International Journal of Information Movement *Vol. 8 Issue VIII (December, 2023)*
Website: www.ijim.in ISSN: 2456-0553 (online) Pages 1-5

AN EXTENSIVE EXAMINATION OF CYBERCRIMES AND LAW

Dr. Meenakshi Dahiya
Assistant Professor
Department Of Law,
PDM,University,Bahadurgarh
Email-id: meenakshidahiya9@gmail.com

Abstract: Cyber law refers to the legal concerns surrounding the use of telecommunication technology. Intellectual property, privacy, freedom of expression, and legal jurisdiction are all included in the section on cybercrime. The IT (Amendment) Act, 2008, which revised the IT Act, 2000, is referred to as the "Cyber laws" and attempts to reduce criminality associated to the internet and cyberspace. To understand cyber law, we need to pay more attention to the phrase "crime," which refers to any criminal conduct carried out via computers, the Internet, cyberspace, and the worldwide web. Cybercrimes include, but are not limited to, hacking, child pornography, cyber stalking, denial of service attacks, malware, phishing, information warfare, and many types of online theft. Indian law, namely the IT (Amendment) Act of 2008 and the Information Technology Act of 2000, penalizes certain cybercrimes and cybercriminals. Cybercriminals conduct crimes for a variety of motives, including monetary gain, some personal gain, annoying victims for any purpose, damaging certain systems, stealing data and information, information warfare, etc. These criminals usually use modern means of communication, such as phishing, email spoofing, mobile phones (SMS/MMS), chat rooms, emails, groups, and bulletin boards on the Internet. Since technological advancements have made Data-related crimes are usually carried out using USB media, Bluetooth technology, wireless media, and data storage devices like DVD, Pen Drive, Flash Drive, Micro chip, etc. since it is easier to steal data and information. The security and financial stability of a nation may be threatened by such crimes. These crimes' related problems have gained attention, especially those involving copyright violations, child pornography, and child grooming. When private information is misplaced or illegally intercepted, privacy issues might also arise. As a result, using common sense, learning IT, being prepared, and taking precautions are your best lines of protection against cyber crime.

Key words: Cyber law and cybercrime, Different aspects of cybercrime, Cybercrime and its types, An Introduction of cyber crimes, How Can You Stay Safe from cyber criminals, Hacking and cracking.

1.0 Introduction

Criminal behavior carried out through computers, a network, or the Internet is known as cybercrime. Cybercriminals are those who participate in online crime. These criminals usually use modern means of communication, such as phishing, email spoofing, mobile phones (SMS/MMS), chat rooms, emails, groups, and bulletin boards on the Internet. Since technological advancements have made it simpler to steal data and information, data-related crimes are typically carried out via USB media, Bluetooth technology, wireless media, and data storage devices like DVD, Pen Drive, Flash Drive, Micro chip, etc.

Because of this, the topic "A Comprehensive Study of Cyber Law and Cyber Crimes" focuses on specifics about cybercrime, its varieties, and the numerous laws under the IT Act 2000 and the IT (Amendment) Act, 2008. There are several helpful tips that might protect you from these scams.

1.2 Objective

The primary goal of the proposed topic, "A Comprehensive Study of Cyber Law and Cyber Crimes," is to increase public awareness of cyberspace, aim to protect people from online fraud, and provide relevant legal frameworks.

1.3 Crime Related to Cyber Law

"Cyber law" describes the legal issues surrounding the use of communications technology, most notably "cyberspace," or the Internet. Unlike earlier legislation, it covers cybercrime in addition to matters pertaining to jurisdiction, intellectual property, privacy, and freedom of speech. Cyber law is an attempt to modify laws meant for the offline world to address people's behavior on the internet. India's cyber laws are outlined in The IT Act, 2000, which was updated by The IT (Amendment) Act, 2008[1]. It features a separate chapter XI labeled "Offences" where many cybercrimes have been designated as criminal offenses subject to both jail time and monetary penalties.

We must put more emphasis on crime, which includes all illegal activity carried out via computers, the Internet, cyberspace, and the global web, in order to fully comprehend cyber law.

1.0 Categories of Cybercrimes

Following are the some activities which come under cybercrime i.e.

1. Hacking
2. Child Pornography
3. Cyber Stalking
4. Denial of Service
5. Dissemination of Malicious Software (Malware)
6. Phishing
7. Information Warfare
8. Data Theft
9. Identity Theft
10. Email Spoofing
11. Network Related Wrongs **[2]**

2.1 Hacking

Unauthorized access to a computer system or network is known as a hack. The word "cracking" is synonymous with "hacking," despite the fact that there is no legal distinction between the two in India. Any activity done to obtain access to a computer system or network is referred to as hacking. Hackers use pre-made programs or write their own to attack the target computer. Hackers who want to profit financially from their exploits may gain credit card information or transfer funds from other bank accounts to their own before taking withdrawals. Based on information obtained when hacking into a specific computer network, they also engage in extortion.
In addition to sections 379 and 406 of the Indian Penal Code, 1860, section 43(a) [3] read in conjunction with section 66 of the Information Technology (Amendment) Act, 2008 is pertinent legislation.

2.2 Child Pornography:

Child pornography is pornography with children in it [4]. A wide range of media, including text, periodicals, photography, artwork, cartoons, paintings, animation, sound recordings, movies, videos, and video games, may be used in pornography. Child abuse photos, commonly referred to as child pornography, can be real, fake, or directly made with the kid's participation. The sexual actions that are captured in the creation of child pornography involve the abuse of children [5].
When it comes to sexual photos of prepubescent, pubescent, or post pubescent children as well as computer-generated images that seem to be of them, the phrase "child pornography" is used legally. The majority of kid possessors photographs of prepubescent children are found in the possession of pornographers who are arrested; nevertheless, even if those photographs also violate the law, individuals who possess images of post-pubescent juveniles are less likely to face legal action. **[6]**.

2.3 Cyber Stalking:

The term is employed to characterize the act of stalking someone else through the internet, email, or other electronic communications tools. Generally, stalking entails a person making repeated threats or acts of harassment. It can be accomplished through making phone calls, leaving notes or other materials, or damaging someone's property. Cyber stalking is also known as persistent acts of harassment or threatening conduct committed by a cybercriminal against a victim while utilizing online services. According to a survey, the following techniques are most commonly used by online stalkers:

a. Gather details regarding the victim's identity. In situations where the stalker is an unknown individual to the victim, he obtains information from internet databases, including profiles the victim may have made while registering for a website, chat service, or email account.

b. By posting information on any website connected to dating or sex services and posing as the victim, the stalker may encourage people to call the victim on her phone in order to seek sexual services.

c. Some stalkers add the victim's email address to a variety of sex and pornographic websites, which causes the victim to start getting inappropriate email offers.

d. Some stalkers send several emails to the victim requesting various favors or threatening them [7].

2.4 Inability to access a service:

This is a technologically-driven cyber attack where the attacker disables the victim's email account or floods their bandwidth with spam emails, preventing them from accessing the Internet and its services. You may launch a DoS attack by employing

a. The utilization of computer resources, including CPU time, disk space, and bandwidth..
b. Disturbance of configuration data, such as routing information, etc.
c. Interference with the actual network's hardware.

2.5 The spread of malicious software, or malware:

Software that impedes computer operations or gathers sensitive data or private computer systems is referred to as malware, often called malicious software. It can take the shape of code, scripts, live content, or other applications. Malware creation and distribution are significant crimes in every country, yet they are nevertheless developed for a variety of purposes, including profit-making and capabilities demonstration.

Computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, and other malicious software are examples of malware that is especially dangerous for information technology. [8]

2.6 Phishing:

It is the act of posing as a trustworthy party via the internet in an effort to get credit card details, usernames, passwords, and sometimes even cash. Phishing often involves tricking victims into entering personal information on a fake website that looks and feels almost exactly like the genuine one. Usually, instant chat or email spoofing are used for it. Phishing is a type of social engineering method that takes use of the usability issues with existing online security mechanisms to trick users [9].

2.7 Information Warfare:

It Information, as well as assaults against information and its system, are utilized as weapons of war in this type of conflict. Information warfare includes both providing the enemy with propaganda to coerce them into giving up and suppressing information that might strengthen their resistance.

It is a strategy for undermining an opponent's data and information systems while preserving and enhancing one's own information advantage. This type of combat has no front line; instead, potential battlegrounds can be located wherever that networked systems can be accessed, such as phone switching networks, power grids, oil and gas pipelines, etc. [10].

2.8 Data Theft:

According to Wikipedia, data theft is an increasing problem that is mostly performed by office workers who have access to technology such as desktop computers and portable devices like flash drives, iPods, digital cameras, and even mobile phones that may hold digital information. Given that large files may now be sent via web pages, USB devices, DVD storage, email, and other portable media, data theft can have a serious negative impact.

The Information Technology (Amendment) Act, 2000 states that the following constitutes a crime of data theft under Section 43 (b) [11]: If someone downloads, copies, or extracts any data, computer data base, or information from a computer, computer system, or computer network without the owner's or another person's permission, including information or data held or if the data is kept on any removable storage device, then it is theft.

2.9 **Theft of identity:**

Identity theft is a form of deception when one individual adopts the identity of another person and presents themselves as them in order to get resources, obtain credit, or obtain other advantages in their name. Identity theft is defined as the unlawful or dishonest use of another person's electronic signature, password, or other distinguishing identifying trait. It is classified as a crime by the Information Technology (Amendment) Act of 2008 (Section 66-C)[12].

Identity theft occurs when someone uses another person's personal information, such as their name, credit card number, or identifying number, to conduct fraud or another crime without that person's permission.

2.10 Email Spoofing:

It is email activity when the sender addresses and other header information are changed to make it seem as though the email came from another source [13]. Email spoofing is the practice of sending an email to a recipient in a way that makes it look as though it was sent by a different individual. An email spoof is one that looks to come from one source but was really received from another. Spoofing is the practice of electronically posing as another computer in order to get access to the password system. You can no longer assume that the email you are getting is indeed from the sender who is identifiable since it has become so commonplace. The sender address and other email header components can be changed by hackers using a method known as "email spoofing" to send emails that appear to have come from a different address than they actually did. Hackers frequently utilize email spoofing as a technique to hide the actual email address from which spam and phishing emails are sent. It can occasionally be used in conjunction with Web page spoofing to deceive users into divulging sensitive and personal data.

2.11 Network Related Wrongs:

The major victims of this kind of cybercrime are network systems. Because of this activity, a computer network's normal operation is momentarily disturbed. Interference refers to anything like Denial of Service Attacks that use all available bandwidth to momentarily slow down data delivery. This group also includes distributed denial of service attacks, ping of death attacks, and smurf attacks. Data Security Network Sabotage: Deleting files or records from storage or otherwise permanently harming a computer network [14].

2.0 The law pertaining to cybercrime and cybercriminals

- Section 43(a) of the Information Technology (Amendment) Act 2008, applies to hacking.
- Section 43(b) of the Information Technology Act of 2000 penalizes data theft.
- Identity theft is a felony under Section 66-C of the Information Technology (Amendment) Act of 2008.
- Email spoofing techniques employed by hackers are considered a cybercrime under Section 43(a) of the IT Act of 2008.
- The Child Pornography Prevention Act of 1996 (CPPA) prohibits the cybercrime of child pornography.
- There were no laws in India that specifically addressed cyberstalking before to February 2013.
- The Information Technology Act of 2000 (IT Act) was a body of laws designed to govern the internet. But it ignored interpersonal criminal behaviors like cyberstalking and only concentrated on financial crimes (Behera, 2010; Halder & Jaishankar, 2008; Nappinai, 2010).
- The Indian Penal Code was amended by the Indian Parliament in 2013, making cyberstalking a crime.

3.0 Various techniques applied for cyberspace safety

- Continue to update and patch your operating system. Set the "auto update" option.
- Use and update anti-virus and anti-spyware programs.
- Avoid visiting questionable websites or clicking on links that come from unidentified or suspect sources.
- Keep your transactions secure. Before completing an online transaction, check the status bar of your browser for the "lock" icon and make sure "https" is present in the website's URL bar. The letter "s" stands for "secure" and denotes that the website's communication is encrypted.
- Be wary of any communications you receive, including those ostensibly coming from "trusted entities," and use caution when clicking any links they may include.
- Don't reply to any incoming unsolicited (spam) emails.
- Avoid opening any attachments included in shady communications.
- Never reply to emails that ask you to "verify your information" or "confirm your user-id and password."
- Be wary of emails that demand that you "verify your information" or face catastrophic repercussions.
- Avoid entering personal data in pop-up screens. By providing such information, you run the risk of having your identity stolen.
- Use different passwords for accounts that are relevant to your job and those that are not.
- Gain knowledge of contemporary technologies.

4.0 Conclusion

We wish to make the suggestion that this kind of crime and criminals need to be prevented at the conclusion of "A Comprehensive Study of Cyber Law and Cyber Crimes". However, this is not that simple; in order to curb the crime connected to internet, our court system must provide stronger laws. So, in order to combat cybercrime, we advise becoming educated about current technology and following the aforementioned advice.

5.0 References

i. IT Amendment Act 2008, Registered No –DL – (N)04/0007/2003-09 http://deity.gov.in/sites/upload_files/dit/files/downl oads/itact2000/it_amendment_act2008.pdf

ii. IGNOU PGCCL (Post Graduate Certification in Cyber Law) Program, MIR-014 Block No.2, Unit No-5, Page No - 8 to12

iii. IT Amendment Act 2008, Registered No –DL – (N)04/0007/2003-09 http://deity.gov.in/sites/upload_files/dit/files/downl oads/itact2000/it_amendment_act2008.pdf, Page No -06, Point No-22

iv. Finkelhor, David. "Current Information on the Scope and Nature of Child Sexual Abuse.". Future of Children. v4 n2 (Sum–Fall 1994): p31– 53.Source -

v. http://en.wikipedia.org/wiki/Child_pornography

vi. Hobbs, Christopher James; Helga G. I. Hanks, Jane

vii. M. Wynne (1999). *Child Abuse and Neglect: A Clinician's Handbook*. Elsevier Health Sciences. p. 328. ISBN 0-443-05896-2. Source -http://en.wikipedia.org/wiki/Child_pornography.

viii. http://en.wikipedia.org/wiki/Child_pornography - [17]. Wells, M.; Finkelhor, D.; Wolak, J.; Mitchell,

ix. K. (2007). "Defining Child Pornography: LawEnforcement Dilemmas in Investigations of Internet Child Pornography Possession" (PDF). *PolicePractice and Research* 8 (3):269–282. doi:10.1080/15614260701450765. Retrieved 2008-07-01.

x. IGNOU PGCCL (Post Graduate Certification in Cyber Law) Program, MIR-014 Block No.2, Unit No-5, Page No – 9

xi. http://en.wikipedia.org/wiki/Malware-[4]. Microsoft active malware threats". *Malware Encyclopedia*. Microsoft Malware Protection Center.

xii. Retrieved 2013-08-26

xiii. http://en.wikipedia.org/wiki/Phishing -[7]. Jøsang, Audun et al."Security Usability Principles for Vulnerability Analysis and Risk Assessment." (PDF). Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07). Retrieved 2007.

xiv. IGNOU PGCCL (Post Graduate Certification in Cyber Law) Program, MIR-014 Block No.2, Unit No-5, Page No – 11

xv. http://deity.gov.in/hindi/node/1210 : IT Act 2000, Registered No –DL –33004/2000, CHAPTER - IX PENALTIES AND ADJUD1CATION Page No - 15

xvi. IT Amendment Act 2008, Registered No –DL – (N)04/0007/2003-09 http://deity.gov.in/sites/upload_files/dit/files/downl oads/itact2000/it_amendment_act2008.pdf, PageNo -10, Section- 66C

xvii. http://en.wikipedia.org/wiki/Spoofing_attack

xviii. IGNOU PGCCL (Post Graduate Certification in Cyber Law) Program, MIR-014 Block No.2, Unit No-5, Page No – 11&12.