VOLUME 4 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBER CRIME IN INDIA

- Prakshi Jain & Priyanka Popat[1]

ABSTRACT

Cyber crime, which includes a broad range of illegal crimes carried out using technology and the internet, is a fast expanding problem in India. Although it doesn't provide a precise definition of the term, the Information Technology Act of 2000 acts as the main piece of legislation regulating cyber crime. Hacking, which occurs scams, theft of identities, malware attack, cyber stalking and assault, breaches of data, cyber extortion, abuse of children, and other offences are considered cyber crimes in India. The act specifies guidelines and sanctions for a range of offences, including unauthorized access, source code modification, identity theft, and breach of privacy.

Strong passwords, utilizing two-factor authentication, keeping software revised, avoiding phishing scams, using secure Wi-Fi networks, routine data backups, teaching others as well as oneself about cyber security best practices, using firewalls and security software, being cautious on social media, and securing mobile devices are some preventive measures that people and organizations can take to stop cyber crimes. Individual can lessen their susceptibility to a better cyberspace in India by putting these preventive steps into practice.

RESEARCH OBJECTIVE & DESIGN

[1]4th Year BBA LLB (Hons.) Students of Unitedworld School of Law, Karnavati University

The main objectives of the research are to analyze the cybercrimes in India with reference to the authentic data available. The data here obtained has been standardized, studied & deeply analyzed. The exclusive objective of this paper is to know:-

1. What is Cybercrime?
2. Types of Cybercrime
3. Laws related to Cybercrime in India
4. How to prevent Cybercrimes?

This paper is divided into four sections. Firstly, I have examined all about Cybercrime and discussed more about it with different definitions. Furthermore, paper deals with types of Cybercrime which include hacking, computer forgery, cyber stalking, logic bombs, cyber defamation and many more other types. Moreover paper talks about laws related to cyber crime in India where Sections related to IT Act are discussed along with broad areas covered under cyber law like internet fraud, harassment & stalking, defamation etc. By concluding I had mentioned some measures to be taken to prevent cybercrime.

RESEARCH METHODOLOGY

The research combines both historical & logical techniques. The data was compiled using both primary and secondary sources; the important data was collected from legislation, reports and other court judgments.

Secondary sources include books, journals, articles, newspapers, magazines and blogs. All of the provisions of the laws, as well as the facts provided concerning cybercrime in India, have been thoroughly analyzed.

INTRODUCTION

Cybercrime is relatively a new crime in India. Any criminal action that takes place via or through the means of gadgets, the internet, or any other technological device is defined by the

"Information Technology Act"(The Information Technology act, 2000), is referred to as Cybercrime.

Cybercrime is the most widespread type of crime in modern India, and it has disastrous consequences. Criminals not only create considerable harm to the community and the state, but they also frequently conceal their identity. Technically skilled criminals use the internet to commit a range of illegal crimes.

In a broad sense, cybercrime is any offence in which an electronic device or the internet is used as a tool, an object of attack, or both.

Indian courts have interpreted the word 'cybercrime' in various cases, despite the fact that it does not have definition in any act or laws approved by the Indian government. Cybercrime is an uncontrolled evil caused by the improper use of modern society's technology.

The use of electronic devices and other associated technology in everyday life is rapidly rising, and it has grown into a requirement that facilitates user ease. It is an infinite and immeasurable medium. Cyber stalking, cyber terrorism, e-mail spoofing, e-mail bombing and other rapidly developing cyber crimes are only examples. Some classic crimes may be classified as cybercrime if they take place utilizing an electronic device or the internet.

CYBER CRIME: MEANING & DEFINITIONS

Cybercrime is defining as any unlawful behavior involving a computer, networked device or network. While most cybercrimes are committed to make profit for the culprits, certain cybercrimes are committed against computers or devices directly in order to cause damage or disable them.

Cybercrime is the use of technology to enable traditional crimes such as robbery, theft and deception, or as a pre-planned strike, such as hacking a warning system before entering into a prohibited area. All of this is true at the individual, government and nation-state levels.

There will be no laws or law-enforcement institutions ready to give a favorable conclusion in the case of a country assault; the primary emphasis will be political, economic or military pressure.

Cybercrime can include "virtual only" violations such as the distribution of illicit photographs, papers or private information. Professional programming organizations are likewise featured in this classification; they provide digital particular items and attempts to anybody, from unknown individuals to government, including administrative attack denial and accountability for traded off systems. As more of our time spent online cyber-only inappropriate behavior will become more widespread. This tendency is certain to keep push law enforcement farther into the internet.

Under no law had the Indian government supplied a specific definition of cybercrime; even the Information Technology Act, 2000which tackles cybercrime, does not define the word. Howeverthe word 'cybercrime' in general refers to any illicit behavior carried out on the internet or through the use of computers.

*"Offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, via modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards, and groups) and mobile phones (SMS/*MMS*)*[2]

We do not have a specific definition of cybercrime however the Oxford dictionary defines cybercrime a follows:

"Criminal activities committed via computers or the Internet."[3]

"Cybercrime can be defined as those species whose genus is traditional crime and where the computer is either an object or a subject of the criminal conduct."[4]

TYPES OF CYBER CRIMES

[2](Saroha, 2014)
[3](Oxford by Lexico, 2021)
[4](Pati, 2021)

1. **Hacking**

   Hacking is the unauthorized entry of computer systems or networks for the purpose of obtaining information, causing harm, or interfering with services. In order to take over systems, hackers use holes in software, networks, or weak passwords. Their motivations can range from monetary gain to political activism or even just making trouble.

   In the case of Jagjeet singh vs. State of Punjab, the apex court held that in cases of data theft and hacking, the offences under the Indian Penal Code will also be applied along with the penal provisions of the IT Act, and this would not exclude the application of the IPC. This shows the gravity with which the judiciary has regarded the crime of hacking holding hackers or the culprit's liable under two acts i.e., IPC and IT Act.

2. **Phishing**

   Phishing is a type of e-commerce fraud in which criminals use their counterfeit emails, texts, or WebPages to deceive victims into divulging personal information such usernames, passwords, credit card numbers, or their social security numbers. To earn the victim's trust and trick them into giving them their private information, they frequently pose as trustworthy business or people.

3. **Identity theft**

   When a professional obtains and improperly utilizes personal data about someone else, such as their name, social security number, financial information, or information about their credits cards, usually for financial benefit, identity theft has occurred. By using the victim's personal data that has been stolen, fraudsters may register accounts, or engage in other illicit acts.

4. **Malware attacks**

   Malware is the term for harmful software that is intended to interfere with, harm, or allow unauthorized access to computer networks or systems. Viruses, which can grow and

spread to other systems, worms, which can duplicate themselves and propagate without human oversight, ransom ware, which locks data and requests a ransom, and spyware, which covertly gathers data from a user's device are examples of common types of malware.

5. **Cyber stalking and harassment**

It involves intimidating, threatening, or harassing somebody via digital channels like emails, social media sites, or messaging services. This can involve harassing someone online, distributing false information, sending threatening or abusive messages, or creating imaginary profiles.

6. **Data breaches**

When unauthorized individuals access private data kept in networks or computer networks, a data breach occurs. Personal information (including names, addresses, and social security numbers), financial information, intellectual property, and other confidential data are examples of this. Threats by insiders can also result in data breaches.

7. **Cyber extortion**

Threatening people or organizations with the disclosure of private information, the interruption of offerings, or the loss of data in exchange for a monetary reward is known as cyber extortion. Cyber extortion commonly takes the form of ransom ware attacks; in which software encrypt data and demands payment in exchange for its decryption.

8. **Child exploitation**

Internet sexual exploitation of minors is referred to as "child exploitation". This encompasses practices including child trafficking, the creation, dissemination, or possession of child pornography, and online grooming, in which adults establish relationships with kids in order to gain their trust and take advantage of them.

9. **Distribution of Pirated software**

   A collection of rights comprise intellectual property. An offence is any unlawful conduct that wholly or partially denies the owner their property rights. Software piracy, copyright infringement, trademark and service mark infringement, theft of computer source code, etc. are the examples of prevalent IPR violations.

   The **Hyderabad Court** has in a land mark judgment has convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software.(Herald, 2003)

LAWS RELATED TO CYBER CRIME IN INDIA

Cyber crime is primarily governed by the Information Technology Act, 2000 and it's subsequently amendments. Here are the key provisions and laws related to cyber crime in India:

1. **Section 43:- Penalty and Compensation for damage to computer or computer system**

   Unauthorized entry, harm, or interruption to machines or networks is all covered by this clause of the Information Technology Act, 2000. It includes infractions including gaining unauthorized access to the resources of a computer, obtaining, stealing, or extracting information without authorization, delivering viruses or malicious software, and harming computer systems.

   The section outlines punishments and Computer source code tampering is covered by Section 65 of the IT Act. It forbids the financial compensation for such offences.

2. **Section 65:- Tampering with computer source documents**

   Unauthorized alterations, transformation, or destruction of source codes for computers, which may have an effect on computer networks or systems. Modifying

source code can result in security lapses, software flaws, and a breach of sensitive data. Penalties and jail are possible for offenders.

3. **Section 66:- Computer related offences**

   Numerous cybercrimes, such as hacking, data theft, and computer-related offences are covered by Section 66 of the IT Act. It includes a broad variety of actions like gaining unauthorized access to computer systems, stealing data, changing or deleting data, and adding pollutants to computers. Penalties for offenders include jail time and fines.

4. **Section 66B:- Punishment for dishonestly receiving stolen computer resource or communication device**

   The penalty for receiving computer resources or communication devices that have been fraudulently stolen is covered in this section. It makes it illegal to have or use stolen computer resources, including communication devices, login credentials, access codes, and passwords. Offenders may receive jail time and fines.

5. **Section 66C:- Identity theft**

   Identity theft is the focus of Section 66C. It makes it illegal to utilize someone else's identifying information without their permission. This includes deceiving others or committing fraud by using someone else's password, digital signature, or other distinctive elements.

   Infractions can result in 3 years of imprisonment and fines.

6. **Section 66D:- Cheating by Impersonation**

   The use of identities to cheat while accessing computer resources is addressed on Section 66D. Impersonation is made illegal, usually in relation to online fraud or

scams. Criminals use technology to pose as someone they are not in order to deceive others and profit financially.

In addition to fines and imprisonment may extend to three years, this offence carries penalties.

7. **Section 66E:- Punishment for Violation of Privacy**

   Invasion of privacy is covered by Section 66E. It makes it illegal to take, distribute, or publish pictures or recordings of another person's private parts without that person's permission. This section tries to shield users against the unauthorized disclosure of their private or intimate images.

   Infractions can result in imprisonment which may extend to three years or fine not exceeding two lakh rupees.

8. **Section 67:- Punishment for publishing or transmitting obscene material in electronic form**

   This Section addresses the electronic dissemination, transmission, or publication of pornographic material. It forbids the production, dissemination or ownership of pornographic material that is explicit, lewd or targets genitalia.

   Penalties include jail time and fines.

9. **Section 67A:- Punishment for publishing or transmitting of material containing sexually explicit act, etc**

   The publication or transmission of sexually explicit content in electronic form that shows youngsters in a sexually explicit way is covered under Section 67A. It targets child pornography explicitly and provides severe penalties for offences including material depicting child sexual abuse.

   Infractions can result in jail time and fines.

10. **Section 69:- Power to issue directions for interception or monitoring or decryption of any information through any computer resource**

    Service providers are required to cooperate with the government in carrying out instructions for the surveillance, tracking or decryption of information. To acquire evidence or take prevention action against cyber risks or criminal activity, the government has the right to access and analyze digital communications, data and other information.

HOW TO PREVENT CYBER CRIMES

Preventive cybercrime involves implementing a combination of proactive measures and security practices. Here are some important steps to consider:-

1. **Use strong and Unique Passwords**
    - Make sure to use mix of uppercase, lowercase, numbers, special characters, and passwords that are at least eight characters long.
    - Don't use details that could be guessed, including names, date of birth, or common words.
    - To lessen the effects of a potential data leak, use a separate password for each online account.
    - Use a password manager, which creates strong, one-of-a-kin passwords for you and securely saves your passwords.

2. **Enable Two-Factor Authentication**
    - By demanding a second form of authentication in place of your password, two-factor authentication offers an additional degree of security.
    - Receiving a special code through SMS or using an authentication software like Google Authenticator are the common type of Two-Factor Authentication.

- When Two-Factor Authentication is an option, just enable it on all of your online accounts, especially the most important ones like email, banking and social media.

3. **Keep Software Updated**
    - Update your operating system, programmers, and security software on a regular basis.
    - Important security fixes that fix known vulnerabilities are frequently included in updates.
    - When possible, enable automatic updates to make sure you are always protected by the most recent security upgrades.

4. **Be Cautious of Phishing Attacks**
    - Cybercriminals frequently employ phishing to deceive people into disclosing sensitive information.
    - Be careful of emails, messages or phone calls asking for login information, personal information or financial information.
    - Avoid downloading attachments from unidentified sources or clicking on dubious links.
    - Instead of using the offered URLs or phone numbers, confirm the veracity of request by getting in touch with the company directly using their official website or other contact information.

5. **Use Secure Wi-Fi Networks**
    - Insecure public Wi-Fi networks make it simple for hackers to collect your data.

- When using public Wi-Fi, avoid accessing confidential information like online banking or personal accounts.
- Consider utilizing a virtual private network to secure your internet connection and shield your data from strangers if you must use public Wi-Fi.

6. Regularly Back Up Data

- Backup critical information frequently to a protected cloud storage provider or an additional storage medium.
- The presence of backups guarantees that you can restore your data in the case of an attack by ransom ware, hardware malfunction or unintentional deletion.
- Check your backups on a regular basis to make sure they are functioning effectively and can be recovered if necessary.

7. Educate Yourself and Others

- Keep up with the most recent developments, dangers and best practices in cyber security.
- Keep up to date by following reliable sources including technology news outlets, security-related blogs and official security websites.
- Inform your friends, family and co-workers on cyber security best practices to assist them become more aware of them.

8. Use Firewalls and Security Software

- Your devices should be updated with reliable antivirus or anti-malware software.
- On your PCs and routers, turn on firewalls to keep an eye on and manage the network traffic that comes and goes.
- Scan your electronic devices for malware on a regular basis, and get rid of any risks found.

9. Be Mindful on Social Media

- Use your social media accounts privacy settings to limit the information that the general public and other users can see.
- Don't disclose any personal information which could be utilized in social engineering or identity theft schemes.
- Refrain from receiving friend requests or interacting with accounts or communications that seem questionable since they might be fraud or scam attempts.

10. Secure your Mobile Devices

- Use the same security precautions you would for your desktops on your cell phones and tablets.
- To protect your Smartphone, use tough pass codes or biometric identification capabilities like fingerprint or facial recognition.

CONCLUSION

In India, cybercrime is a developing and pervasive problem that poses serious hazard to people, businesses, and the country at large. It includes a variety of illicit behaviors committed online and via technological devices. Although cybercrime is not specifically defined by Indian law, it is often seen as any illegal activity involving computers, networked devices or networks.

The main laws controlling cybercrime in India are the Information Technology Act, 2000.

Unauthorized accessibility, phishing, hacking, theft of identities, malware attacks, cyber stalking, breaches of data, cyber fraud, child exploitation, and other offences are all covered by these laws, there are precise guidelines and sanctions for each offence, such as jail and fines.

Cyber crime needs to be prevented and security measures need to be put in place. This includes creating secure passwords that are both long and unique, enabling two-factor authentication, updating software, avoiding phishing scams, connecting to secure Wi-Fi networks, frequently

backed up data, learning about cyber security best practices, utilizing antivirus programmers and security software, being cautious on social networking sites, and securing mobile devices.

In order to limit threats and safeguard people, organizations, and the country's digital infrastructure, preventing cyber crime in India needs a combination of strong legislation, law enforcement initiatives, public awareness campaigns and proactive cyber security measures.