IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

A Study on the Increasing Incidence of Cyber Crimes and their Prevention

Mr. Pawan Kumar[1] and Mr. Raj Kumar[2]
Computer Faculty, Government Senior Secondary School Bagrian,Karpurthala[1]
Assistant Professor, Faculty of Management and Commerce, Guru Kashi University, Punjab[2]
pkattrii@gmail.com and rrajkumar53131@gmail.com

Abstract: *The rapid growth of information and communication technology has made computers and the internet an integral part of modern life. Alongside these advancements, cyber-crime has emerged as a major challenge in the digital age, affecting individuals, organizations, and governments. Cyber-crime includes offences such as hacking, phishing, ransomware attacks, cyber stalking, identity theft, and online financial frauds, which have increased due to widespread internet usage, technological advancements, and lack of cybersecurity awareness. This study examines the nature, forms, and causes of cyber-crime, highlighting its social and economic impact. It also discusses preventive measures and technological safeguards to combat cyber threats. The study emphasizes that enhancing digital awareness and adopting secure online practices are essential for protecting personal data and reducing cyber risks in today's interconnected world.*

Keywords: Cyber Crime, Internet Security, Hacking, Phishing, Cyber Awareness, Digital Safety

I. INTRODUCTION

India is becoming one of the biggest digital societies in the world thanks to the quick development of information and communication technology. Accessibility and efficiency have been greatly enhanced across sectors by increased internet adoption, smartphone use, the expansion of digital payments, e-governance efforts, and online education and commerce. Cybersecurity is now a major worry for people, organisations, and the government due to the dramatic increase in cybercrimes brought on by this digital change. Illegal behaviours using computers, digital gadgets, and networked systems are referred to as cybercrimes. Cybercrime incidences in India have significantly increased between 2020 and 2025, especially after the COVID-19 epidemic, which increased reliance on online platforms for communication, work, education, and banking. The number and sophistication of crimes like ransomware attacks, phishing, hacking, identity theft, online financial fraud, cyberstalking, and social media abuse have increased. Cybercrime is one of the fastest-growing types of crime in the nation, according to official statistics and national cybercrime reporting portals, which show a steady upward trend in reported incidents.

Table: Year-wise Cyber Crimes Reported in India

S. No.	Year	Number of Cyber Crimes Reported
1	2012	3,477
2	2013	5,693
3	2014	9,622
4	2015	11,592
5	2016	12,317
6	2017	21,796
7	2018	27,248

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

S. No.	Year	Number of Cyber Crimes Reported
8	2019	44,546
9	2020	50,035
10	2021	52,974
11	2022	65,893
12	2023	75,656
13	2024	More than 7,40,000

Increased internet usage, a lack of digital awareness, technological weaknesses, and the changing strategies of cybercriminals are some of the factors contributing to the rising prevalence of cybercrimes during this time. In addition to causing monetary damages, these crimes jeopardise national security, individual privacy, and public confidence in digital systems. Therefore, in order to establish effective legal, technological, and preventive policies, it is imperative to comprehend the nature and growth of cybercrimes in India between 2020 and 2025. The purpose of this study is to investigate the need for more robust cybersecurity measures in the Indian setting, as well as emerging patterns and underlying causes.

Year	Cybercrime Cases (Approx.)	Key Notes
2020	50,035	Base level in early digital era.
2021	52,974	Continued rise.
2022	65,893	Large jump, high share of fraud.
2023	86,420	31% rise vs 2022; fraud dominant.
2024	22,68,346 (incidents reported on NCRP)	Massive reporting surge; huge financial losses.

Government Schemes and Support to Reduce Cyber Crimes in India

To combat the rising number of cybercrimes, the Indian government has implemented a number of institutional, technological, and legal measures. A robust legal framework for dealing with cybercrimes such hacking, identity theft, online fraud, and cyberterrorism is provided by the Information Technology Act of 2000 and pertinent sections of the Indian Penal Code. The National Cyber Crime Reporting Portal and the 1930 cybercrime helpline were established by the government to streamline reporting, allowing citizens to promptly report cybercrimes, particularly financial frauds, and enabling authorities to respond promptly. Law enforcement agencies are now better coordinated thanks to the creation of the Indian Cyber Crime Coordination Centre (I4C), and police and judiciary officials' cyber investigation and forensic skills are improved through ongoing training programs. Additionally, programs like Digital India and Cyber Surakshit Bharat encourage citizens to practise safe online conduct and raise knowledge of cybersecurity. Additionally, the government has made investments in real-time monitoring systems, sophisticated cyber forensic infrastructure, and CERT-In services for quick incident response. Additionally, addressing cross-border cybercrimes is aided by international cooperation with other nations. When taken as a whole, these actions demonstrate the government's all-encompassing strategy for stopping and minimising cybercrimes in India.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

Government Schemes and Support to Reduce Cyber Crimes in India

Scheme / Initiative	Year Launched	Objective / Support Provided
Information Technology Act (IT Act), 2000	2000	Provides the legal framework to deal with cyber offences such as hacking, identity theft, cyber terrorism, and online fraud.
Indian Cyber Crime Coordination Centre (I4C)	2018	Strengthens coordination among law enforcement agencies and builds capacity for investigation of cybercrimes.
National Cyber Crime Reporting Portal (cybercrime.gov.in)	2019	Enables citizens to report cybercrimes online, with special focus on crimes against women, children, and financial frauds.
Cyber Crime Helpline – 1930	2020	Allows immediate reporting of financial cyber frauds to help block transactions and recover stolen money.
Cyber Surakshit Bharat Programme	2018	Promotes cybersecurity awareness and strengthens cyber resilience among government officials and organizations.
CERT-In (Indian Computer Emergency Response Team)	2004	Handles cyber security incidents, issues alerts and advisories, and coordinates responses to cyber threats.
Digital India Programme	2015	Enhances digital literacy and promotes safe and secure use of digital technologies across the country.
Capacity Building of Police under Cyber Crime Prevention	Ongoing	Provides training, cyber forensic labs, and modern tools to police and judicial officers for effective investigation.
International Cyber Cooperation	Ongoing	Facilitates intelligence sharing and joint action with other countries to combat cross-border cyber crimes.

Cyber Crime Awareness Programmes in India

The Government of India runs several cyber awareness programmes to reduce cybercrimes by educating citizens about safe online practices. Initiatives such as Cyber Surakshit Bharat, Digital India campaigns, CERT-In advisories, and cyber awareness drives by police departments focus on promoting cyber hygiene, identifying frauds, and protecting personal data. Awareness of the 1930 cybercrime helpline and the National Cyber Crime Reporting Portal has also helped citizens report incidents quickly. Additionally, schools, colleges, and community outreach programmes play a vital role in building a cyber-aware society and preventing cyber offences.

Programme / Initiative	Launched By	Purpose / Focus
Cyber Surakshit Bharat	Ministry of Electronics & IT (MeitY)	Creates awareness about cyber hygiene and strengthens cybersecurity awareness among government officials and institutions.
Digital India Awareness Campaigns	Government of India	Promotes digital literacy and safe use of internet, online payments, and e-governance services.
Stay Safe Online Campaign	CERT-In	Educates users on safe browsing, phishing prevention, password security, and data protection.
Cyber Jaagrookta (Cyber Awareness) Programmes	Ministry of Home Affairs / Police Departments	Conducts workshops, seminars, and outreach programmes for students, senior citizens, and the general public.
1930 Helpline Awareness Drives	Ministry of Home Affairs	Informs citizens about quick reporting of financial cyber frauds to reduce losses.
Social Media & Mass Media	State Police & Cyber Cells	Uses social media, radio, TV, and posters to spread

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

Programme / Initiative	Launched By	Purpose / Focus
Campaigns		awareness about cyber frauds and online safety.
School & College Cyber Awareness Programs	State Governments / NGOs	Educates youth on cyber safety, cyber bullying, and responsible internet use.

Latest Types of Cyber Crimes

With the rapid evolution of digital technology, cyber criminals are continuously adopting new and sophisticated methods. Some of the **latest and most prevalent types of cybercrimes** are as follows:

Phishing and Smishing Attacks

Fraudulent emails, messages, or calls are used to trick individuals into revealing sensitive information such as passwords, OTPs, and bank details.

Ransomware Attacks

Malicious software locks or encrypts data and demands ransom for restoring access. These attacks increasingly target hospitals, educational institutions, and government offices.

Online Financial Frauds

Includes UPI frauds, fake investment schemes, digital arrest scams, loan app frauds, and e-commerce scams, which have sharply increased in recent years.

Identity Theft

Personal information is stolen and misused for illegal activities such as opening fake accounts or committing financial fraud.

Cyber Stalking and Online Harassment

Continuous monitoring, threatening messages, and misuse of social media platforms to harass individuals, particularly women and minors.

Deepfake and AI-Based Crimes

Use of artificial intelligence to create fake images, videos, or voice recordings to spread misinformation, defame individuals, or commit fraud.

Social Media Crimes

Account hacking, fake profiles, impersonation, and spreading false or harmful content through social networking sites.

Data Breaches and Hacking

Unauthorized access to computer systems or databases to steal, alter, or destroy sensitive information.

Cyber Terrorism

Use of cyberspace to threaten national security by targeting critical infrastructure, government systems, or spreading extremist propaganda.

Online Gaming and App-Based Frauds

Criminal activities involving fake gaming apps, in-app purchases fraud, and exploitation of minors through online gaming platforms.

Schemes and Support by Banks to Prevent Cyber Crimes in India

Banks in India play a crucial role in preventing cybercrimes, especially online financial frauds, by adopting technological safeguards, customer awareness initiatives, and regulatory compliance measures. The major schemes and support mechanisms introduced by banks, in coordination with the Reserve Bank of India (RBI) and the Government of India, are summarized below. Banks in India actively support the prevention of cybercrimes by implementing strong security measures such as two-factor authentication, real-time transaction alerts, EMV chip-based cards, and secure UPI systems. RBI's zero liability policy safeguards customers against losses if frauds are reported in time. Banks also employ advanced fraud detection systems and conduct regular security audits to identify and prevent cyber threats. Additionally, customer awareness campaigns and dedicated fraud reporting mechanisms help users identify scams and

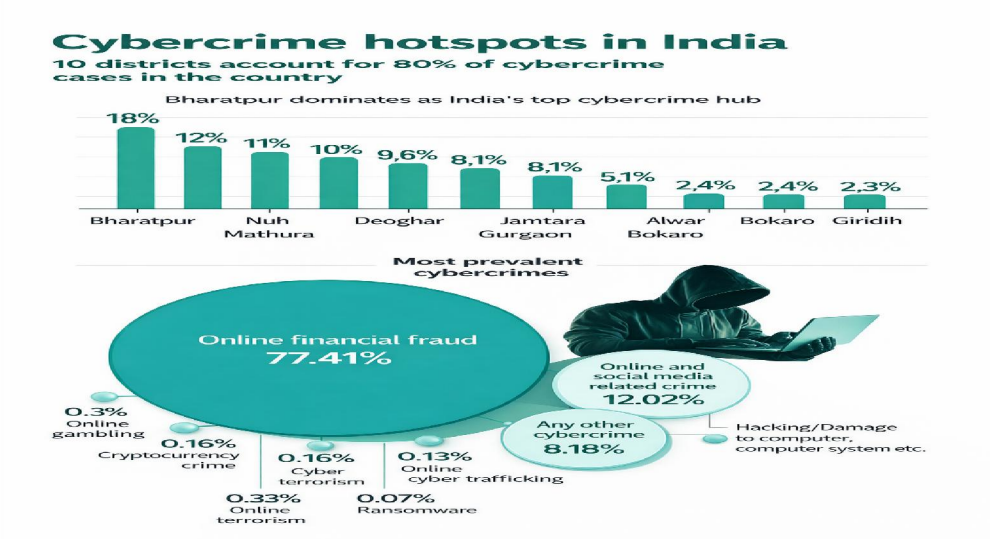
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

respond quickly. Through coordination with cybercrime cells and regulatory authorities, banks play a vital role in reducing financial cybercrimes and protecting digital banking systems.

Banking Schemes and Support to Prevent Cyber Crimes

Scheme / Support Measure	Implemented By	Purpose / Description
Two-Factor Authentication (2FA)	RBI & All Banks	Ensures additional security for online banking and card transactions using OTPs or biometric verification.
Transaction Alerts (SMS/Email)	All Banks	Provides real-time alerts for every transaction to enable quick detection of unauthorized activity.
Zero Liability Policy	RBI Guidelines	Protects customers from financial loss if fraud is reported promptly and no customer negligence is involved.
EMV Chip and PIN Cards	RBI & Banks	Replaces magnetic stripe cards with chip-based cards to prevent card cloning and skimming.
UPI Security Features	NPCI & Banks	Includes UPI PIN, device binding, transaction limits, and time-based OTPs to prevent fraud.
Fraud Monitoring Systems	Banks	Uses AI and real-time monitoring tools to detect suspicious transactions and block them instantly.
Customer Awareness Campaigns	Banks	Educates customers about phishing, fake calls, OTP sharing, and safe digital banking practices.
Dedicated Fraud Reporting Channels	Banks	Provides toll-free numbers, emails, and apps for immediate reporting of cyber frauds.
Account Freezing & Fund Recovery Support	Banks & Cyber Cells	Assists in freezing fraudulent accounts and recovering funds upon timely complaint.
Regular Security Audits & Compliance	RBI & Banks	Ensures periodic system audits and adherence to cybersecurity standards.

India's cybercrime landscape



Source: Google

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

The image highlights India's cybercrime landscape by identifying key geographic hotspots and dominant crime types. It shows that **just 10 districts account for nearly 80% of reported cybercrime cases**, indicating a high concentration rather than uniform spread. **Bharatpur** emerges as the largest cybercrime hub with **18%** of cases, followed by **Mathura (12%), Nuh (11%), Deoghar (10%), Jamtara (9.6%),** and **Gurgaon (8.1%),** with smaller but notable shares from **Alwar, Bokaro, Karma Tand, and Giridih.** In terms of nature of offences, **online financial fraud overwhelmingly dominates at 77.41%,** revealing that cybercrime in India is primarily economically motivated. This is followed by **online and social media–related crimes (12.02%)** and **other cybercrimes (8.18%),** while technically sophisticated crimes like **hacking (1.57%), ransomware (0.07%), cyber terrorism (0.16%),** and **cryptocurrency-related crimes (0.16%)** remain relatively limited in proportion. Overall, the image underscores that India's cybercrime challenge is both **regionally concentrated and financially driven**, pointing to the need for targeted policing, financial awareness, and localized cybercrime prevention strategies.

II. CONCLUSION

The present study highlights that cybercrime has emerged as one of the most serious challenges of the digital era, particularly in a rapidly digitizing country like India. The analysis of year-wise data clearly indicates a sharp and continuous rise in cybercrime cases from 2012 to 2025, with an alarming surge in recent years. The concentration of cybercrimes in specific districts and the dominance of online financial fraud reveal that cyber offences are largely organized, economically motivated, and driven by social engineering rather than purely technical expertise. The study further establishes that increased internet penetration, digital payments, lack of cybersecurity awareness, and technological misuse are the major factors contributing to the growth of cybercrimes.

The paper also underscores the significant role played by the government, banks, and law enforcement agencies in combating cybercrime through legal frameworks, reporting mechanisms, awareness programmes, and advanced security measures. Initiatives such as the IT Act, National Cyber Crime Reporting Portal, 1930 helpline, I4C, and banking safeguards have strengthened India's response to cyber threats. However, the findings suggest that technology alone cannot address this problem. Greater emphasis on public awareness, digital literacy, ethical use of technology, and targeted interventions in cybercrime hotspots is essential.

REFERENCES

[1]. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
[2]. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z
[3]. Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Sage Publications.
[4]. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global South*. Palgrave Macmillan.
[5]. Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.
[6]. Government of India. (2000). *Information Technology Act, 2000*. Ministry of Law and Justice.
[7]. National Crime Records Bureau. (2022). *Crime in India: Cybercrime statistics*. Government of India.
[8]. Symantec Corporation. (2021). *Internet security threat report*. Symantec.
[9]. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
[10]. Chawki, M., Darwish, A., Khan, M. M., & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction*. Springer.