Cyber Crime Causes and prevention: An Analysis

Dr. Jaya Sharma[1]

[1]*Head, Deptt. of Computer Science College of Professional Studies, Ambikapur, Surguja, Chhattisgarh*

OPEN ACCESS

Volume: 4

Issue: 3

Month: July

Year: 2025

ISSN: 2583-7117

Published: 11.07.2025

Citation:

Dr. Jaya Sharma “Cyber Crime Causes and prevention: An Analysis” International Journal of Innovations in Science Engineering and Management, vol. 4, no. 3, 2025, pp. 66–72.

DOI:

10.69968/ijisem.2025v4i366-72

Abstract

Cybercrime is the term used to describe criminal actions that either target computers or networks, such hacking, phishing, and spamming, or utilize computers to carry out offensive and unlawful acts, including child pornography and hate crimes. This article reviews the many viewpoints found in the literature about the causes and ways to avoid cybercrime. This review highlights that cybercrime is increasing rapidly due to widespread internet usage, weak cybersecurity infrastructure, and lack of awareness. Common causes include poor security practices, untrusted websites, and sophisticated hacking methods. Key preventive measures include using antivirus software, encrypted channels, strong passwords, disabling unused devices, and avoiding sharing sensitive data. The study emphasizes the need for strong cybersecurity frameworks, regular audits, and training to bridge the skills gap. Despite legal measures in place, enforcement remains challenging. The review concludes that a collaborative approach involving government, industry, and education is vital to prevent cyber threats and ensure digital safety.

Keywords; Cybercrime, Causes, Prevention, Hacking, Phishing, Spamming, Cyberattack, Artificial Intelligence, Machine Learnings, Cybersecurity, Ransomware Attack.

INTRODUCTION

The frequency of technological advancements is increasing the prevalence of cybercrime; however, the development of countermeasures and prevention strategies to protect both the technology and its consumers is not progressing at the same pace [1]. India has the potential to emerge as one of the world's most significant digital centers. A digital economy and more connectivity offer significant gains, but they also present new risks to our digital society. Cybercrime has emerged as an increasingly grave concern in the digital era, as cyberattacks and data intrusions have experienced a substantial rise in India [2]. Networking and cyberspace have been immensely beneficial to humanity; however, there are individuals who exploit this advancement to obtain illicit benefits. Transnational in nature, cybercrimes have evolved at a pace that is similar to that of emerging technology [3], [4]. Advanced techniques like artificial intelligence (AI) and machine learning (ML) are being used by scammers and cybercriminals to develop malware that circumvents conventional security barriers. Since they are exceedingly difficult to locate, they capitalize on this circumstance. Two potential reasons of cyberattacks are the use of new technology by cybercriminals or a country's inadequate cyber security measures [5].

Cyber Crime

Cybercrime is a broad phrase that refers to a variety of illegal behaviors that are conducted employing a computer, network, or other collection of digital devices. Think of cybercrime as the catch-all term for cybercriminals' wide range of illicit actions. These include, among many other things, ransomware, malware assaults, phishing, identity theft, and hacking [6]. Cybercrime's reach transcends geographical limits. Technical infrastructure, victims, and criminals are global in scope.

Cybercrime takes numerous forms and is always changing as a result of the use of technology to take advantage of security flaws on both a personal and business level. In turn, there are several dynamic problems in the continuous battle to successfully investigate, punish, and prevent cybercrimes [7], [8] Cybercrime is a severe threat to government entities, enterprises, and individuals, and it can lead to severe financial losses, compromised documents, and a damaged reputation. It is now more important than ever to take precautions against cybercrime because of the growing danger posed by this phenomenon as technology develops and more people depend on digital devices and networks for everyday tasks [9].

Causes of cybercrime

Cybercrime targets wealthy individuals or wealthy institutions, such as financial corporations, casinos, and banks, where hackers may readily get sensitive data and a substantial quantity of money is transferred every day [10], [11]. It is a simple approach to earn a lot of money. It is difficult to apprehend these crooks. Every day, more and more cybercrimes are committed worldwide. It is necessary to implement a number of laws to protect computer usage from different threats [12]. The several causes of computer vulnerability are outlined below:

- **Capacity to store data in comparatively small space:** The ability of a computer to store data in a relatively little amount of space is one of its special features. Furthermore, this facilitates the theft of our data from the system by criminals, who then exploit it for their own gain.
- **Negligence:** This is a feature of human behavior. Any carelessness on our part when safeguarding the computer system might allow criminals to easily get access to and control of it.
- **Easy to access:** Preventing unauthorized access to a computer system is a challenging task due to the intricate technology employed. Information that can easily trick biometric systems and get past firewalls is stolen by hackers and utilized to go past a lot of security measures.
- **Loss of evidence:** It is easy to erase the data associated with the crime. Therefore, losing evidence is a regular problem while looking into a cybercrime.

Types of Cybercrime

Let's talk about a few typical cybercrimes.

- **Phishing and Scam:** A sort of social engineering assault known as phishing aims to deceive users by sending phony emails and messages to get private information about them or by attempting to download malicious software and utilize it on the target device [13].
- **Identity Theft:** The act of identity theft is the unauthorized use of personal information, such as credit card numbers or confidential photographs, by a cybercriminal to perpetrate a crime or commit deception [14].
- **Ransomware Attack:** One of the most prevalent forms of cybercrime is ransomware assaults. By encrypting users' personal information and then requesting a ransom to unlock it, this particular sort of malware may stop users from accessing any of their data on the machine [15].
- **Hacking/Misusing Computer Networks:** This term denotes the criminal act of illicit access to private computers or networks, which can be exploited through the tampering with the data stored, the shutdown of the system, or other unlawful methods [16].
- **Internet Fraud:** The word "internet fraud" may be used to refer to any sort of cybercrime that involves the use of the internet, including theft of service, financial fraud, spam, and other crimes [17].

Cyber Crime Prevention

Prevention methods and technologies must be regularly implemented, monitored, and upgraded as the total cost and hazards of cybercrimes continue to rise. Cyber-attacks are becoming increasingly sophisticated and intelligent, between foreign adversaries, militants, and commonplace fraudsters [18]. Proactive steps must be taken by people, organizations, and governmental bodies to stop cybercrime from breaching security systems and stealing private information. A new generation of contemporary technology has emerged to complement these efforts, even if certain cybercrime prevention tactics are still effective in deterring attackers [19].

- **Advanced Cybersecurity Systems:** Using modern cybersecurity protection is one of the most important ways to avoid cybercrime. This covers basic technologies like intrusion detection systems, firewalls, and antivirus software, but more sophisticated cybersecurity systems are developing using machine learning (ML) and artificial intelligence (AI). For any company or person looking to defend themselves against cyberattacks and digital threats, putting the appropriate cybersecurity technologies into place should be their first concern [20].

- **Multifactor Authentication:** Two-factor authentication, often known as multifactor authentication (MFA), is a popular security measure that guards against direct cyberattacks, hacks, and data breaches. This procedure, to put it simply, requires users to authenticate access to their accounts using two or more means of identity, such as a password and an access code that is delivered to a machine. By adding additional levels of protection to online accounts, MFA has become a best practice technique for enterprises, making it more harder for hackers to access your data [21].
- **Virtual Private Networks:** User security and anonymity are enhanced by "a Virtual Private Network (VPN) service", which allows users to browse the Internet. VPNs are designed to encrypt your internet activities, making it more harder for hackers to intercept and steal your information. By adding their own encryption layer and using their own servers to route traffic, VPNs operate as a middleman between your device and the intended server. VPNs are particularly good at protecting you against phishing scams and other email frauds by hiding your location and IP address [22].
- **Email Security Solutions:** One of the most common ways that cybercriminals get access to private information and sensitive data is via email accounts. This practice may be stopped by using specialized email security technology, such as spam filters, antivirus software, and email encryption. Email information is shielded from interception by encryption, a powerful technology. harmful attachments in emails are identified and eliminated by antivirus software, while spam filters identify and stop unsolicited and harmful emails from getting to your inbox [23].
- **Password Managers:** Password credentials are frequently targeted by cybercriminals. Software programs known as password managers not only generate strong, hard-to-crack passwords but also safely store many login credentials in an encrypted database that is secured by a master password. Password managers are often used by individuals, remote teams, and companies to securely store passwords in a secure location and provide additional safety during Web browsing. Apple's iCloud Keychain, KeePass, LastPass, and Password are the most widely used password managers. But there are hazards associated with some password managers.
- **Security Awareness Training:** Many cyberattacks are the consequence of human mistake, such as downloading files that contain viruses or clicking on harmful links. Training in security awareness is meant to assist people learn how to recognize, prevent, and lessen the risk of cyberattacks. Phishing simulation exercises, in which staff members receive fictitious phishing emails to gauge their response, and computer-based awareness training are the most popular types of training. By helping businesses develop a security-conscious culture, security awareness training makes their networks more immune to cyberattacks [24].
- **Data Backup and Recovery:** Numerous cyberattacks have the potential to cause significant data loss, which may have detrimental effects on an organization's or individual's operations and finances. Backup and recovery solutions can assist in the mitigation of data loss by generating backup copies of data and guaranteeing a quicker recovery in the event of a ransomware attack, data intrusion, or other cyber-attack. To guarantee that you can retrieve your data in the case of an attack, regular data archiving is a crucial security measure [25].
- **AI and ML Cyber Crime Protection:** Artificial intelligence and machine learning are being used by more sophisticated cybercrime prevention systems to collect and analyze data, monitor and trace threats, identify vulnerabilities, and react to breaches. For instance, by seeing patterns that point to fraudulent conduct and marking them for further examination, machine learning algorithms may identify and stop fraud in financial transactions. Similarly, via network traffic analysis, anomaly detection, and real-time threat response, AI technologies may discover and stop cyberattacks on networks and systems [26].

LITERATURE REVIEW

(Kumar, 2025) [15] The researchers aimed to ascertain the extent to which educators were knowledgeable about cybercrime, its consequences, and their potential role in its prevention. The findings of a literature review and questionnaires of sixty educators indicate that while most educators are aware of cybercrime, their understanding varies widely, particularly when it comes to specific threats. Privacy concerns, inappropriate use of public Wi-Fi, and ignorance of policies and safety measures are typical challenges. The study's findings emphasize the significance of increasing awareness of cybercrime, particularly among educators, in order to provide safer online experiences for both them and their pupils. Teacher preparation programs should include thorough cyber security training to bridge the knowledge gap, protect personal information, and prepare educators to promote responsible online behavior.

(Kirti & Singh, 2023) [27] In addition to Indian cybercrime data, the study intends to investigate the changing nature of cybercrime in India and the reasons behind it, such as extortion, fraud, sexual exploitation, terrorist operations, inciting hatred against the nation, the sale of illicit medicines, etc. To provide a bibliographic overview of the changing landscape of cybercrime in India, this study will use a review-style research approach and includes both quantitative and qualitative data analysis methodologies. Utilizing statistical methods to condense and meaningfully display the data will be part of the data analysis process. This investigation's conclusions will prove advantageous to stakeholders, including policymakers and law enforcement agencies, in their endeavors to combat cybercrime in India. Several research related to digital forensic investigations will use this article as their data set.

(Thomas, 2023) [28]Generally speaking, the purpose of this study is to analyze different cybercrimes and the accompanying preventative measures. Crimes committed online or via computer systems are referred to as cybercrimes. Since cybercrimes are seen as a serious danger to national security, personal data and information, and individual security in the modern world, individuals must take some fundamental precautions and be aware of the risks in order to protect themselves from these crimes. Financial losses, compromises of sensitive data, system failures, and the potential impact on an organization's reputation are all detrimental consequences of cybercrimes, which are regarded as a significant risk. More information on cybercrimes and their causes will be included in this essay. Additionally, learn about the many forms of cybercrimes, who are cybercriminals, and how to avoid them.

(Batra et al., 2020) 0 No matter one's location, the world is deeply reliant on technology in the contemporary era. These criminals have exploited our dependence on technology to their advantage. One of the current crimes with the quickest rate of growth is cybercrime. Cybercrime is notorious for bringing down several businesses, organizations, and individual identities. The definition of cybercrime, the many kinds of cybercriminals, how cybercrime impacts the world, and how to avoid it are the primary goals of this study. In addition, this paper will examine statistical data regarding the expansion of cybercrime over the past few years and the diverse varieties of cybercrime.

(Khadas, 2020) [30] Computers are employed as criminal tools, and cybercrime incorporates both computers and networks. An crime may also be committed using the computer as a tool. The criminal may also target the computer. For whom is the internet a great location to participate in a wide range of activities? Many of us may be susceptible to the criminals who access the internet through hacking. This essay focuses on the general overview of cybercrime, its primary causes, its many forms, and ways to avoid it.

(Shah, 2019) [31] Internet access is required to participate in India's transition to a digital age. This essay focuses on examining the patterns in internet use increase and the dangers that Indian consumers confront. It also looks at the patterns of cybercrimes that were reported in India in 2012–16 under "the Indian Penal Code (IPC)" and the IT Act 2000. It aims to examine both emerging and persistent forms of cybercrimes that happened in 2012–16 under the IPC and the IT Act 2000, respectively. In addition, this article attempts to examine the new forms of crime that emerged in 2017 as well as the steps the Indian government took to prevent them. It also recommends the best ways to stay out of trouble.

(Sinha & Kumar, 2018) [32] We think that this work is the first to systematically examine cybercrime prevention strategies. Governments are seeking to determine the appropriate size of the investment and the allocation of funds to information security as they compete to invest in this area. With cars, appliances, and other gadgets connected to the Internet, the virtual and real worlds may become more intertwined, which might make cyberterrorism more alluring. Even while there is still a significant risk of politically motivated harmful conduct occurring globally, companies deal with a daily flurry of assaults that come in many forms. Financial services are one area with significant concentration and, therefore, a valuable target for hackers. People also have to avoid typical attacks like phishing emails on a sometimes daily basis, thus everyone has to be at least somewhat knowledgeable about cybersecurity to keep secure.

RESEARCH GAP

Despite the growing body of literature on cybercrime, significant research gaps remain in understanding its evolving nature and the effectiveness of current preventive strategies. Most existing studies focus on technical aspects, while socio-psychological factors driving cybercriminal behavior are underexplored. Additionally, there is limited empirical data on the implementation and success of cybersecurity policies in developing countries like India. The rapid advancement of technologies such as AI and IoT has outpaced regulatory frameworks, creating new vulnerabilities. This review identifies the need for interdisciplinary research, region-specific studies, and updated preventive models to address the dynamic and complex landscape of modern cyber threats.

RESEARCH OBJECTIVE

- In this article review the various literature's perspective on causes and prevention of cybercrime.
- Study the causes of cybercrime, method to prevent cybercrime, and type of cybercrime.

RESEARCH METHODOLOGY

This review paper adopts a qualitative research methodology, utilizing secondary data to investigate the causes and prevention of cybercrime. The study is grounded in an extensive and systematic literature review, drawing insights from peer-reviewed academic journals, scholarly articles, technical reports, government publications, and relevant case studies published between 2014 and 2025. The collected literature was critically analyzed to identify recurring patterns, emerging trends, and gaps in current preventive strategies. This approach enables a comprehensive understanding of the multifaceted nature of cybercrime and provides a foundation for evaluating existing cybersecurity measures and recommending effective prevention strategies for diverse digital environments.

CONCLUSION

This review paper on "Cyber Crime Causes and Prevention: An Analysis" highlights that cybercrime is a growing threat due to increasing digital dependency and technological advancement. Key findings reveal that poor cybersecurity awareness, outdated systems, and lack of encryption expose individuals and organizations to risks like data theft, phishing, and online fraud. The paper emphasizes preventive measures such as using secure, encrypted communication channels, regularly updated antivirus software, disabling unused hardware (camera, microphone, GPS), and refraining from sharing sensitive banking details. Shopping only on secure, SSL-certified websites and clearing session data also helps reduce vulnerabilities. Organizational recommendations include deploying firewalls, encryption, intrusion detection systems, and conducting regular security audits. A crucial concern is the shortage of skilled cybersecurity professionals, which can be addressed through collaborations between academia, industry, and government to offer specialized training and certifications. Cybercrime's psychological and financial impact is significant, and its integration into traditional crimes like terrorism and drug trafficking is alarming. Law enforcement agencies worldwide are adopting technologies like data mining, machine learning, and bioprinting to combat such threats. India, with one of the largest online populations, faces higher cyberattack risks due to inadequate cybersecurity infrastructure, particularly in small firms. Strengthening legal enforcement and enhancing public awareness are critical to reducing cybercrime prevalence.

REFERENCES

[1] B. Dupont, F. Fortin, and R. Leukfeldt, "Broadening our understanding of cybercrime and its evolution," *J. Crime Justice*, vol. 47, no. 4, 2024, doi: 10.1080/0735648X.2024.2323872.

[2] J. Curtis and G. Oxburgh, "Understanding cybercrime in 'real world' policing and law enforcement," *Police J. Theory, Pract. Princ.*, vol. 96, no. 4, pp. 573–592, 2023, doi: 10.1177/0032258X221107584.

[3] P. U. Chinedu, W. Nwankwo, F. U. Masajuwa, and S. Imoisi, "Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models," *Rev. Int. Geogr. Educ.*, vol. 11, no. 7, pp. 956–974, 2021, doi: 10.48047/rigeo.11.07.92.

[4] M. Anant, K. Kanwar, and S. KumarIndulkar, "An Empirical Study On Awareness Of Cyber Security In Digital Banking Among College Going Students (With Special Reference To Korba District Of Chhattisgarh)," *Int. J. Innov. Sci. Eng. Manag.*, vol. 3, no. Specail, pp. 45–49, 2024.

[5] N. K and C. V K, "A Study On Cybercrime Its Impact And Awareness Towards Society," *Int. J. Creat. Res. Thoughts*, vol. 12, no. 4, pp. 23–31, 2024.

[6] R.Shital and K.Swapna, "CYBER-CRIMES IN INDIA: A CRITICAL REVIEW," *J. Emerg. Technol. Innov. Res.*, vol. 12, no. 4, pp. 579–585, 2025.

[7] V. Krishna Viraja and P. Purandare, "A Qualitative Research on the Impact and Challenges of Cybercrimes," *J. Phys. Conf. Ser.*, vol. 1964, 2021, doi: 10.1088/1742-6596/1964/4/042004.

[8] M. P. Gupta and P. (Dr. . L. Singh, "The Rising Threat of Recruitment Frauds – Analysing the Role of HRM Practices in Mitigating Cybercrime in India," *Int. J. Innov. Sci. Eng. Manag.*, vol. 4, no. 1, 2025, doi: 10.69968/ijisem.2025v4si194-102.

[9] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," *J. Crime Justice*, vol. 42, no. 5, pp. 495–499, 2019, doi: 10.1080/0735648X.2019.1692426.

[10] M. Vajagathali, N. K. S, and B. N. B, "Cyber Crime Awareness among College Students in Mangalore," *J. Forensic Sci. Crim. Investig.*, vol. 12, no. 1, pp. 1–6, 2019, doi: 10.19080/JFSCI.2019.12.555828.

[11] G. Das, Y. A. Ali, M. B. Singh, and M. K. Nag, "Digital Forensics in E-Commerce: Investigating Online Payment Fraud and Data Breaches," *Int. J. Innov. Sci. Eng. Manag.*, vol. 4, no. 1, 2025, doi: 10.69968/ijisem.2025v4i1262-268.

[12] S. Sulaiman and B. Sreeya, "Public awareness on cyber crime with special reference to Chennai," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 1, pp. 3362–3364, 2019, doi: 10.35940/ijitee.A9187.119119.

[13] M. Kaur, G. Kaur, and E. R. C.K., "Cyber Crime and Its Preventive Measures," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 6, no. 3, 2017, doi: 10.17148/ijarcce.2017.63214.

[14] G. Onwuadiamu, "Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts," *J. Econ. Criminol.*, vol. 8, 2025, doi: 10.1016/j.jeconc.2025.100136.

[15] A. Kumar, "Cyber Crime Awareness from the Perspective of Educators: A Conceptual Study," *SEEJPH*, vol. 26, no. s2, 2025.

[16] J. Shah, "A Study of Awareness About Cyber Laws for Indian Youth," *Int. J. Trend Sci. Res. Dev.*, vol. 1, no. 1, 2016, doi: 10.31142/ijtsrd54.

[17] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, "Cybersecurity and cybercrime: Current trends and threats," *J. Int. Stud.*, vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[18] K. Nir, "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future," *Crime, Law Soc. Chang.*, vol. 66, no. 3, pp. 313–338, 2016.

[19] L. Wu, Q. Peng, and M. Lembke, "Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database," *Int. J. Cybersecurity Intell. Cybercrime*, vol. 6, no. 1, pp. 5–28, 2023, doi: 10.52306/ozmb2721.

[20] M. Ahmead, N. El Sharif, and I. Abuiram, "Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study," *Crime Sci.*, vol. 13, 2024, doi: 10.1186/s40163-024-00230-w.

[21] N. Jain and V. Srivastava, "Cyber Crime Changing Everything -An Empirical Study," *Int. J. Comput. Appl.*, vol. 1, no. 4, 2014, [Online]. Available: http://www.rspublication.com/ijca/ijca_index.htm

[22] A. K. Mokha, "A Study on Awareness of Cyber Crime and Security," *Res. J. Humanit. Soc. Sci.*, vol. 8, no. 4, pp. 459–464, 2017, doi: 10.5958/2321-5828.2017.00067.5.

[23] S. Kemp, "Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach," *Comput. Secur.*, vol. 127, 2023, doi: 10.1016/j.cose.2022.103089.

[24] P. Mali, J. S. Sodhi, T. Singh, and S. Bansal, "Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: An empirical study," *Int. J. Mech. Eng. Technol.*, vol. 9, no. 2, 2018.

[25] H. T. N. Ho and H. T. Luong, *Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis*, vol. 2, no. 4. Springer International Publishing, 2022. doi: 10.1007/s43545-021-00305-4.

[26] D. J. KV, M. J. Jaiswal, M. S. Santosh, and M. S. Baiju, “A Study on People’s Opinion on Awareness about Cybercrime in India,” *Int. J. Indian Psychol.*, vol. 11, no. 3, 2023, doi: 10.25215/1103.026.

[27] Kirti and D. J. Singh, “Exploring the Evolving Landscape of Cybercrime in India and Strategies for Prevention,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 6, 2023, doi: 10.22214/ijraset.2023.53624.

[28] A. Thomas, “Analysis on Cyber Crimes and Preventive Measures,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 5, pp. 3738–3744, 2023, doi: 10.22214/ijraset.2023.52481.

[29] S. Batra, M. Gupta, J. Singh, D. Srivastava, and I. Aggarwal, “An empirical study of cybercrime and its preventions,” *PDGC 2020 - 2020 6th Int. Conf. Parallel, Distrib. Grid Comput.*, pp. 42–46, 2020, doi: 10.1109/PDGC50313.2020.9315785.

[30] H. M. Khadas, “The Causes of Cyber Crime,” *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 8, pp. 476–478, 2020, doi: 10.38124/ijisrt20aug432.

[31] R. Shah, “CYBER CRIMES IN INDIA: TRENDS AND PREVENTION,” *Int. J. Res. Anal. Rev.*, vol. 6, no. 1, pp. 25–37, 2019.

[32] R. Sinha and H. Kumar, “A Study on Preventive Measures of Cyber Crime,” *Int. J. Res. Soc. Sci.*, vol. 8, no. 11, pp. 265–272, 2018, doi: 10.13140/RG.2.2.14212.04480.