Cyber Crime: A Serious Threat to the Country

Pradeep Kushwaha
Assistant Professor, Department of E.A.F.M., Government Commerce College, Kota, E-mail: pdk7791@gmail.com

Abstract

We are living in an era in which people increasingly rely on mobile gadgets and internet-enabled devices to perform most of their daily activities. Personal information is no longer completely private because the adoption of computer networks for work and communication. Similarly, due to the progression in different kinds of computer networks, cybercrimes have also progressed, as the use of new technology has enabled a better future for cybercriminals. There is a huge count of cybercrimes occurring in the country every day, which is becoming difficult for the public to detect, leading them towards increased complexities while trying to prevent them. This phenomenon has further led people towards the use of various kinds of cyber technology, which makes the public more prone to cybercrimes. This kind of cybercrime leads the public towards huge economic as well as a threat to their integrity. With changing technologies and user needs, cybercrime methods continue to evolve, intensifying associated threats. This study aims to raise awareness about the various types of cybercrimes prevalent in society, examine their causes and threats, and highlight effective preventive measures. The information is based on data and publications derived from news reports, news portals, and related websites. The results indicate a unanimous increase in the prevalence of cyber fraud across states, however significant disparities among states on reporting, actual financial losses, and recovery rates. Further, the analysis shows that while reporting mechanisms have been strengthened, the recovery rates remain inappropriately low. This indicates a need to strengthen preventive measures as well as awareness campaigns.

Keywords: cybercrime, cyberattacks, cyber security, internet crime, phishing

Corresponding Author: Pradeep Kushwaha, Assistant Professor, Department of E.A.F.M., Government Commerce College, Kota, E-mail: pdk7791@gmail.com
How to cite this article: Kushwaha P., (2025). Cyber Crime: A Serious Threat to the Country, Commerce Research Review 3(1) 76-87
DOI: https://doi.org/10.21844/crr.v3i01.1142
Source of support: Nil
Conflict of Interest: None
Received: 19.10.2025 **Accepted:** 30.11.2025 **Published:** 20.12.2025

Introduction

Cybercrime refers to criminal activities facilitated by a computer or network. In other terms, when a computer or network participates in a criminal act, it is referred to as cybercrime. Cybercrime refers to the perpetration of illegal activities by individuals or groups aimed at damaging a person's image or inflicting physical or psychological harm. These offenses occur in either way through contemporary communication technologies such as mobile phones and the internet, encompassing chat rooms, emails, online forums, and other platforms.

The Information Technology Act characterizes cybercrime as any offense perpetrated by computers, the internet, or other technological means. Cybercrime is prevalent in contemporary India. It adversely affects both society and the government, yet the attackers manage to cover up their identity. The internet serves as a medium for numerous illicit activities conducted by individuals possessing advanced technological

expertise. Cybercrime encompasses all illicit activity in which a computer or the internet serves as a tool, a victim, or both of them.

The Indian law framework has not explicitly defined "cybercrime," however the term has been employed in various court decisions to signify distinct concepts. This is a novel hazard arising from the prevalent usage of computers in contemporary society. The substantial advantages of the internet meet with its negative aspects, including the rise of cybercrimes such as cyber-stalking, cyber-terrorism, email spoofing, cyber pornography, and cyber defamation. Conventional crimes can be classified as cybercrimes if executed using computers and the internet.

The oxford Learners Dictionary defined the term cybercrime as *"crime that is committed using the Internet, for example by stealing someone's personal or bank details or infecting their computer with a virus."*

In today's digital age, the fast growth and spread of smart technology and internet services have had a big effect on the way social, economic, and administrative processes work in the country. A new epoch has commenced for digital financial services, encompassing UPI, digital wallets, and online banking services. This epoch is inextricable from cyberspace. The government's initiatives to enhance India's digital infrastructure and implement e-governance have rendered services more efficient and user-friendly. Nonetheless, they have rendered cyber attacks more pervasive and perilous due to the substantial volume of critical information disseminated online.

Cybercriminals can now employ increasingly sophisticated forms of cyberattacks in a more targeted manner due to the continuous evolution of technology. Currently, fraudsters employ phishing tactics, QR code fraud, SIM switching, identity theft, and various other forms of cybercrime to exploit individuals without technological proficiency. This is due to the emergence of new technologies like as artificial intelligence, cloud computing, and messaging automation systems, which have complicated cybersecurity efforts. The majority of cybercrimes are currently perpetrated via these technologies, which facilitate significant and elusive offenses. Cybercrime has significantly escalated beyond mere isolated incidents.

A significant aspect in the current context is the substantial disparity between the rate of digital technology use and the capacity of individuals and societies to address cyber crimes. This aspect led to an escalation in losses incurred and the capacity to recover those losses. An other significant aspect is that the transnational character of the crime, along with the evolving nature of evidence, presents a substantial challenge in finding the attackers.

Given the preceding instance, it is essential to regard cybercrime not merely as a technological issue but also as a socio-economic and governance-related concern, taking into account the current technological landscape and its demands.

Research Gap:

Despite the increasing frequency of cybercrime, a limited number of individuals comprehend its nature, underlying causes, or preventive measures. The existing studies predominantly focus on legal, technological, or statistical matters. Insufficient emphasis has been placed on awareness, regarded as one of

the most effective methods to mitigate cybercrime, particularly as its frequency increases.

Objectives of the study

Currently, cybercrime is becoming a significant concern for the nation. With advancements in technology, cybercrimes are escalating daily. Therefore, it is imperative to assert authority over this matter. Taking all these factors into account, the preparation objectives for this study are as follows:

- The primary objective of this study is to raise societal awareness of the many forms of cybercrime occurring inside the country.
- To elucidate methods for safeguarding society from various cybercrimes.
- To understand the primary factors contributing to the prevalence of cybercrime.
- To know the ways in which a person can keep his important information safe from cybercriminals.

Causes of Cyber Crime

According to Hart, in his book "The Concept of Law", the weakness of human nature makes the protection offered by the rule of law necessary. Similarly the concept of the rule of law is applicable in the cyber world, as the weaknesses of computers require the establishment of the law for the security of these systems from cybercrimes. The causes of the vulnerabilities in the security of the computer are as follows:

Compact Data Storage:

Computers are unique in storing the data in a very compact space, that makes the process of data retrieval very efficient, using both physical and digital means.

Accessibility Challenges:

It is very hard to protect the security of the computer from unauthorized access, not just because of human error, but because of the complexity of the technology used in the systems, as the hidden installation of viruses like logic bombs, keystroke logging programs that are capable of accessing the login details, sophisticated audio recording devices, and retina scanners can easily bypass the security systems like the firewall, posing a great threat to the security systems.

The complexity of Systems

Computers function through diverse operating systems characterized by sophisticated coding. No matter how sophisticated the human intellect may be, errors are inevitable. Consequently, computer systems are subject to threats. Cybercriminals exploit these system vulnerabilities to obtain sensitive information.

Human Error

Human behavior is intrinsically susceptible to mistakes, rendering it nearly impossible to guarantee

infallible security of computer systems. These security lapses provide thieves the opportunity to seize control of these computer systems.

Ephemeral Evidence:

A significant difficulty is the transitory nature of evidence, which implies a considerable risk of its loss owing to mishandling. Moreover, the international dimension of data collection complicates cybercrime investigations

Various methods through which cybercrime activities are carried out

Hacking:

Hacking is a cyberattack that is widely used to abuse people's PC infrastructure or a private network within a PC. Basically, it is a denied access on the security framework of the PC to serve some illegal purpose. This is done by hackers who are highly skilled and trained individuals in breaking into a security system.

Trojan Attack:

Trojan is a type of invisible virus. The term originates from the 'Trojan horse' concept. A Trojan horse virus is a form of malicious software that masquerades as a legitimate application to infiltrate a computer. In computing, it denotes a rogue application that pretends to be legitimate to stealthily take over another's system. Email is typically the most prevalent method for distributing Trojans. By hiding dangerous virus in Trojan by cyber criminals, it is presented as a reliable file.

Virus Attack:

Viruses are a type of software that latches onto a computer or a file and then propagates to other files and computers within a network. Typically, they compromise the data on a computer, altering or eradicating it.

Worm Attack:

A worm is distinct from a virus in that it doesn't need to attach to a host program. It autonomously replicates itself repeatedly, consuming all the available memory in a computer.

E-Mail Bomb:

It is a kind of Internet abuse which is executed by sending multiple emails in bulk to a mail box at a particular email address. This includes the main mail servers being compromised and the service crashing. This type of activity refers to the sending of a huge amount of mails to the victim, which may be a person or a company or even an entire mail server, eventually resulting in a crash. Which has many side effects.

Phishing:

Phishing is a cybercrime strategy where a target is contacted through email with a specific aim or objective, phone or instant message by someone acting as an authentic establishment to persuade the individual into providing sensitive information, for example banking information, Debit card, Credit card details and password etc. This data is used to obtain vital records and later misuse of this collected data is capable of causing widespread fraud, identity theft and monetary loss.

Identity Theft:

Identity theft is the obtaining of personal or financial data of another individual's with the intent of making transactions or purchases through the name or identity of that person. This type of attack, the personal information of the individual is stolen and misused, with the victim having to bear the consequences.

Cyber Pornography:

Nowadays a lot of cybercrimes involve the use of cyberpornography. For example - criminals make obscene video calls to a person and by recording it blackmail the victim and extort money from him. Similarly, sometimes blackmail is done by sending obscene chat messages and sometimes by obtaining personal pictures with the help of third party apps.

Fraud by Pasting Fake QR Code on Original:

As the trend of making payment through QR code is increasing, similarly cybercrime has also started increasing through QR code. Now cyber criminals put fake QR code on top of the real QR code looks like the real one and people fall prey to it after scanning it.

Fraud by SIM card Swap:

Cybercrimes are also being committed through SIM swap. Such cyber criminals get a new SIM issued by the service provider using the personal information of the people. As soon as the SIM is released, calls, messages, notifications etc. stop coming. After this the criminals get access to OTP etc. by which they commit all the crimes.

Table 1: State/UT wise comparative details of Citizen Financial Cyber Fraud Reporting Management System

(from 01.01.2023 to 31.12.2023)

S.N.	State	No. of complaint reported	Amount Reported (Rs in lakhs)	No. of complaints (put on hold)	Lien Amount (Rs. in lakhs)
1	Uttar Pradesh	197547	72,107.46	44089	5906.86
2	Maharashtra	125153	99,069.22	32050	10308.47
3	Gujarat	121701	65,053.35	49220	15690.9
4	Rajasthan	77769	35,392.09	20899	3934.82
5	Telangana	71426	75,905.62	26148	13137.94

Source: public information bureau

(https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158)

As it clear from the above table, the highest number of crimes in the nation in the year 2023 has been registered in Uttar Pradesh. Similarly, a sum of 11,28,265 cases were reported nationwide from 01.01.2023 to 31.12.2023, the total amount of which is Rs. 7,48,863.9(in lakhs).

Table 2: Showing the data of top 5 states in Rate of total cybercrime

S.N.	State	2020	2021	2022	Mid-Year Projected Population (in lakhs)	Rate of Total Cyber Crimes(2022)	Charge sheeting Rate (2022)
1	Telangana	5024	10303	15297	379.5	40.3	17.1
2	Karnataka	10741	8136	12556	674.1	18.6	21.1
3	Maharashtra	5496	5562	8249	1257.4	6.6	30.5
4	Goa	40	36	90	15.7	5.7	37.5
5	Assam	3530	4846	1733	354.9	4.9	14

The crime rate is determined by the no. of crimes occurring per 1,00,000 persons in the population.
(Data Source: National Crime Records Bureau–https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf)

The above table shows the data from 2020 to 2022 of the top 5 states in terms of cybercrimes rates in 2022. The 2020 to 2022 cybercrime data indicate an upward trend in the number of reported cases across different Indian states. Telangana recorded the most significant increase, with the cases increasing from 5,024 in 2020 to 15,297 in 2022, with the highest rate of cybercrime at 40.3 cases per lakh population.

Karnataka recorded 12,556 cases in 2022 and a rate of cybercrime at 18.6 per lakh. Maharashtra, with a massive population, reported 8,249 cases, and thus a lower rate of cybercrime at 6.6 per lakh. Goa reported the lowest number of cases, with just 90 in 2022, and a rate of 5.7 per lakh.

Assam was the lone exception to the increasing trend, with a decrease in cases from 4,846 in 2021 to 1,733 in 2022, and a rate of 4.9 per lakh. Whereas the charge sheeting rates are analyzed, the highest was by Goa at

37.5%, followed by Maharashtra at 30.5%, which showed comparatively effective processing through the legal system.

The other two, Karnataka and Telangana, recorded moderate rates of charge sheeting at 21.1% and 17.1%, respectively. Assam reported the lowest rate at 14%. This would indicate prosecution problems in spite of the high level of reported cybercrimes. The report points towards the increasing threat of cybercrime in India and the requirement of increased law enforcement and judicial effectiveness to manage the increased cases. The combination of the analysis from the above tables 1 and 2 such as "State / UT Wise Comparative Information of the Citizen Financial Cyber Fraud Reporting Management System (CtC-FCFRMS)" as of 2023, and the "Top Five States by Cyber Crime Rate 2021- 2023," may facilitate an extensive review of a substantial perspective concerning the growth rate, awareness, and reporting levels, concerning the occurrence of cybercrimes in India in general. Following a substantial foundation, as revealed in the existing tables, the incorporation of the NCRP state-wise information as of February 2025, in turn, may facilitate an in-depth evaluation by considering a series of critical elements concerning the financial aspect, lien actions, and refund outcomes in general.

Table 3: State-wise Statistics of Cyber Fraud Cases Reported on the NCRP

As on 28 February 2025 *Rs. in lakhs*

State	Total incidents Reported	Amount Reported	Lien Amount	Refunded Amount
Uttar Pradesh	630778	285875.57	30610.47	382.2
Maharashtra	427607	575492.05	62187.87	918.83
Gujarat	367754	274589.93	55698.11	1031.58
Rajasthan	267781	150912.65	18338.66	543.4
Karnataka	252487	415117.32	40341.8	475.96

Source: NCRP

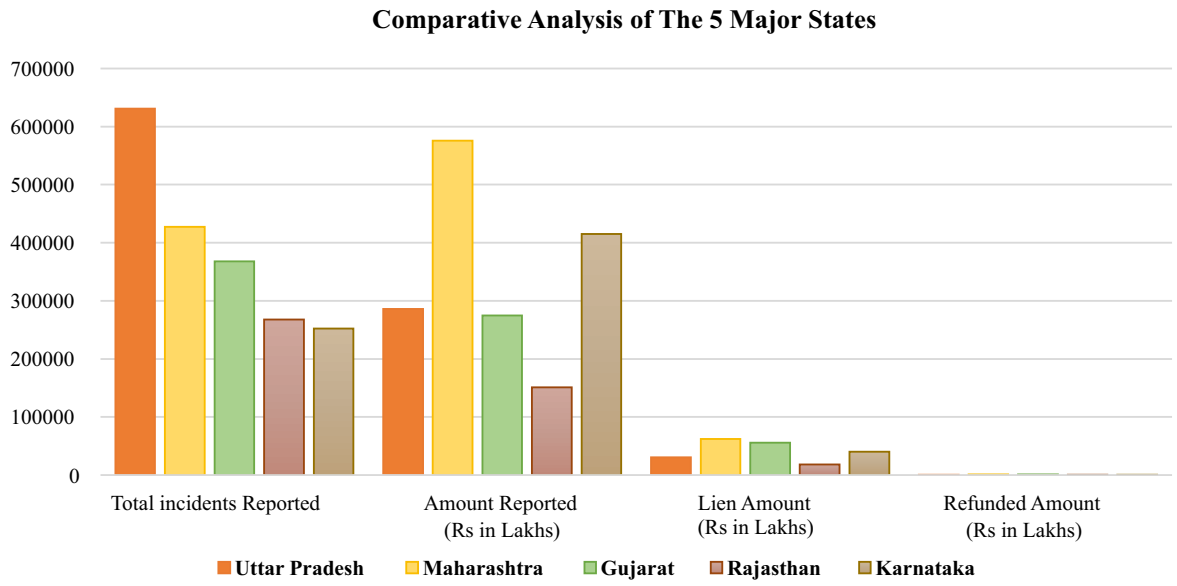

Fig. 1: Comparative Analysis of Cyber Fraud Incidents, Reported Amounts, Lien Amounts, and Refunds across Selected States (NCRP, 2025)

The table and figure provide a comparative analysis of cybercrime instances recorded on the NCRP across five prominent Indian states—Uttar Pradesh, Maharashtra, Gujarat, Rajasthan, and Karnataka—as of 28 February 2025. Uttar Pradesh has the greatest incidence of cyber fraud (630,778), signifying a significant prevalence of cybercrime, despite the total amount recorded is slightly less than that of Maharashtra and Karnataka. In Maharashtra, there is a considerably high financial impact, with the highest amount reported at ₹5,75,492.05 lakhs. This shows the high financial value of cyber crimes in developed economies.

In Gujarat and Karnataka, the amounts are considerably high. This shows the rise in cyber financial crimes as digital financial transactions increase.

In Rajasthan, the figures are low for all parameters. This can be because of fewer occurrences or a lack of reporting.

The lien amount is high in Maharashtra, which may be due to efficient handling and freezing of funds. The repaid amount is high in Gujarat, which can be because of efficient handling in this state.

The findings indicate significant disparities in the occurrence of cyber frauds in the respective states. This may be due to differences in financial vulnerability and recovery. This shows that awareness and prevention programs need to be state-specific.

The aggregate numbers also show the alarming extent and financial implications of the cybercrime cases reported and registered on the NCRP as of 28th February 2025. The total number of cybercrime cases reported and registered across the nation is 38,22,550. This shows the high frequency of cybercrime in the nation. The total amount reported and registered is ₹36,44,819.85 lakhs. This also shows the financial damages caused due to cybercrime. Out of the total reported amount, ₹4,38,080.57 lakhs has been seized. This shows the efforts made by law enforcement agencies and financial institutions to freeze suspicious and illegal transactions. The total amount returned is ₹6,051.65 lakhs. This amount is quite low similar to the total amount lost due to cybercrime.

National-level indicates that though reporting systems and first response measures have improved, the recovery ratio remains low. The data shows the urgent need to step up preventative measures, public education, digital literacy, and inter-agency cooperation in continuation to effectively combat the growing threat of cyber fraud in the nation.

From an examination of all three tables of data, a trend emerges: U.P., Maharashtra, Gujarat, Rajasthan, and Karnataka, which were previously identified as either high burden or high incidence states, are again at the top of the list for this year as well, with respect to sheer volume and financial exposure. However, the NCRP data adds an important analytical element in highlighting the inter-state variations in financial impact as well as the efficiency of financial recovery: Maharashtra, for example, shows the highest level of financial loss, highlighting the financial implications of cybercrime in the more advanced digital states, while Gujarat shows a relatively better level of refund efficacy in spite of comparable financial loss, while in Rajasthan, despite the relatively lower level of financial loss, the lien-to-loss ratio is significantly higher, indicating the efficacy of interim response measures.

This integration of this latest information gathered from NCRP with the already available data set using trends and reporting would provide a general understanding related to the concept and occurrence of cybercrime in India, ranging from levels of rate to levels of vulnerability and recoverability.

Ways to avoid cybercrimes:

- Avoid scanning QR codes received from unknown and unwanted sources. The web address must be checked while scanning the QR. If it looks like a sticker covering another QR code, it should not be scanned. Must ensure that auto-opening links from QR code scanning is disabled.
- If ever suddenly the mobile network goes out, then it should not be considered as a mere coincidence because it can also be a trap laid by cyber criminals for SIM swap. That's why the sim should be checked when the network goes.
- People should be cautious about receiving any kind of unknown video calls, as it can be a ploy by cyber criminals.
- Avoid clicking on any kind of link coming from unknown number and any link displayed in any browser. as this could be a fraudulent link sent by criminals to gain access to the device
- Do not pay attention to any unnecessary or spam email, and avoid sharing OTP or any kind of private data with any unknown person.
- One should secure their social networking profiles or personal accounts by two step authentication system. And the password should be changed at regular intervals.
- Along with changing the password at regular intervals, it should also be kept in mind that different passwords should be used for different accounts; otherwise it facilitates unauthorized access by cybercriminals.
- Do not register UPI on more applications than necessary and should avoid sharing banking information at unnecessary places.

Discussion:

It's also crucial to remember that technology isn't the only thing that causes cybercrime; human factors and institutional practices are also very important. Individuals commit errors, particularly when lacking knowledge, which is the primary catalyst for cybercrime. This directly results in cybercrimes such as phishing, wherein individuals disclose sensitive information by accessing fraudulent websites or replying to deceptive emails. The absence of passwords and other security measures is closely associated with hacking, when thieves get access to private and financial information. Online financial crime, including fraudulent investments and identity theft, is exacerbated by the lack of information verification and an overreliance on digital interactions. Excessive use of social media without appropriate privacy settings increases the likelihood of online stalking. A significant correlation exists between the motivations for cybercrime and a specific kind of cybercrime. Measures to combat cybercrime should encompass not just technological protections but also the promotion of knowledge and the encouragement of responsible online conduct.

Furthermore, organizational issues, such as protracted software updates and inadequate cybersecurity protocols, can enhance individuals' resilience to cyber attacks. Small enterprises and individual users may lack a systematic approach to safeguard themselves against cybercriminals. This indicates the necessity of collaborative efforts to establish a robust system of cyber resilience.

Limitations of the study:

Notwithstanding the significance and appropriate focus on the chosen topic, the current research is nonetheless constrained by many limits that must be acknowledged. The current research primarily relies on secondary data, with the author utilizing numerous news stories, government websites, and other pertinent online material. Nonetheless, it is acknowledged that the present research significantly relies on the veracity of material gathered from diverse news items and websites, which may differ from one state to another. The author employs a purely descriptive research methodology, undertaking the study solely to identify the characteristics of cybercrime. Thirdly, the research yielded inconclusive results owing to the absence of personal experiences and data that could have facilitated a deeper comprehension of the nature and classifications of cybercrime. The research examines cybercrime from a macro perspective, potentially causing the author to overlook subtle distinctions that occur. The report's results may become obsolete as cybercrime evolves with the emergence of new technology.

Conclusion:

The internet usage among individuals in India is increasing, and the habit of acquiring information online is expanding. Information collecting online is being facilitated even in collaboration with government departments. However, this facilitates work, while cyberattacks are concurrently increasing. The report indicates that cybercrime is increasing in the country and requires intervention. It is essential for individuals to be informed about cybercrimes, leading to the implementation of various programs. Cyber police stations have been established in many locations, including Rajasthan. However, these offenders must be swiftly penalized, and specialized courts should be established to address cybercrimes promptly. The government has established a web platform for reporting cybercrimes; nevertheless, few citizens are aware of its existence or functionality. To disseminate information, they must employ various media channels. Consequently, it is recommended that the nation formulate an effective cyber security strategy to deter cybercrime, penalize offenders adequately, and safeguard individuals' digital information. The study indicates that the issue must also be considered from an organizational standpoint, where, alongside individual incompetence, organizational factors that significantly contribute to the rise of cybercrime include inadequate cybersecurity measures, delayed system updates, and insufficient employee training. The results show that to improve cyber resiliency, the agencies need to get better at cooperating, there need to be improvements to funding the recovery effort, and there need to be improvements to digital literacy. To enhance the digital landscape and protect against digital dangers, a comprehensive plan involving the government, financial institutions, telecoms, and individuals is essential.

Scope of further research:

This study also offers avenues for further research in the following manners:

The researcher must employ an empirical study approach and gather primary data to investigate the facets of public awareness, victimization, and reporting in the context of cybercrime. The researcher's next step is to examine the relationship between the factors influencing the recognition of illiteracy and human errors with different aspects of cybercrimes, including phishing, identity theft, and financial fraud. The researcher may employ a quantitative research methodology for this purpose. The subsequent step for the researcher is to

evaluate the results in comparison to those from other states, regions, and demographic cohorts. This may yield more significant outcomes. The researcher may investigate the efficacy of government initiatives, the functions of cyber police stations, and the overall effectiveness of regulations aimed at preventing and reducing cybercrime. The researcher might also look into different parts of banking, health, education, and so on. The researcher can also look into the impact of the aforementioned programs on digital literacy, education, and related areas, within the framework of mitigating the risk of cybercrime in an increasingly digital landscape.

Bibliography, References and Webliography:

http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

https://www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office Research Report No. 75. Home Office.

Lu, Y. C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime and cybercriminals: An overview of the Taiwan experience. *Journal of Computer Information Systems, 46*(2), 118–126.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202–209.

Dashora, A. (2011). Cyber crime in society: Problems and prevention. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240–259.

Halder, D., &Jaishankar, K. (2011). Cyber crime and the victimization of women: Laws, rights, and regulations. Hershey, PA: IGI Global.

Saroha, R. (2014). Profiling a cyber criminal. *International Journal of Information and Computation Technology, 4*(3), 253–258.

Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: A social network approach to understanding cybercrime. *Journal of Money Laundering Control, 15*(3), 1–15.

Chang, L. Y. C. (2017). Cybercrime and cyber security in ASEAN. *Asian Journal of Criminology, 12*(2), 135–148.

Kandpal, V., & Singh, R. K. (2013). Latest face of cybercrime and its prevention in India. *International Journal of Basic and Applied Sciences, 2*(4), 150–156.

Tanwar, S., Paul, T., Singh, K., Joshi, M., & Rana, A. (2020). Classification and impact of cyber threats in India: A review. In *Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)* (pp. 129–135). IEEE.
Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *International Journal of Computer Science and Network Security, 9*(5), 252–261.

Singh, Pravin & Agrawal, Animesh & Singh, Vishal & Singh, Pankaj. (2025). Examine the Intention of Generation Z to Adopt Metaverse Apps and Devices: A Technology Acceptance Model Approach. COMMERCE RESEARCH REVIEW. 2. 1-12. 10.21844/crr.v2i02.1128.

Rai, Anjanee. (2025). From Cash to Clicks: UPI's Role in Shaping Digital Payments in India. COMMERCE RESEARCH REVIEW. 2. 37-44. 10.21844/crr.v2i02.1131.

Sharma, Neeti & Singh, Brahmdev. (2025). Digital Banking: Transforming Consumer Habits in the Modern Financial Landscape. II. 76-87. 10.21844/crr.v2i01.1124.

National Cyber Crime Reporting Portal (2025). *State wise statistics of cyber fraud cases*. Government of India. https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber

PIB India (2025). *Curbing Cyber Frauds in Digital India. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=2*

https://www.bbau.ac.in/dept/Law/TM/1.pdf

https://www.naavi.org/pati/pati_cybercrimes_dec03.htm

https://legaljobs.io/blog/cyber-crime-statistics/

https://www.getastra.com/blog/security-audit/cyber-crime-statistics/#:~:text=year%20to%20792k.-,How%20many%20cyber%20crimes%20are%20committed%20each%20year%3F,around%2033%20billion%20account%20breaches

.

https://m.economictimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/amp_articleshow/100096450.cms

https://www.statista.com/statistics/1197074/india-cyber-security-market-size/

https://scholar.google.com/

https://cybercrime.gov.in/

https://ncrb.gov.in/en/node/2318

https://home.rajasthan.gov.in/content/homeportal/en/sardarpateluniversityportal/academics/centers/cfcs.html

https://www.indiatoday.in/technology/features/story/cyber-fraud-incidents-rising-in-india-how-to-file-a-complaint-online-on-cyber-crime-portal-2335149-2023-02-15

https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html#:~:text=Sending%20threatening%20messages%20by%20email,cyber%20frauds%20%2D%20Sec%20420%20IPC

https://infosecawareness.in/cyber-laws-of-india

https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158

https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber