Research Vidyapith International Multidisciplinary Journal

(International Open Access, Peer-reviewed & Refereed Journal)

(Multidisciplinary, Monthly, Multilanguage)

*** Vol-2* *Issue-11* *November 2025***

www.researchvidyapith.com **ISSN (Online): 3048-7331**

Cyber Crime: A Challenge of Digital Age

Dr. Parul Malik

Assistant Professor, B.Ed. Department, S.M.P. GOVT. Girls PG College, Madhavpuram, Meerut

Abstract:

Majority of people depend on internet for online money debit and credit, communications, entertainment and for knowledge & information. As science and technology has progressed, our reliance upon it and on internet has grown at rapid rate and cybercrimes are also increasing at the same pace. Cyber-crime is committed using computer, technology and network. It is criminal and illegal act where computer and digital devices along with network is used. In cyber-crime, harmful activities are committed through the use of electronic devices, technology and internet. Cyber-crime is the recent fastest growing issue and the fastest growing area of crime, still not fully understood by the law enforcement agencies. It involves illegal or unlawful and undistinguished activities that exploit technology to commit different and various forms of crimes and can affect person, Institution, Company and even governments.

Cyber-crime is a major challenge of the current digital age and an increased reliance on technology for daily life creates vulnerabilities or risks that criminals exploit and damage through malware, phishing and identity theft, causing physical, mental, social, financial, emotional and reputational damage. Cybercrime includes a wide range of illegal work that damages and harm data and information contained in computer system's files and folders. Cybercrime profoundly impacts individuals and society causing financial losses, reputational damage and operational disruption. Cybercrimes have devastating effects like breaches of sensitive and confidential data, financial losses, failure of systems, and also, it can affect an organization's or an individual's reputation.

So, it is our responsibility to be updated of recently prevailing cyber-fraud in our society and nation. Earlier, Cyber-crime was committed by many small group or individuals, but now it is committed by Professional hackers, young technically advanced children, spammers, etc. Practicing good cybersecurity habits, such as regular software updates, creating strong passwords and phishing awareness training and camp, can reduce cybercrime vulnerability.

Cybercrime is dynamic in character because of progress in digital technology field. India can build a safer digital environment for its citizens through a combination of public awareness, robust legislation and technological advancements.

Keywords: Cyber-crime, Internet, IT Act, Bharatiya Nyaya Sanhita, Dynamic, Digital Environment.

Introduction

Cybercrime can be defined as a major crime where any communication device is

used illegally to commit or facilitate in committing any illegal or unlawful act. Computer is the main instrument of the crime or is used as a tool to commit an offence. Cybercrimes comes under State subjects as per the Seventh Schedule of Indian Constitution. It involves illegal or unlawful and undistinguished activities that exploit technology to commit different and various forms of crimes and can affect person, Institution, Company and even government

Our government plays an important role to strengthen the mechanism for tackling with Cybercrimes in a coordinated and comprehensive way.

With the benefits of technology, man has become completely dependent on internet to fulfil all his desires, demand and requirements. Internet has become an essential part of daily life and helps an individual to access anything while sitting at one place. Internet and computer devices are involved in all domains whether it is business, online shopping, sports, banking, education, entertainment, research, military services, logistics and many more. The development of ICT (Information and Communication technology) has made our daily life simple, relax able, easy and flexible. The advancement of information and technology has introduced a new form of sophisticated crime i.e. cyber-crime. Information technology and computers can be used both for Profitable and corrosive purposes that can have either positive or negative influence on the lives of human beings. The positive side of information and communication technology is that they can be utilized as a communication medium, for data sharing and receiving, for transactions, education and commercial operations. While the negative effects of information technology and internet are addiction, cyber bullying and privacy violations, cyber-theft, proliferation of fake news, revenge porn, etc. Information and facts flowing over a computer network is susceptible to being intercepted, altered or stolen. The stolen information and facts are subsequently utilized for personal advantage, can even be used for illegal activities such as pornographic media, fraud, gambling, and theft of money. Cybercrime profoundly impacts individuals and society causing financial losses, reputational damage and operational disruption. Examples of Cyber-crime against individuals are: Cyber-stalking, Cyber Bullying, Identity-Theft. Cyber Crimes Against Property are: Cybersquatting, Phishing, Intellectual Property Infringement. Cyber Crimes Against Organizations are DDoS' (Distributed-Denial-of- Service) Attack, Cyber espionage. Cyber Crimes Against Society are: Cyberterrorism, Child Pornography and Cyber Warfare. Cybercrime has negative impacts on individuals and society causing financial losses, reputational damage, depression and operational disruption. Cybercrimes have devastating effects like breaches of sensitive and confidential data, financial losses, failure of systems, and also, it can affect an organization's or an individual's reputation. Thus, it is the duty of law enforcement agencies and government to build a safer digital environment and platform for its citizens through a combination of public awareness, camp to aware digital fraud, robust legislation and technological advancements.

Categories of Cybercrime:

1. **Cyber Crimes Against Individuals:** These crimes attack particular individuals, often for gathering personal information or to cause harm and harassment. This includes identity theft, cyberstalking, online fraud, online harassment and cyberbullying.

A. **Cyber-stalking:** It is the illegal and harmful act by using internet or digital platform or space to harass, threaten, or stalk someone. Its main aim is to intimidate the victim by hacking their accounts, spreading lies online and repeatedly sending unwanted weird messages.

B. **Cyber Bullying:** It is the intentional bullying or harassment that takes place

over digital devices or platform like mobiles and laptops. It includes posting embarrassing photos or videos, sending or sharing false, negative and harmful content about someone else anonymously.

C. **Identity-Theft-** Internet and technology is used to commit crime and fraud by gathering confidential information about someone without the consent of that person and using that information for committing fraud related to identity and financial benefit. This type of crime harm individual socially, economically, personally and emotionally. So never share your personal and family details and bank account details to anyone on phone and social sites because this can be used to commit cyber-crime or cyber-fraud.

2. **Cyber Crimes Against Property:** In this cybercrime computers and internet are used illegally to steal, damage and interfere someone digital assets like data, intellectual property and financial information. It includes cybersquatting, cyber vandalism, hacking, malware attacks, ransomware, software Piracy, intellectual property infringement and Phishing and Pharming.

A. **Cybersquatting-** Also known as domain squatting. It is a cybercrime or digital crime in which the criminal purchases or registers a domain name that is similar in appearance to an already existing domain name with the aim or intent of making money or profit from the goodwill of a trademark belonging to someone else.

B. **Phishing-** It is cyber-attack where criminal minded person pretend to be legitimate companies and create link that appears to be from authentic sources or entities to put psychological pressure on individuals to click the link without thinking that results into revealing personal and confidential information like user Id and passwords, credit and debit card details, bank details, OTP, etc. The stolen information is used for identity theft or financial gain thus harming person psychologically.

C. **Intellectual Property Infringement-** It is unauthorized use, copying or distribution of someone else's intellectual property without their permission. It can result into legal action, reputational damage and financial penalties.

D. **Ransomware-** This word is made up of the combination of Ransom and Malware. This Cyber-attack destroys files and folders on computer system or Laptop devices. Criminals or hackers first hack or lock the system or file and after hacking and locking, they demand money from system owner in exchange for a key to unlock the encrypted data.

3. **Cyber Crimes Against Organizations:** These attacks target businesses and government entities often for aim of theft, financial gain or disruption. Examples are DDoS (Distributed Denial of Service), Cyber Espionage and Data Breaches.

A. **'DDoS' (Distributed-Denial-of- Service) Attack-** It is a cyber-crime in which digital attackers attack the website making it slow and unresponsive for customers and users to use. It digitally crowds the targeted website with fake users and fake requests. It affects the normal functioning of websites and sometimes the crash of websites occurs thus affecting individuals and organisations financially, reputationally and socially.

B. **Cyber espionage:** Cyber espionage or cyber spying is the unauthorized infiltration of computer systems, networks, or devices to steal confidential information for political, financial advantage or competitive advantage.

4. **Cyber Crimes Against Society:** These are illegal and unlawful acts harming the community and society. It includes cyber terrorism targeting crucial and critical infrastructure, spread of misinformation to misguide and manipulate

public opinion, Cyber Warfare, online gambling, forgery, sale of illegal articles ,web jacking and child pornography.

A. **Cyberterrorism-** It is the use of computer system and telecommunication devices to commit acts of destruction, violence or disruption against non- combatant targets to create panic and fear and achieve political or ideological goals. Its aim is to cause real-world harm and influence governments or populations, with consequences that can include physical harm, the disruption of essential public services, or financial loss.

B. **Child Pornography-** If any person possesses, create, transfer or store any sexually explicit photos, videos involving children below 18 years of age then it is considered as heinous digital or cyber-crime. These things create depression, anger, isolation and mental disorder in child. This crime leads to rigorous imprisonment and imposes high fine.

C. **Cyber Warfare-** It is a computer or network based cyber-attack involving politically motivated or state-sponsored attacks by a nation or country on another country. It includes the disruption of activities of organizations or nation-state, especially for strategic or military goal-oriented and is acting as a modern form of conflict beyond traditional battlefields.

Suggestions to prevent to be a victim of cyber-crime:

1. Always form complex and difficult password on social site, bank account and in registration process.
2. Antivirus that is updated and real must be installed in laptops and mobile.
3. Activate two-factor authentication for an extra layer of security.
4. Keep devices and system software updated to prevent from being attacked and hacked by cyber-criminals.
5. Avoid using public Wi-Fi and use safe and secure network for financial transactions.
6. Never open attachments in spam emails from an unknown sender.
7. Always double-check or recheck the spelling of URL, HTTP, website.
8. Never ever share personal details like name, account number, Aadhaar number, OTP, date of birth and CVV number on phone calls or text messages.
9. Always remember to log out from public computer system and change the password at a regular routine.
10. Keep yourself updated with the recent news of cyber crime and follow measures to prevent you and your family from becoming a victim of cyber-crime.

Conclusion-

The development of science and technology has been a significant step in improving lives, but it has provided a new platform for criminals to commit digital illegal act anonymously, especially through the Internet and Computers. With the benefits of technology, man has become completely dependent on internet to fulfil all his desires, demand and requirements. Internet has become an essential part of daily life and helps an individual to access anything while sitting at one place. Internet and computer devices are involved in all domains whether it is business, online shopping, sports, banking, education, entertainment, research, military services, logistics and many more. The development of ICT (Information and Communication technology) has made our daily life simple, relax able, easy and flexible. In order to combat cybercrimes effectively and efficiently, it is pivotal for government, international organizations, agencies and countries to update the existing laws regularly. Different kinds of cyber-

crimes effects negatively the life of persons everyday but nobody aware of various types of crimes. Most of the people know only about common crime like hacking and virus/worms but they are unaware of many other crime defamation, cyber Espionage, Data Breaches etc. It is the demand of the time to have complete Sense and information about these types of crimes which are co-related with the Computer and internet. Individuals can report complaints related to cyber offenses through the official online portal at cybercrime.gov.in. The "Information Technology Act, 2000" (IT Act) criminalises and punishes activities like hacking, phishing, data theft, and unauthorised access. Additionally, laws under the Bharatiya Nyaya Sanhita,2023 (BNS) address crimes like forgery, fraud and extortion, covering aspects of cybercrime. Crime-oriented behaviour or mindset on the Internet and cyber-space has become a great and current challenge for Indian Government and Abroad law enforcement organisations and agencies. Information and communication technology (ICT) has become more prevalent and pervasive, the aspects of electronic, digital and technical crime will feature in all forms of criminal behaviour and activities comprise of people smuggling, drug trafficking, money laundering, and cyber -terrorism. Law enforcement agencies are tirelessly working day and night to develop new techniques, partnerships, new forensic tactics and methodologies to deal and fight with online network crime efficiently and effectively in order to ensure safety, security and privacy on the digital and network platform. Current investigative tactics and technologies and updated modern skills, to find out, stop, respond and react quickly and immediately to crime related to technology will be required. It is not the duty of government but also a righteousness of a person catches and identifies the criminals. Victim of any of cyber-crimes should come forward and file a complaint against cyber criminals. It will be helpful to resolve the problems and fight against these types of crimes. Practicing good cybersecurity habits, such as regular software updates, creating strong passwords and phishing awareness training and camp, can reduce cybercrime vulnerability.

Author's Declaration:

I/We, the author(s)/co-author(s), declare that the entire content, views, analysis, and conclusions of this article are solely my/our own. I/We take full responsibility, individually and collectively, for any errors, omissions, ethical misconduct, copyright violations, plagiarism, defamation, misrepresentation, or any legal consequences arising now or in the future. The publisher, editors, and reviewers shall not be held responsible or liable in any way for any legal, ethical, financial, or reputational claims related to this article. All responsibility rests solely with the author(s)/co-author(s), jointly and severally. I/We further affirm that there is no conflict of interest financial, personal, academic, or professional regarding the subject, findings, or publication of this article.

Reference:

1. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 5, Issue 8
2. Mehta, Saroj and Singh, Vikram (2013), A Study of Awareness about Cyber laws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1.
3. Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.
4. Akdeniz, Y., &. Walker C. (2018). Cybercrime: Key Issues and Debates. Routledge
5. Wall, D. S. (2018). Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime. Information & Communications Technology Law, 27(2), 195-210.
6. Harsh, K., Singh, T., & Singh, P. K. (2015). Emerging threats of cybercrimes. 1(1), 21–24.
7. Seamus O Clardhuanin (2004), An extended model of Cybercrime investigations, International journal of digital evidence, Summer 2004, Vol 3, Issue 1
8. Paul, P. K., & Aithal, P. S. (2018). Cyber-Crime: Challenges, Issues, Recommendation and

Suggestion in Indian Context. 3(1), 59–61.
9. Richard Raysman& Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L. J.
10. Eric J. Sinrod and William P Reilly, Cyber-Crimes (2000), A practical approach to the application of federal computer crime laws, Santa Clara University, Vol 16, Number 2.

Cite this Article

'Dr. Parul Malik', "Cyber Crime: A Challenge of Digital Age", Research Vidyapith International Multidisciplinary Journal, ISSN: 3048-7331 (Online), Volume:2, Issue:11, November 2025.

Journal URL- https://www.researchvidyapith.com/

DOI- 10.70650/rvimj.2025v2i11006

Published Date- 04 November 2025