The person gets access to someone's ID and password either by hacking or by gaining access to it by illegal means, access the internet without the owner's knowledge.
- Cyber Terrorism: It is a major burning issue in both local as well as international levels. The common form of these terrorist attacks on the Internet is by disturbed denial of service attack, hate websites and hate e-mails. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- Online Gambling: online fraud and cheating is one of the most worthwhile businesses that are growing today in the cyber space. It includes credit card crimes, offering jobs etc.

A. Cyber Law

Cyber law governs the legal issues of cyberspace. The term cyberspace is not restricted to the internet. It is very wide term such as computers and computer networks, the internet, Data, software etc. cyber law encompasses laws relating to electronic and digital signature, computer crime, intellectual property, data protection and privacy and telecommunication laws.

B. Electronic And Digital Signature

Electronic signature are the fast becoming the defacto standard for authentication of electronic records, electronic data interchange, emails etc.
Comprehensive laws are required so that uniform standards and procedures can be established. These laws relating to electronic signature e.g. the electronic signature in global and national commerce Act of the USA, are part of cyber law.

C. Computer Crime Laws

Outgrowing dependence on computers and the Internet has made us all potential victims of Internet threats. Some countries have enacted legislations that specially deals with computer crime and yet others have adapted their existing laws to make computer crime an offence existing statutes. These laws are under the gambit of cyber law.

D. Intellectual Property Law

Cyber law covers the intellectual property laws that relate to cyber space and its constituents. These include:

- Copyright law in relation to computer software, computer source code etc.
- Trademark law in relation to domain names
- Semiconductor law, which relates to the protection of semiconductor design and layouts.
- Patent law in relation to computer hardware and software.

Data Protection and Privacy laws:
Many nations have enacted legislation relating to data protection and privacy within their jurisdictions. It is pertinent to note that due to the nature of Internet and the amount of information that may be accessed through it, such as legislation is critical to protect the fundamental rights of privacy of an individual. These laws would probably play a vital role, as the dependence on insecure networks such as the Internet grows further.

E. Telecommunication Laws

Telecommunication systems also fall within the ambit of cyberspace and therefore would form an integral part of cyber laws.

F. Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following-

- Unauthorized access of the computers
- Data diddling
- Virus/worm attack
- Theft of computer system
- Hacking
- Denial of attack
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physical damaging computer system.

The offences included in the I.T act 2000 are as follows-

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of controller to give directions.
- Directions of controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty of misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing digital signature certificate false in certain particulars.
- Publishing for fraudulent purpose.
- Act to apply for offence or contravention committed outside India confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

The following detail shows the offence and penalties against all the mentioned sections of the I.T Act-

Under I.T Act-section 65, offence such as tampering with computer source code is liable for the punishment of imprisonment up to 3 years or fine up toRs 2 lakhs. Moreover, such offence is bailable, cognizable and triableby court of judicial magistrate of first class.

Under I.T Act-section 66, offence such as computer related offence is liable for the punishment of imprisonment up to 3 years or fine up to Rs 5 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-A, offence such as Sending offensive messages through communication service is liable for the punishment of imprisonment up to 3 years and fine. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-B, offence such as dishonestly receiving stolen computer resources or communication devices is liable for the punishment of imprisonment up to 3 years or fine up to Rs 1 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-C, offence such as Identity theft is liable for the punishment of imprisonment of either description up to 3 years and/or fine up to Rs 1 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-D, offence such as Cheating by Personation by using computer resource is liable for the punishment of imprisonment of either description up to 3 years and/or fine up to Rs 1 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-E, offence such as Violation of Privacy is liable for the punishment of imprisonment of either description up to 3 years and/or fine up to Rs 2 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 66-F, offence such as Cyber Terrorism is liable for the punishment of imprisonment extend to imprisonment for life. Moreover, such offence is Non-bailable, cognizable and triable by court of sessions.

Under I.T Act-section 67, offence such as Publishing or transmitting obscene material in electronic form is liable for the punishment of imprisonment of up to 3 years and/or fine up to Rs 5 lakhs on first conviction and on subsequent conviction imprisonment of up to 5 years and/or fine up to Rs 10 lakhs. Moreover, such offence is bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 67-A, offence such as Publishing or transmitting of material containing sexually explicit act,etc…in electronic form is liable for the punishment of imprisonment up to 5 years and/or

fine up to Rs10 lakhs on first conviction and on subsequent conviction imprisonment of up to 7 years and/or fine up to Rs 10 lakhs. Moreover, such offence is Non-bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 67-B, offence such as Publishing or transmitting of material depecting children in sexually explicit act etcin electronic form is liable for the punishment of imprisonment of either description up to 5 years and/or fine up to Rs 10 lakhs on first conviction and on subsequent conviction imprisonment of up to 7 years and/or fine up to Rs 10 lakhs. Moreover, such offence is Non-bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 67-C, offence such as Intermediary intentionally or knowingly contravening the directions about preservation and retention of information is liable for the punishment of imprisonment of up to 3 years. Moreover, such offence is Non-bailable, cognizable and triable by court of judicial magistrate of first class.

Under I.T Act-section 68, offence such as Failure to comply with the directions given by controller is liable for the punishment of imprisonment of up to 2 years and/ or fine uptoRs 1 lakh. Moreover, such offence is bailable andnon-cognizable by court of judicial magistrate of first class.

Under I.T Act-section 69, offence such as Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource is liable for the punishment of imprisonment of up to 7 years and fine. Moreover, such offence is non-bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 69-A, offence such as Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource is liable for the punishment of imprisonment of up to 7 years and fine. Moreover, such offence is non-bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 69-B, offence such as Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) is regard monitor and collect traffic data or information through any computer resource for cyber security is liable for the punishment of imprisonment of up to 3 years and fine. Moreover, such offence is bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 70, offence such as any person who secures access or attempts to secure access to the protected system in contravention of provision of sec.70 is liable for the punishment of imprisonment of either description up to 10 years and fine. Moreover, such offence is non-bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 70, offence such as any person who secures access or attempts to secure access to the protected system in contravention of provision of sec.70 is liable for the punishment of imprisonment of either description up to 10 years and fine. Moreover, such offence is non-bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 70-B, offence such as Indian Computer Emergency Response Team (ICERT) to serve as national agency for incident response. Any service provider, intermediaries, data centers, etc, who fails to prove the information called for or comply with the direction issued by the ICERT is liable for the punishment of imprisonment up to 1 year and/or fine up to Rs 1 lakh. Moreover, such offence is bailable and non-cognizable by court of judicial magistrate of first class.

Under I.T Act-section 71, offence such as misrepresentation to the controller to the certifying authority is liable for the punishment of imprisonment up to 2 years and/or fine up to Rs 1 lakh. Moreover, such offence is bailable and non-cognizable by court of judicial magistrate of first class.

Under I.T Act-section 72, offence such as Breach of confidentiality and privacy is liable for the punishment of imprisonment up to 2 years and/or fine up to Rs 1 lakh. Moreover, such offence is bailable and non-cognizable by court of judicial magistrate of first class.

Under I.T Act-section 72-A, offence such as Disclosure of information in breach of lawful contract is liable for the punishment of imprisonment up to 3 years and/or fine up to Rs5 lakh. Moreover, such offence is bailable and cognizable by court of judicial magistrate of first class.

Under I.T Act-section 73, offence such as publishing electronic signature certificate false in certain particular is liable for the punishment of imprisonment up to 2 years and/or fine up to Rs 1 lakh. Moreover, such offence is bailable and non-cognizable by court of judicial magistrate of first class.

Under I.T Act-section 74, offence such as publishing for fraudulent purpose is liable for the

punishment of imprisonment up to 2 years and/or fine up to Rs 1 lakh. Moreover, such offence is bailable and non-cognizable by court of judicial magistrate of first class.

The use of the Internet has several advantages. It has changed the way the world communicates and does business. However, there can be negative aspects to the excessive use of the Internet. Disadvantages of using the Internet are loneliness, lack of face-to-face communication, poor conflict resolution, diminishing interpersonal skills, overdependence on technology, mood swings and physical problems such as painful wrists and arms and obesity. Potential financial loss is another possibility. People who use the Internet to carry out banking and other forms of financial transactions are at a risk of losing their money, as hackers are always on the prowl.

REFERENCES

[1] Broadhurst, R. G. (2006). Developments in the global law enforcement of cyber-crime. Policing: an International Journal of Police Strategies and Management, 29(3), 408-433.

[2] Casey, E. (2002). Error Uncertainty and Loss in Digital Evidence. International Journal of Digital Evidence, 1(2).

[3] Chaikin, D. (2006). Network investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, 46, 239-256.

[4] Chaski, C. E. (2005). Who's At The Keyboard? Authorship Attribution in Digital Evidence Investigations. International Journal of Digital Evidence, 4, 1-13.

[5] Downing, R. W. (2005). Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. Columbia Journal of Transnational Law, 43, 741-762.

[6] Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, 10(2), 139-223.

[7] Kirby, M. D. (2008). The Urgent Need for Forensic Excellence. Criminal Law Journal, 32.

[8] Liao, Y. (2001). Analysis of computer crime characteristics. Journal of Information Technology and Society, 1, 119-133.

[9] Luen, T. W., & Al-Hawamdeh, S. (2001, October). Knowledge management in the public sector: principles and practices in police work. Journal of Information Science, 27(5), 311-318.

[10] Mitchell, K. J., Wolak, J., &Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working? Sex Abuse, 17, 241-267.

[11] Mitchell, K. J., Wolak, J., &Finkelhor, D. (2005).The Internet and family and acquaintance sexual abuse. Child Maltreat, 10, 49-60.

[12] Pallaras, P. (2011). New Technology: opportunities and challenges for prosecutors. Crime, Law and Social Change, 54(1), 71-89.

[13] Pocar, F. (2004). Defining Cyber-Crimes in International Legislation. European Journal on Criminal Policy and Research, 10, 27–37.