Manuscript ID:
TIJCMBLIR-2025-0202030

Volume: 2

Issue: 2

Month: April

Year: 2025

E-ISSN: 3065-9191

Submitted: 05 Mar 2025

Revised: 15 Mar 2025

Accepted: 26 Apr 2025

Published: 30 Apr 2025

Address for correspondence:
Amuksiddha Shrimant Pujari (Assistant Professor in Faculty of Commerce) Dr. Patangrao Kadam Arts and Commerce College, Pen. Dist. Raigad.
Email:
amitpujari9999@gmail.com

DOI: 10.5281/zenodo.15967490
DOI Link:
https://doi.org/10.5281/zenodo.15967490

Cyber Crimes and Strategies for Mitigating in Banking and Financial Services

Dr. Amuksiddha Shrimant Pujari
(Assistant Professor in Faculty of Commerce) Dr. Patangrao Kadam Arts and Commerce College, Pen. Dist. Raigad.

Abstract:

A computer, network device, or network-based criminal activity is called a cybercrime. Nowadays, technology that is meant to enhance life, such as computers, the internet, and cell phones, has become the means to be cheated. Both ordinary and educated individuals are victims of cheats who cheat them out of their hard-earned cash. The Indian government launched the 'Citizen Financial Cyber Fraud Reporting and Management System' in 2021 due to an increase in cybercrimes in the banking sector. Individuals have lost money due to a range of cybercrimes such as phishing, identity theft, SIM switch scams, and vishing. Best practices such as do not pay by responding to alarming or threatening messages immediately. Do not click on unusual links or rely on unknown messages from unknown senders. To confirm the validity of such claims or allegations, the bank or lending institution should be contacted promptly through formal channels. Never shares sensitive or financial information with anyone, such as card number, expiration date, CVV, PIN, OTP, or bank credentials. To pay, not receive money, enter your UPI PIN, or scan a QR code. Do not accept requests for payments or financial transfers from unknown UPI IDs. Make payments via an authorized, official website or application, and always check the Customer Care or Helpline number on the original electricity bill. With Karnataka, Uttar Pradesh, and Telangana as the top states that reported the highest incidents, an analysis of cybercrime data between 2018 and 2022 reveals a staggering increase in cybercrime activities. Greater smartphone usage, e-transactions, and online interactions are culprits that drive cybercrimes upward. This highlights the importance of continuous awareness, improved reporting mechanisms, and more robust security protocols to shield individuals and businesses from cyber threats.

Keywords: *crime, cybercrime, credit card, ATM, Debit card, fraud, fishing, phishing, spamming, cryptojacking, espionage*

Introduction:

Cybercrime is broadly defined as " any criminal act that involves a computer, networked device, or a network". Everyday useful gadgets such as computers, the Internet, and any electronic devices that are useful for communication are becoming tools of scam. You are just that, and it is all the equipment for your life betterment and self-development. No need to speak about the Internet, computers, and mobiles is the strongest creation ever occurring in humans. However, ill-natured individuals are ethically less and individuals' hard-earned money is stolen from them in seconds due to cheating people's time we termed cybercrime, individuals involved in cybercrime. Financially bank related online crime is counted as widespread. For this reason, the Government of India enacted a law, and in the year 2021 'Citizen Financial Cyber Fraud Reporting and Management System,' under I4C was initiated for gathering instant reports on financial fraud and stopping money from being remitted to such scammers. In it, a toll-free number '1930" was set up to provide information about cybercrime and report it.

Methodology:

The researcher gathered secondary data from books, government websites, newspaper articles, research articles, and papers published in online research journals.

Cybercrime methods Banking and Financial Services:

- **Vishing:** Definition and Prevention Practices in 2022. Vishing is a cybercrime that involves tricking people to share sensitive information over the phone. It is also known as "voice phishing."
- **Credit/Debit Card Scam:**
  Technique of scammers trying to obtain personal details through telephone call, e.g., Customer ID, Net Banking password, ATM PIN, OTP, Card validity date, CVV, etc.

How to Cite this Article:
Pujari, A. S. (2025). Cyber Crimes and Strategies for Mitigating in Banking and Financial Services. The International Journal of Commerce Management and Business Law in International Research, 2(2), 128–131. https://doi.org/10.5281/zenodo.15967490

- **SIM Swap Scam:** The SIM swap cam is used when fraudsters can utilize the mobile service provider to illegally obtain a new SIM card against a registered mobile number. They receive notifications and the One-Time Password (OTP), which is required to make financial transactions from the victim's bank account, with the help of this new SIM card. The phrase SIM Swap is used to describe the illegal procurement of a new SIM card through a registered cell phone number.
- **Debit/Credit Card Fraud:** The illegal use of another individual's credit or debit card data for purchasing or withdrawing money from it is referred to as credit card (or debit card) fraud.
- **Impersonation and Identity Theft:** Use of another individual's password, electronic.
- signature, or other unique identification characteristic fraudulently or dishonestly is referred to as impersonation and identity theft.
- **Phishing:**
  Phishing is a type of deception where emails appearing to be from a credible source are utilized to gather personal data such as Customer ID, IPIN, Credit/Debit Card number, Card validity date, and CVV number**.**
- **Spamming:** Ransomware is a type of computer program that kidnaps information and data by encrypting data and storage media on communication hardware such as desktops, laptops, and mobile phones, etc. The victim pays the demanded ransom if he wants his device to be decrypted.
- **Cryptojacking:**
  Crypto mining illegally using computer resources is called cryptojacking.
- **Espionage:**
  The process of collecting information and data wi thout the knowledge or approval of the owner is referred to as espionage.

Best practices to avoid financial scams/frauds:

- Do not depend on the voice of an unknown caller and do not post excessive details on social media.
- Do not pay by responding to alarm or threat messages immediately.
- Do not click on unusual links or rely on unknown messages from unknown senders.
- To confirm the validity of such claims or allegations, contact the bank or lending institution promptly through formal channels.
- Avoid using search engines to search for customer service or helpline numbers. Instead, for authentic customer service contact details, use the official websites or mobile apps of the company or organization.
- Never share sensitive or financial information with anyone, such as card number, expiration date, CVV, PIN, OTP, or bank credentials.
- To pay, not receive money, enter your UPI PIN, or scan a QR code.
- Do not accept requests for payments or financial transfers from unknown UPI IDs.
- Make payments via an authorized, official website or application, and always check the Customer Care or Helpline number on the original electricity bill.
- Avoid reacting to or believing in unsolicited messages that promise instant money in return for online responsibilities on social media or instant messaging applications such as Telegram and WhatsApp.
- Verify the legitimacy of investment prospects, employment opportunities, etc., from genuine and official sources.
- Be cautious of unsolicited calls claiming severe threats or legal problems, especially if they demand money transfers or quick actions.
- If threatened with legal action, verify with the relevant authorities, ask for official notification, and contact the local police station first before taking any orders or transferring money.
- For confirmation or clarification, always telephone the local police station at once and ask for formal notifications, other relevant information, etc.

Discussion and Result:

In 2018-2022 the following cyber-crimes were reported by people in various states of India. Based on the data, the following observations were made:

Total Rise in Cyber Crimes (2018-2022):

From 27,248 in 2018 to 65,893 in 2022, the total number of cases of cybercrime registered across India has steadily increased, showing a pronounced spike in instances reported across a period of five years. Either a trend in expanding cybercrime activity or increasing reporting and gathering of information with the passing years can be implied through a surge in case registration.

Highest Case-Registering States:

Karnataka has always recorded the highest number of cybercrime cases in all years, with 12,556 cases in 2022 being the highest in any state or union territory (UT).

1. Digital Transformation: Being its technology capital, Bangalore, Karnataka is witnessing a boom in digital activity, online transactions, e-commerce, and smartphone usage, all of which might be expressed in increased cybercrimes.
2. Enhanced Reporting and Awareness: A more efficient system of reporting cybercrimes and greater awareness can be the factors behind the state's rise in cases.
3. Heightened Targeting: With the population of internet-conscious individuals and online businesses, technological hubs tend to attract more traffic of cybercrime.

Uttar Pradesh follows with a high of 10,117 cases in 2022.

1. Urbanization and Digital Penetration: The scope for cybercrime rises in Uttar Pradesh with more individuals being exposed to digital platforms and the internet.

2. Gigantic Population: Cybercriminals find more scope to exploit a gigantic population base, thus increasing crime rates.

Maharashtra also witnesses a high incidence of cybercrimes with 8,249 cases in 2022:

1. Financial and commercial Center: Maharashtra, especially Mumbai, is India's financial and commercial center. E-commerce, digital business, and online financial transactions can provide an environment in which cybercriminals can work.
2. Large Population and Increased Internet Use: Maharashtra is exposed to cyberattacks more due to its large and well-connected population.

Telangana is one of the other states where significant increases (from 1,205 cases in 2018 to 15,297 cases in 2022) have been seen.

1. Increased Digital Connectivity: Telangana's IT infrastructure, especially Hyderabad and other urban areas, has substantially increased. There is a higher incidence of cybercrime owing to this increased connectivity.
2. Increased Transactions and Internet Usage: Cybercriminals have more opportunities due to the increase in social media, online banking, and digital transactions.
3. Improved Reporting Mechanism: The dramatic increase in cases could be accounted for by an increase in the state's awareness and reporting of cybercrimes.
4. The state of Andhra Pradesh has witnessed 1207 cybercrime cases in 2018 and 2341 in 2022.

States where Cases of Cyber Crime Decreased:

The instances drop in Arunachal Pradesh to a large extent from 30 in 2020 to merely 14 in 2022. Manipur's dipped from 79 in 2020 to 18 in 2022. Mizoram saw its cases dipping from 13 in 2020 to 1 in 2022.

States with Steady or Moderate Growth:

Over time, there has been a steady increase in cases in states such as Kerala and Haryana. The number of individuals in Punjab has grown steadily from 239 in 2018 to 697 in 2022.

Union Territories with Significant Trends:

Delhi showed a significant increase from 189 cases in 2018 to 685 cases in 2022.

1. Technological Development: Delhi's high degree of digital activity as the capital of the country might offer more scope for cybercriminals.
2. Government and Business Hub: This region is a good location for cybercrimes because it is where the government and major corporations are located, making it easier for cybercriminals to target the public and private sectors.
3. Awareness and Reporting: More incidents are likely to be reported as individuals become more knowledgeable about cybercrime.

Jammu and Kashmir's cases have also grown from 73 in 2018 to 173 in 2022. Zero in 2021 to sixty-four in 2022 represented Puducherry's unbelievable growth. Only five in 2022, D&N Haveli and Daman and Diu, have comparatively very low figures overall.

Increase in Cyber Crime Cases in the Nation:

Over a span of five years, the number of cases has increased by approximately 141.3%, from 27,248 in 2018 to 65,893 in 2022. Various variables, including increasing digitization, increased online transactions, and greater usage of smartphones and Internet services, could be responsible for the increase in instances of cybercrime. These factors may provide further opportunities for cybercrime prevention.

State/UT Trends:

The major states with the highest reporting of cases were Andhra Pradesh, Karnataka, Uttar Pradesh, Maharashtra, and Telangana. The lesser numbers are by minor states and union territories (UTs), such as Sikkim, Lakshadweep, and Mizoram; for instance, Sikkim had a very insignificant occurrence (26 in 2022). There are several reasons for this minor number of cybercrimes.

1. Less Population Density: Owing to the small number of inhabitants, the small states and UTs obviously possess lesser possibilities of cybercrime.
2. Shorter Digital Infrastructure: As low Internet accessibility and reduced online payments lead to shorter possibilities of cyberspace attacks for culprits, culprits have shorter options here too.
3. Less Reporting: Not just shortening, possibly their weak or non-existent mechanisms in understanding how or reporting, to get awareness that has, too, lesser repercussions.
4. In particular, Telangana and Karnataka's very high case increases are indicative of increased cybercrime, which could be induced by increased numbers of people on the Internet, higher populations, or better reporting mechanisms.

Conclusion:

The states that have high rates of urbanization, digitization, and technologically advanced people are Karnataka, Telangana, and Maharashtra. These states also show an increasing trend in cybercrime. Increased awareness: More cases have been recorded due to greater awareness of cybercrimes, mainly in larger states and cities. Computerization of smaller States: Cybercrime offenses are starting to increase significantly even in smaller states such as Puducherry (from 0 to 64 cases in 2022), showing the ubiquity of cyber-crime. Underreported Smaller States: Due to lower rates of Internet penetration, cybercrimes might not be as prevalent in smaller states and union territories such as Mizoram and Lakshadweep, or they might not be reported. Based on this data, cybercrimes are becoming a larger issue in India, especially in urbanized areas such as Karnataka, Telangana, and Maharashtra, which have good Internet connectivity. Instead of an actual increase in criminal activity, the increase in cybercrime cases in certain states may be an outcome of better reporting methods or greater awareness. To combat these crimes, however, this also highlights the need for a stronger cyber security infrastructure, awareness campaigns, and police operations.

Acknowledgement
I am Dr. Amuksiddha Shrimant Pujari, Assistant Professor of Commerce at Dr. Patangrao Kadam Arts and Commerce College, Pen. Tal. Pen, Dist. Raigad, thankful to Dr. Murlidhar Wagh, HOD, and the I/C Principal of Dr. Patangrao Kadam Arts and Commerce College, Pen. Tal. Pen, Dist. Raigad for granting permission to conduct work. I am thankful to Shri. Mangesh Bhitre Librarian at our college for giving me access to library resources in research work. I am also grateful to the IQAC and Research Committee of my college for their guidance and cooperation in research activities.

References:

1. https://financialservices.gov.in
2. https://cybercrime.gov.in
3. Lerner, K. L., & Lerner, B. W. (Eds.). (2005). Computer security and computer crime investigation. In *World of forensic science* (Vol. 1, pp. 164-166). Gale.
4. Marimon'd., & Hunt, D. E. (2020, February). Cybercrime investigations and prosecutions. In *Oxford bibliographies*. Oxford University Press. https://doi.org/10.1093/OBO/9780195396607-0276
5. Richards, J. (2018, January). Cyber warfare. In *Oxford bibliographies*. Oxford University Press. https://doi.org/10.1093/OBO/9780199743292-0076
6. Rogers, M. K. (2010). Cyber forensics. In J. G. Voeller (Ed.), *Wiley handbook of science and technology for homeland security* (Vol. 2, pp. 1009-1021). Wiley.
7. Abbott, K. W. and Snidal, D. (2000). Hard and soft law in international governance. International Organization, 54, 421–56. Cross Ref (Google Scholar)
8. Bryant, R. (2008). The challenge of digital crime. In Bryant, R. (ed.), Investigating Digital Crime. Chichester, UK: John Wiley and Sons (pp. 1–26).Google Scholar
9. Cronan, T. P., Foltz, C. B. and Jones, T. W. (2006). Information systems misuse and computer crime: an analysis of demographic factors and awareness of university computer usage policies. Communications of the ACM, 49 (6), 84–90.Google Scholar
10. ANNEXURE-I, R.S. US.Q.NO. 234 FOR 27.11.2024, Ministry of Home Affairs, Rajya Sabha, Government of India.
11. Crime in India (Combined data of erstwhile D&N Haveli UT and Daman & Diu UT for 2018, 2019*'Data of erstwhile Jammu & Kashmir State including Ladakh for 2018, 2019)