https://shikshabodh.in/

SHIKSHA BODH

ISSN:
IMPACT FACTOR:
VOLUME-1|ISSUE-1|Jan-March,2026

Cyber Crime and Safety Measures in India: Strategies & Challenges

***Dr. Dharmendra kumar**
Assistant professor
Gandhi Mahavidyalaya, orai, jalaun
Email- dkumarorai@gmail.com
****Ritesh Kumar**
Assistant professor
Gandhi Mahavidyalaya, orai, jalaun
Email- Riteshgmv@gmail.com

ABSTRACT:

Cybercrime refers to actions that use computer systems and the internet as a tool to obtain private information about a person, without the person's knowledge &disclose it on online platforms to damage the person's reputation or cause them mental or physical harm. The rate of cybercrimes has increased as a result of technologicaladvancement. Internet crimes have increased along with our growing reliance on the internet. This is mostly because more than half of online users have inadequate training and education, are unaware of technical changes, and are not completely aware of how online platforms operate India is one of the few nations that passed the **IT Act 2000** to address concerns linked to cybercrimes and prevent their exploitation. However, this act ignores some of the most serious threats to security and challenges that are still rapidly expanding in the current era. Secondary data was acquired for the research paper.The aim is to better understand the idea, its application, and its impact on the economy through various dimensions.

Keywords: Cybercrime,Strategies and Challenges in India, Cyber Law, IT Act 2000.

INTRODUCTION

Since the dawn of civilization, people have fought for advancement and experimented with new technologies to improve their chances of survival. The creation of the computer, which has made life for people easier and more comfortable and serves as a replacement for the human intellect in terms of knowledge and information storage, is the pinnacle of humankind's discoveries and creations. Computer networking has radically facilitated access to and storage of information, eliminating all barriers associated with time and space in communication. As a result, the world has practically become a little village thanks to this technique of information sharing. When the internet first appeared, the founding fathers probably never imagined that it would one day change and be used for illegal purposes, and we would need laws and regulations to safeguard us. These days, a lot of criminal activity takes place online. Cybercrime refers to offenses or crimes that occur on or through the use of a computer or the Internet.Cybercrime is a catch-all phrase that can be used to group a variety of criminal behaviors. Due to the anonymity of the internet, there are a lot of unpleasant actions taking place in cyberspace that could allow the offender to engage in a variety of criminal activities known as cybercrimes. Technology is the primary tool used in cybercrimes,

thus persons who perpetrate these crimes are typically technically skilled and have a solid understanding of the internet and computer programs.Cyberstalking, cyberterrorism, email spoofing, email bombing, cyberpornography, cyberdefamation, polymorphic viruses, and worms are a few of the most recent cybercrimes to arise. If they are committed online or using an internet-based platform, some typical crimes may also fall under the category of cybercrimes. Examples include theft, vandalism, fraud, misrepresentation, pornography, intimidation, threats, and other offenses that are all prohibited by **the Indian Penal Code**. The act of creating, disseminating, changing, stealing, misusing, and deleting information through computer manipulation of cyberspace is known as cybercrime. This is done without the use of physical force and against the victim's wishes or interests. The term "cybercrime" is typically used to describe a variety of illegal behaviors that are directly tied to being carried out through or against digital technology. Cyber Laws have been developed to protect people from cybercrime. The term "cyber law" refers to all the constitutional protections for individuals and institutions as well as measures to monitor online behavior for illegal activities performed through computer networks. "Cyber law is a broad phrase that encompasses the legal and administrative aspects of the Internet and the World Wide Web. Cyber law encompasses everything that is concerned with, relates to, or arises from any legal aspects or obstacles concerning any behavior of digital users and others in cyberspace.

OBJECTIVES:

- To contemplate the concept of cybercrime.
- To get an overview of the common types of cybercrime.
- Know the causes of prevailing cybercrime
- Analyse the different Cyber laws that exist for the protection of people in India
- To specify how one can be prevented from illegal practices

RESEARCH QUESTIONS:

1.What is the meaning of cybercrime?
2.What does cyber law mean?
3.What are different types of cybercrime?
4.What are the major challenges to combat cybercrime in India?
5.What are the safety measuresand legal frameworksavailable to prevent cybercrime?

CYBERCRIME AND CYBER LAW

"Any unlawful act where computer, communication device, or computer network is used to commit or facilitate the conduct of a crime" is ***cybercrime***. Any illegal behavior that occurs on or through a computer, the internet, or another piece of technology recognized under the Information Technology Act is referred to as such. The most pervasive crime that has a severe impact on contemporary India is cybercrime. Criminals not only cost society and the government a lot of money, but they are also very good at hiding who they are. Numerous unlawful actions are carried out by technically proficient criminals on the internet.

Cyber law is the part of the overall legal system that deals with the internet, cyberspace, and their respective legal issues. Cyberlaw covers a fairly broad area covering several subtopics ncluding freedom of expression, access to and usage of the internet, and online privacy.

Generically, cyber law is referred to as the Law of the Internet. Cyber Law is a generic term referring to all the legal and regulatory aspects of the Internet. Everything concerned with or related to or emanating from any legal aspects or concerning any activities of the citizens in cyberspace comes within the ambit of cyber laws. Cyberlaw covers legal issues that are related to the use of communicative, transactional, and distributive aspects of network information technologies and devices. It encompasses the legal, statutory, and constitutional provisions which affect computers and networks.A broader definition of cybercrime would be any illicit conduct that uses a computer or the internet as a tool, a target, or both. The area of the legal system that deals with the internet, cyberspace, and the corresponding legal issues is known as cyber law. Online privacy, access to and use of the internet, and freedom of expression are only a few of the many subtopics covered by the large field of cyber law. The Law of the Internet is a term used to describe cyber law. All legal and regulatory facets of the internet are collectively referred to as "cyber law" in this context. Cyber laws cover everything that has to do with, is connected to, or arises from any legal issues or that relates to citizen actions in cyberspace.Cyberlaw deals with legal matters that are connected to the use of network information technology and devices in a communicative, transactional, and distributive capacity. It includes all statutory, legal, and constitutional provisions that have an impact on networks and computers.***The Information Technology Bill*** was approved by the Indian Parliament's two chambers in ***May 2000***. The Information ***Technology Act of 2000*** was created after the President gave his assent to the bill in ***August 2000. On October 17, 2000***, the Information Technology Act went into effect. This Act applies to all of India, and its provisions also apply to any violation or offense committed by any person, regardless of nationality, even outside the Republic of India's territorial authority. Such an infraction or breach shall involve a computer, computer system, or computer network located in India to be subject to the provisions of this Act. The extraterritorial applicability of the provisions of the ***IT Act 2000*** is provided by ***Section 1(2)*** read in conjunction with Section ***75. 90 Sections*** make up this Act. Rules for cyber cafés, electronic service delivery, data security, and website blocking are among the rules that supplement the Act. The ***IT Act of 2000*** contains cyber laws. The Information ***Technology Act of 2000*** also intends to establish the legal framework necessary to give all electronic records and other actions conducted via electronic means legal sanctity. According to the Act, a contract acceptance may, unless otherwise agreed, be expressed using electronic means of communication and shall have full legal force and effect.

COMMON CYBER CRIMES&LEGAL FRAMEWORK

Cyberbullying

Cyberbullying means repeated acts of harassment or threatening behavior of the cyber-criminal against the victim through the use of Internet services. A person found guilty is criminalized under ***Section 66E***

Phishing

Phishing involves impersonating a reliable person or company in an official electronic communication, like an email or an instant message, to fraudulently acquire sensitive information, such as passwords and credit card numbers.**Section 66D** deals with such cybercrimes.

Cyber Stalking

It entails tracking someone's whereabouts and sneakily chasing them. It entails obtaining information that might be used to threaten or harass a person, the person who committed this

offense may be charged under ***section 72*** of the ***IT Act, 2000*** for breach of confidentiality and privacy. Additionally, ***IPC sections 441and 509*** are also applicable.

Cyber Pornography

It poses a serious risk to the safety of women and children since it entails posting or sending pornographic content online that can be promptly replicated on a variety of other technological devices.According to ***IT Amendment Act 2008*** "crime of pornography under ***section 67-A*****,** whoever publishes and transmits or causes to be a published and transmitted in the electronic form any material which contains sexually explicit act or conduct can be called as pornography. Additionally applicable are ***Sections 292/293/294, 500/506, and 509 of the Indian Panel Code.***

Cyber Morphing

It is an illegal act when the original image is altered by an unauthorized user or someone using a false identity. users' photos are copied from their profiles and edited before being uploaded for sexual reasons by bogus accounts on several websites. The users' lack of understanding is what encourages crooks to perpetrate such horrible actions. ***Sections 43 and 66*** of the Information ***Act of 2000***criminalize cybermorphing and cyberobscenity.

Email Spoofing and Impersonation

One of the most frequent cybercrimes is this one. Its beginnings can be seen in the sending of emails. Today, this type of crime is so prevalent that it is quite challenging to determine whether mail that is received is coming from the intended sender. Most often, email spoofing is used to illegally get personal information and private photographs from women, which are then used to blackmail them. ***Section 66-D*** of the Information Technology Amendment ***Act of 2008 and Sections 417, 419, and 465*** of the Indian Panel Code both make email spoofing a crime.

Identity Theft

Identity theft is a type of fraud or identity theft in which someone appears to another person's identity and appears to be them to access resources, get credit, or get other benefits in their name. *Section 66* specifically addresses identity theft, where someone uses another person's identity for fraudulent purposes.

Hacking

Hacking simply implies getting into another's computer without permission. Gaining unlawful access or unauthorized entry into a computer or any other electronic as well as digital device belonging to another is hacking. Hacking into computer systems or networks without authorization iscovered under **Section 66 of the IT Act.**

CHALLENGES OF CYBERCRIME

There is constant debate over obstacles in our battle against cybercrime. The following is a discussion of a few of them:

1. Security forces and law enforcement personnel are unprepared to handle high-tech crimes.
2. Lack of promotionof research and development in combating the issues of ICT.
3. The current protocols are insufficient in identifying the investigative responsibility for crimes that cross international borders.

4. Budgets allocated by the government for security purposes, particularly for educating law enforcement, security officers, and investigators in ICT, are lower than for other offenses.
5. Lack of skilled and competent personnel to carry out the countermeasures.
6. A lack of cyber security awareness and culture, both at the individual and organizational levels.
7. No electronic mail addresses are allowed, especially for members of the armed forces, law enforcement, and security services.
8. The bare minimum needed to join the police doesn't include any knowledge of the computer industry, making them virtually illiterate when it comes to cybercrime.

9. The rapid pace of cyber advancements always outpaces the progress of the govt. sector, making it impossible for them to pinpoint the source of these cyber crimes.

PREVENTIVE MEASURES & RECOMMENDATIONS TO COMBAT CYBER CRIMES

Use strong passwords for each account, use a unique combination of usernames and passwords, and avoid writing them down. Your passwords can be easily cracked using a variety of techniques if they are weak. Utilise diverse letters, special characters, and numbers to make the passwords challenging.

Constantly change your passwords:Avoid using a single password for everything. You can often update your password to make it more challenging for hackers to access the password and the stored data.

Be Cautious: It is nearly difficult to use an online platform without disclosing any personal information; as a result, one should exercise caution when disclosing any personal information online.

Parental Supervision: Parents should monitor all of their children's online activity. Parents should routinely examine their children's email accounts and browsing histories. Enable parental controls in browsers and mobile apps so that children can only visit the websites that have been registered. This will shield kids from online scams.Inform people and staff on best practices for cybersecurity.

Education and Awareness:The need of the hour is Keeping up with the rate of change. Since the majority of internet crimes occur as a result of users' ignorance and lack of understanding.Education systems must initiate contemporary issues regarding online crimes and awareness should be spread regarding safe internet uses

Data Encryption:Encrypt sensitive data both at rest and in transit.This ensures that even if data is compromised, it remains unreadable without the encryption keys.

Regular Backup:Create and maintain regular backups of critical data.Ensure backupsfrom time to time.

Keep social media private Make sure your social networking profiles (e.g. Facebook, Twitter, Instagram) are set to private.Check your security settings, and be careful what information you post online. Once it is on the Internet, it is there forever.

Strict Legal Framework:The government should impose stricter regulations on Internet

Service Providers **(ISPs),** as they have a complete record of the data that Internet users accuse of being misused. Additionally, to stop crimes before they start, they should report any suspicious activity.

CONCLUSION

One of the biggest difficulties facing Indian and international law enforcement is cybercrime, or criminal activity on the Internet,which includes unauthorized access to information and violating security such as privacy, passwords, etc. anyone who has Internet use.ICT spreads even more, components of technological crime will be present in all types of criminal activity, including those that are today seen as more traditional. It already plays a role in numerous international crimes involving the trafficking of illegal drugs, smuggling of persons, terrorism, and money laundering. We must be ready to handle this new issue as digital evidence becomes more prevalent, even in traditional crimes. To assure safety and security on the Internet, law enforcement agencies from all around the world are collaborating to create new alliances, new forensic techniques, and new responses to cybercrime.To combat, stop, and respond to cybercrime, new investigative techniques, technologies, and abilities will need to be used in a global environment. New types of crime, a considerably wider scope and scale of victimization, the need to respond much more quickly, and difficult technical and legal complications will all be features of this "new business." To resolve the severe jurisdictional concerns, creative solutions like the establishment of "cyber cops," "cyber courts," and "cyber judges" might be required.**FERENCES**

1.Adv. Prashant Mali, *IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part1*

*2.*A comparative analysis of cybersecurity initiatives worldwide, International Telecommunication Union, Geneva, 28 June -1 July 2005.

3. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.

4. Cybercrime classification,[Online],Available: http:// shodhganga. inflibnet.ac.in/ bitstream /10603/7829/12/12_ chapter % 203.pdf [29 September 2013]

5. Cybercrime system requirements in India: Most necessary thing inIndia, [Online],Available: http://www.cyberlawsindia.net/ requires. html [13 May 2012].

6. Animesh Sarmahand and Amlan Jyoti Baruah (2017), Volume 04, Issue 06, PP. 1633-1640.

7..https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGIN G_EVERYTH ING_-_AN_EMPIRICAL_STUDY

8.https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-tocurtail-its-spread-worldwide

9. cybercrime | Definition, Statistics, & Examples | Britannica

10.A Study on Cyber Crime and its Legal Framework in India - International Journal of Law Management & Humanities (ijlmh.com)

11. A Study on Cyber Crime and its Legal Framework in India - International Journal of Law Management & Humanities (ijlmh.com)