Page 3215 - 3225 **DOI:** *https://doij.org/10.10000/IJLMH.114769*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 2

2023

Cyber-Crime Causes and Prevention

NIKITA VERMA[1]

ABSTRACT

Cybercrime refers to crook sports that are finished the use of the net or other varieties of virtual verbal exchange era. This consists of a wide variety of illegal sports, consisting of hacking, identity robbery, phishing, ran-somware attacks, and dispensed denial-of-carrier attacks. Cybercriminals use numerous methods to gain unauthorized access to laptop systems or networks borrow touchy records, and purpose harm or disruption to computer systems and networks. They may additionally take advantage of vulnerabilities in software program or operating systems, use social engineering strategies to trick people into presenting personal information or downloading malware, or use botnets to launch coordinated assaults. The impact of cybercrime can be significant, both in terms of financial losses and damage to reputations. Preventing cybercrime requires a combination of technological solutions, such as firewalls and antivirus software, and effective cyber security policies and procedures. This includes educating individuals about the risks of cybercrime and how to protect themselves, as well as implementing strong password policies, regular software updates, and data backup protocols.

Keywords: *Cyber, Crime, Security*

I. INTRODUCTION

Cybercrime is a developing hazard in ultra-modern digital age, with criminals the usage of era to carry out a range of unlawful activities. These sports include hacking, identity theft, on line fraud, ransom ware assaults, and disbursed denial-of-provider attacks. Cybercriminals can goal people, agencies, and even governments, and the effect in their sports can be widespread, inflicting monetary losses, reputational damage, and even endangering country wide security. As technology keeps strengthening and greater humans rely on the internet for enterprise, communiqué, and enjoyment, the threat of cybercrime is increasing. Cybercriminals are constantly developing new techniques to exploit vulnerabilities in laptop systems and networks, and that they regularly use state-of-the-art strategies to stay away from detection. Law enforcement agencies around the world are working to combat cybercrime, but it can be challenging to track down and prosecute cybercriminals, who may be located in different countries and using anonymous online identities. Despite these challenges, efforts to prevent

[1] Author is a student at B.S. Anangpuria Instititue of Law, Alampur, Faridabad, Haryana, India

 [ISSN 2581-5369]

and prosecute cybercrime are essential to protect individuals, businesses, and governments from the growing threat of online crime.

The history of cybercrime can be traced back to the early days of computing in the 1970s and 1980s when hackers started exploring the capabilities of computer systems. These early hackers were often motivated by curiosity or a desire to push the limits of technology, but some also engaged in illegal activities such as stealing data or disrupting computer systems. In the 1990s, as the internet became more widespread, cybercrime began to take on a more organized and malicious character. This period saw the rise of computer viruses, malware, and denial-of-service attacks. One notable example is the Morris worm, which in 1988 infected thousands of computers, causing significant disruption to the nascent internet.

The early 2000s saw a further increase in cybercrime, with the emergence of new threats such as phishing, identity theft, and ransom ware. Cybercriminals began to target individuals and businesses with greater frequency, seeking to exploit weaknesses in their computer systems and steal sensitive information or extort money. In recent years, cybercrime has continued to evolve, with criminals using increasingly sophisticated methods to carry out their activities. This includes the use of artificial intelligence, machine learning, and social engineering techniques to deceive individuals and evade detection. The fight against cybercrime has also evolved, with law enforcement agencies around the world working to track down and prosecute cybercriminals. Governments and businesses have also invested in cyber security measures to protect their computer systems and networks from attacks.

II. TYPES OF CYBER CRIME

There are various types of cybercrime that can be classified based on the nature of the offense.

- Hacking: Unauthorized access to computer systems or networks with the intention of stealing or manipulating data.
- Identity theft: Stealing someone's personal information, such as name, address, credit card details, or social security number, to commit fraud or other illegal activities.
- Phishing: Sending fraudulent emails or messages to trick individuals into sharing their personal information or installing malware on their devices.
- Malware: Installing malicious software, such as viruses, Trojans, and worms, on a computer system or network to damage or control it.
- Cyber stalking: Harassing or threatening someone through digital channels, such as social media, email, or messaging apps.

 [ISSN 2581-5369]

- Denial of Service (DoS) attacks: Overloading a website or network with traffic to disrupt its normal operation.
- Cyber bullying: Using digital channels to harass, intimidate, or humiliate someone.
- Cyber extortion: Threatening someone to leak or destroy their personal or confidential information in exchange for money.
- Child pornography: Creating, distributing, or possessing pornographic content involving children.
- Online scams: Using fake websites, ads, or messages to deceive individuals into paying money for fake products or services.

III. CAUSES OF CYBER CRIME

There are various causes of cybercrime, including:

- Ideology: Cybercrime can also be motivated by political or ideological beliefs. For example, activists may engage in illegal activities to protest against government policies or corporate practices.
- Complexity: Cybercrime is often complex and difficult to investigate due to the use of sophisticated technologies, encryption, and anonymity tools.
- Lack of awareness: Many individuals and businesses are not aware of the risks and vulnerabilities associated with cybercrime, making them easy targets for cybercriminals.
- Lack of resources: Law enforcement agencies often lack the resources and expertise to investigate and prosecute cybercrime cases.
- Rapidly evolving threats: Cybercrime is a constantly evolving threat, with criminals constantly developing new techniques and technologies to exploit vulnerabilities in computer systems and networks.
- Thrill-seeking: Some cybercriminals are motivated by the challenge of breaking into secure systems or the excitement of causing disruption or damage.
- Insider threats: Cybercrime can also be carried out by insiders, such as employees who have access to sensitive information or computer systems and use this access to carry out illegal activities.
- Profit: Cybercrime can be highly profitable, with cybercriminals targeting individuals and businesses to steal financial information or extort money through ransomware

 [ISSN 2581-5369]

attacks.

- Anonymity: The internet provides a level of anonymity that makes it easier for cybercriminals to carry out illegal activities without fear of being caught.
- Advancement in technology: As technology advances, new vulnerabilities and opportunities for cybercrime emerge, which cybercriminals can exploit for their own gain.
- Ideology: Some cybercriminals are motivated by political or ideological beliefs, using cyber-attacks to protest against government policies or corporate practices.
- Thrill-seeking: Some individuals engage in cybercrime as a form of thrill-seeking or to prove their skills to their peers.
- Revenge: Cybercrime can also be motivated by a desire for revenge against individuals or organizations perceived to have wronged the perpetrator.
- Insider threats: Cybercrime can be facilitated by insiders, such as employees or contractors, who have access to sensitive information or computer systems.

IV. CYBER LAWS

India has several laws and regulations to combat cybercrime and protect individuals and organizations against cyber threats. Some of the key cyber laws in India include:

- Information Technology Act, 2000: This act provides legal recognition for electronic transactions and outlines provisions for dealing with cybercrime, including unauthorized access, data theft, and computer-related offences.
- The Indian Penal Code: The Indian Penal Code has several provisions that can be used to prosecute cybercriminals, including those related to fraud, identity theft, and cyber stalking.
- The National Cyber Security Policy, 2013: This policy outlines a framework for managing cyber security in India and sets out guidelines for protecting critical infrastructure and responding to cyber-attacks.
- The Personal Data Protection Bill, 2019: This bill, which is currently pending approval, aims to regulate the use of personal data by businesses and government agencies and provide individuals with greater control over their data.
- The Cyber Appellate Tribunal: This tribunal was established under the Information

 [ISSN 2581-5369]

Technology Act, 2000 to hear appeals against orders issued by adjudicating officers in cases related to cybercrime.

- The Cyber Swachhta Kendra: This is a government-run initiative to provide cyber security tools and services to individuals and organizations in India.
- The Indian Evidence Act, 1872 is a law that regulates the admissibility of evidence in legal proceedings in India, including evidence related to cybercrime. Here are some key provisions of the Indian Evidence Act that are relevant to cybercrime cases in India:
    - Section 65B: This section provides guidelines for the admissibility of electronic records as evidence in court. It states that any electronic record that is produced as evidence in court must be accompanied by a certificate that verifies the authenticity of the record. The certificate must be signed by a person who is in charge of the computer that was used to create or store the record, or by any other person who has knowledge of the computer system.
    - Section 45A: This section deals with the opinion of experts in court. It states that when the court has to form an opinion on any matter related to cybercrime, it may obtain the opinion of experts in the field of science or art. The expert's opinion may be admissible as evidence in court.
    - Section 114A: This section deals with the presumption as to electronic records. It states that if an electronic record is produced in court, and the authenticity of the record is not disputed, the court may presume that the information contained in the record is accurate.

Penalties Cyber Crime

The Information Technology (IT) Act, 2000

The Information Technology (IT) Act, 2000 is legislation in India that deals specifically with cybercrime. It was introduced to provide legal recognition for electronic transactions and to facilitate e-commerce in India. The IT Act, 2000 also defines various types of cybercrime and provides for penalties for committing such offenses. Some of the key provisions of the IT Act, 2000 under cybercrime are:

- Section 43: This section deals with unauthorized access to computer systems or networks. It provides for penalties for accessing or attempting to access a computer system or network without authorization, including fines and imprisonment.

 [ISSN 2581-5369]

- Section 65: This section deals with tampering with computer source documents. It provides for penalties for intentionally or knowingly concealing, destroying, or altering computer source code, including fines and imprisonment.
- Section 66: This section deals with computer-related offenses, including hacking, cyber stalking, and transmission of obscene content. It provides for penalties for committing such offenses, including fines and imprisonment.
- Section 66A: This section deals with sending offensive messages through communication services. It provides for penalties for sending offensive or false messages through communication services, including fines and imprisonment.
- Section 66B: This section deals with dishonestly receiving stolen computer resources or communication devices. It provides for penalties for knowingly receiving stolen computer resources or communication devices, including fines and imprisonment.
- Section 66C: This section deals with identity theft. It provides for penalties for using someone else's identity to commit an offense, including fines and imprisonment.
- Section 66D: This section deals with cheating by personation using computer resources. It provides for penalties for cheating or attempting to cheat someone by pretending to be someone else through computer resources, including fines and imprisonment.
- Section 66E: This section deals with violation of privacy. It provides for penalties for capturing, publishing or transmitting images of private parts of a person without their consent, including fines and imprisonment.

The Information Technology (Amendment) Act, 2008

This amendment introduced several new provisions to the IT Act, including the criminalization of certain cyber offenses such as identity theft, cyber terrorism, and child pornography. It also increased the penalties for various cybercrimes and established the Cyber Appellate Tribunal to hear appeals against orders passed by the Adjudicating Officers.

The Information Technology (Amendment) Act, 2011

This amendment introduced several new provisions related to data protection and privacy. It requires companies to obtain consent from individuals before collecting and using their personal information, and also provides for the appointment of a Data Protection Officer.

The Indian Penal Code, 1860

The Indian Penal Code (IPC) has several provisions that can be used to prosecute cybercrime.

 [ISSN 2581-5369]

The penalties for cybercrime under the IPC are as follows:

- Section 66D: Punishment for cheating by personation by using computer resources: Imprisonment for a term which may extend to three years and a fine.
- Section 66E: Punishment for violation of privacy: Imprisonment for a term which may extend to three years and a fine.
- Section 66F: Punishment for cyber terrorism: Imprisonment for a term which may extend to life imprisonment.
- Section 419: Punishment for cheating by personation: Imprisonment for a term which may extend to three years and a fine.
- Section 420: Cheating and dishonestly inducing delivery of property: Imprisonment for a term which may extend to seven years and a fine.
- Section 463: Forgery: Imprisonment for a term which may extend to two years or fine, or both.
- Section 464: Making a false document: Imprisonment for a term which may extend to two years or fine, or both.
- Section 468: Forgery for purpose of cheating: Imprisonment for a term which may extend to seven years and a fine.
- Section 469: Forgery for purpose of harming reputation: Imprisonment for a term which may extend to three years and a fine.
- Section 471: Using a forged document as genuine: Imprisonment for a term which may extend to seven years and a fine.

V. CASES

There have been several high-profile cybercrime cases in India over the years, some of which have resulted in significant legal and judicial outcomes. Here are a few notable examples:

- Shifu Sunkriti case: In 2016, four members of a hacking group called "Shifu Sunkriti" were arrested for allegedly stealing confidential data from several Indian companies. The case is still on-going.
- Indu Khurana case: In 2016, a woman named Indu Khurana was arrested for running a phishing scam that defrauded people of several crores of rupees. She was sentenced to 20 years in prison in 2019.

 [ISSN 2581-5369]

- Airtel data breach case: In 2018, a former Airtel employee was arrested for allegedly stealing customer data and selling it to a third party. The case is still ongoing.
- Noida call center scam: In 2020, over 30 people were arrested in connection with a call center scam that involved defrauding people in the US and Canada. The case is still ongoing.
- State of Maharashtra v. Vijay Kumar Mishra (2017) SCC Online Bom 1348 - In this case, the accused was charged with sending obscene messages to a woman on Facebook. The Bombay High Court upheld his conviction under Section 354D of the Indian Penal Code and Section 67 of the Information Technology Act.
- Avnish Bajaj v. State (2005) 3 SCC 211 - This case involved the arrest of Avnish Bajaj, CEO of a web portal, in connection with allegedly objectionable content posted by a user on the portal. The Delhi High Court held that intermediaries like web portals could not be held liable for user-generated content and quashed the charges against Bajaj.
- Zahid Hussain v. State of Rajasthan (2015) SCC Online Raj 4865 - In this case, the accused had created a fake Facebook profile of a woman and posted her personal information online, causing her mental harassment. The Rajasthan High Court held him guilty under Sections 66C and 66D of the Information Technology Act.
- Reserve Bank of India v. Jayantilal N. Mistry (2018) SCC Online Bom 6447 - This case involved a phishing scam where the accused had created a fake email address to defraud a bank customer. The Bombay High Court upheld his conviction under Sections 419 and 420 of the Indian Penal Code and Section 66D of the Information Technology Act.
- Jitender Kumar v. State of NCT of Delhi (2013) SCC Online Del 3434 - In this case, the accused had hacked into the email account of his former employer and threatened to leak confidential information. The Delhi High Court upheld his conviction under Sections 66 and 66D of the Information Technology Act and Section 381 of the Indian Penal Code.

VI. PREVENTION OF CYBER CRIME

Preventing cybercrime in India requires a multi-pronged approach that involves government agencies, law enforcement, and individuals. Some of the measures that can be taken to prevent cybercrime in India include:

 [ISSN 2581-5369]

- Strengthening laws and regulations: Enacting and enforcing laws and regulations that is in line with international standards, to deter cybercrime and ensure that cybercriminals are held accountable for their actions.
- Investment in cyber security infrastructure: Investing in cyber security infrastructure and resources for law enforcement agencies to better detect and respond to cybercrime.
- Implementation of best practices: Encouraging the implementation of best practices in cyber security, such as regular updates of software and security systems, use of strong passwords, and regular backups of important data.
- Cyber insurance: Encouraging the use of cyber insurance to protect businesses and individuals from financial losses due to cybercrime.
- Reporting incidents: Encouraging individuals and businesses to report incidents of cybercrime to law enforcement agencies, to help them investigate and prosecute cybercriminals.
- Stronger Cyber Laws: Governments should enact and enforce strong cyber laws to deter cyber criminals and provide legal remedies for victims of cybercrime.
- Strengthened Cyber Security Measures: Individuals and organizations should take steps to strengthen their cyber security measures, such as using strong passwords, regularly updating software, and using anti-virus and anti-malware software.
- Incident Response Planning: Organizations should develop and implement incident response plans to respond quickly and effectively to cyber incidents.
- Cyber Security Training: Organizations should provide regular training to their employees on cyber security best practices and how to identify and respond to cyber threats.
- Technological Innovation: Advances in technology can be used to prevent and address cybercrime. Governments and the private sector should invest in technological innovation to develop new tools and techniques for combating cybercrime.

The government plays an important role in combating cybercrime. Here are some of the ways in which governments can address cybercrime:

- Enacting and enforcing strong cyber laws: Governments can enact and enforce strong cyber laws to deter cyber criminals and provide legal remedies for victims of cybercrime.

 [ISSN 2581-5369]

- Developing cyber security strategies and policies: Governments can develop and implement cyber security strategies and policies to protect their citizens and critical infrastructure from cyber threats.
- Establishing specialized agencies: Governments can establish specialized agencies to investigate and prosecute cybercrime. These agencies can also provide assistance to victims of cybercrime.
- Collaboration with other countries: Cybercrime is a global phenomenon that requires international cooperation and coordination. Governments can collaborate with other countries to share information and resources to combat cyber-crime.
- Awareness and education: Governments can raise awareness and educate the public about cyber security and cybercrime. This can include public awareness campaigns and providing training and resources to schools and businesses.
- Partnerships with the private sector: Governments can partner with the private sector to develop and implement effective cyber security solutions. This can include sharing information about threats and vulnerabilities, and collaborating on the development of new technologies and solutions.

VII. CONCLUSION

Cybercrime has become a significant threat to individuals, businesses, and governments around the world, including India. The rapid advancement of technology has made it easier for cybercriminals to carry out their illegal activities, ranging from identity theft and financial fraud to cyber espionage and terrorism. To combat cybercrime effectively, it is crucial for governments, law enforcement agencies, and individuals to take proactive measures to prevent cyber-attacks, such as increasing awareness, investing in cyber security infrastructure, and implementing best practices in cyber security. Strong cyber laws and regulations are also needed to deter cybercriminals and ensure that they are held accountable for their actions. While there have been notable cybercrime cases in India in recent years, more needs to be done to strengthen the country's cyber security capabilities and prevent cybercrime. With the increasing reliance on technology in all aspects of life, it is essential for everyone to take responsibility for their cyber security and stay vigilant against cyber threats.

*****

 [ISSN 2581-5369]

VIII. REFERENCES

- S. Prakash, *Cyber Crime and Digital Evidence: Materials and Cases* (Universal Law Publishing, 2021).
- Pavan Duggal, *Cyber Crime and Cyber Law in India* (Pavan Duggal, LexisNexis, 2018).
- Thomas J. Holt and Adam M. Bossler, *Cyber Crime and Digital Forensics: An Introduction* (Routledge, 2018).
- Dr. Karnika Seth, *Cyber Law in India* (Bloomsbury India, 2018).
- K.V. Chalam, "Cybercrime and Its Impact on India's Economy" *Journal of Internet Banking and Commerce*, Volume 20, Issue 3, 2015.
- Ravi Shankar and A. Srinivasan, "Challenges and Solutions for Combating Cybercrime in India," *International Journal of Applied Engineering Research*, Volume 10, Issue 55, 2015.
- N. Jayaprakash, "Cyber Crime and the Challenges for Criminal Justice in India," *Indian Journal of Criminology and Criminalistics*, Volume 35, Issue 1, 2014.
- Jyoti Rana and Kirti Gupta, "Cybercrime in India: Trends and Challenges," *International Journal of Scientific and Engineering Research*, Volume 7, Issue 3, 2016.
- A Prabhat Pandey and Akshay Tyagi, "Study of Cybercrime and Its Impact on Indian Society," *International Journal of Advanced Research in Computer Science*, Volume 8, Issue 6, 2017.
- R. Vijayakumar and D. Mohanasundaram, "Cyber Crime and Cyber Security: Challenges and Solutions," *International Journal of Engineering and Technology*, Volume 8, Issue 5, 2016.
- Anshika Srivastava and R.S. Kushwaha, "Emerging Trends and Challenges in Cybercrime in India," *International Journal of Management, Technology and Engineering*, Volume 7, Issue 1, 2017.
- A. Jyoti and G.K. Singh, "Cybercrime in India: A Review of the Current Scenario" *International Journal of Engineering Science and Computing*, Volume 7, Issue 9, 2017.

*****

 [ISSN 2581-5369]