International Journal of Finance and Commerce
www.commercejournals.com
Online ISSN: 2664-715X
Received: 29-12-2025, Accepted: 28-01-2026, Published: 12-02-2026
Volume 8, Issue 1, 2026, Page No. 53-55

Cyber banking frauds in India: An overview

Thakur Vijay Kumar Munna
Research Scholar, Department of Commerce and Business Administration, Lalit Narayan Mithila University, Darbhanga, Bihar, India

Abstract
Banking system in the modern times have become the backbone of any economy and the need for quality banking with robust risk management has been the concern of not just economists but also the legislators. One of the biggest problems in recent times has been that of Banking Frauds, both internal and external, and many laws and regulations have been enacted. Fraud has been broadly defined in various laws to include deliberate acts to cause either unlawful gain to oneself or unlawful loss to another. However, banking fraud has not been specifically defined, resulting in difficulties at the enforcement level, due to the multitude of activities that may be encompassed within its ambit.
The digital frauds rate is highly significant in banking sector which causes the loss of money by the public and hamper the public confidence on the digital banking and entire banking sector. However, still banking sector failed in recovery of money and detecting and preventing the accounts of frauds. There is inadequate research studies focused on the types of frauds exposed by the public, pushing factors towards becoming of victims of the banking frauds, examining the impact of banking online frauds on the victim's economic status and reactivation rate of digital banking after experience of frauds.

Keywords: Cyber crime, cyber security, cyber trespass, hacking, indian banking sector

Introduction
Financial stability lies at the heart of a nation's economic strength- and for India's banks, it remains the unwavering North Star. As the world's fourth-largest economy, India's financial sector has evolved into a resilient and dynamic force, ready to power the country's growth ambitions and investment needs. Over the past two and a half decades, India's banking system has undergone a remarkable transformation- from the early days of ATM networks to the emergence of RTGS, NEFT, IMPS, and the revolutionary UPI, now extending its frontier to digital currency. This steady march of innovation has reshaped how India transacts, saves, and invests. Today, the banking sector stands stronger than ever- with robust capital and liquidity buffers, improved asset quality, and sustainable profitability. The resilience of public sector banks (PSBs) and scheduled commercial banks (SCBs), reflected in their high-quality capital, declining loan losses, and solid earnings, underscores their capacity to finance growth while withstanding shocks.
As a result of the Government's strategy of recognition, resolution, recapitalisation and reforms, gross NPA ratio have since declined to ₹2,73,413 crore (gross NPA ratio of 2.79%) as on 31st March 2025. Further, as per RBI data on domestic operations, stressed assets, including restructured standard assets, as percentage of gross advances in SCBs has declined from 9.8% as on 31st March 2014 to 3.55% as on 31st March 2025.
The Indian banking industry has seen robust growth, driven by strong economic expansion, rising disposable incomes, growing consumerism, and easier credit access. Digital modes of payments, dominated by UPI, have grown by leaps and bounds over the last few years. As per the RBI, India's banking sector is sufficiently capitalized and well-regulated. Notably, profitability of banks improved for the sixth consecutive year in 2023-24. Building on their strong financial performance and improved asset quality, Indian banks are now focusing on sustaining growth through innovation, inclusion, and strategic expansion.

Concept and Meaning of Cyber Crime
Cybercrime is defined as any criminal activity which takes place on or over the medium of computers, or internet or, other technology recognized by the Information Technology Act. Cybercrime is the most prevalent crime playing a devastating role in the banking domain. It is a problem banks have been facing since the advent of e-commerce in the 1990s, and its threat only increases with each passing year. All of these threats have potentially serious financial, legal and reputational implications. Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor.
However, some banks could develop more sensitive burglar alarms, so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system. The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, be likely to be the most carefully secured. Complex encryption software is used to protect account Information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities.
A primary effect of cybercrime is financial. Cybercrime can include many types of profit-driven criminal activity, including ransomware attacks, email and Internet fraud, identity fraud, and attempts to steal financial account, credit card or other payment card information. Cybercriminals may target an individual's private information or corporate data for theft and resale. As many workers settle into remote work routines due to the pandemic, cybercrimes are expected to grow in frequency in 2023, making it especially important to protect backup data.

Cyber Banking Frauds in India

Every day, fraudsters are trying to think of new and innovative ways of tricking innocent customers. Therefore, there is dire need to be aware and never give out any personal or banking account details. In order to keep all up to date with the various kinds of cyber frauds, we present o comprehensive list of such frauds reported to Indian Banks so far. These are as follows:

- **Networks:** The word botnet is made from two words robot and network. A cyber-crime is called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control a group of computers too remotely.

- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account.

- **Cracking:** It is a dreadful feeling to know that a stranger has broken into user computer systems without user's knowledge and consent and has tampered with precious confidential data and information. A Cracker differs from the hacker because hacker is hired by companies to audit network security or test software but cracker do the same work for their own profit or to harm others.

- **Cross-site Scripting:** Cross-Site Scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefined access permissions of website. Reflected XSS is the non-persistent XSS. Scripting languages like java script, VB script etc. are used for Reflected XSS attack.

- **Cyber Crime and Social Networking:** Cyber criminals use social media for not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms.. This risk is associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. To protect one self, get to know the security and privacy settings, and configure them to protect from Identity theft. One in five online. Adults (21 percent) have reported of becoming a victim of either social or mobile cybercrime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

- **Cyber Squatting:** Squatting is the act of occupying an abandoned or unoccupied space. Cyber-squatting is the act of registering a famous domain name and then selling it to needy for a high cost. It means where two persons claim for the same Domain Name either by claiming that they had registered the name first or by right of using it before the other or using something similar to that previously.

- **Cyber stalking:** Online harassment and online abuse all comes under stalking. The term "stalking" generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Cyber stalking shares important characteristics with offline stalking. Many stalkers (online or offline) are motivated by a desire to control their victims. A major damaging effect of online abuse is a victim avoiding his/her friends, family and social activities.

- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons through Internet. Trafficking in the cyberspace is also a gravest crime.

- **Cyber Trespass:** It means to access someone's computer without the proper authorization of the owner without disturbing, altering, misusing, or damaging data or system by using wireless internet connection.

- **Cyber Vandalism:** Vandalism means destroying or damaging property of another. Thus cyber. Vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.

- **E-Mail/SMS Spoofing:** A spoofed E-mail/SMS may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates. Here an offender steals identity of another in the form of email address, mobile phone number etc. and send the message via internet.

- **Hacking:** In general, the word 'hacking' means seeking and exploiting weakness and security of a computer system or a computer network for unauthorized access. The person who does hacking is known as hocker. A Hacker uses his/her computer expertise and some tool or scripts to hack any computer system.

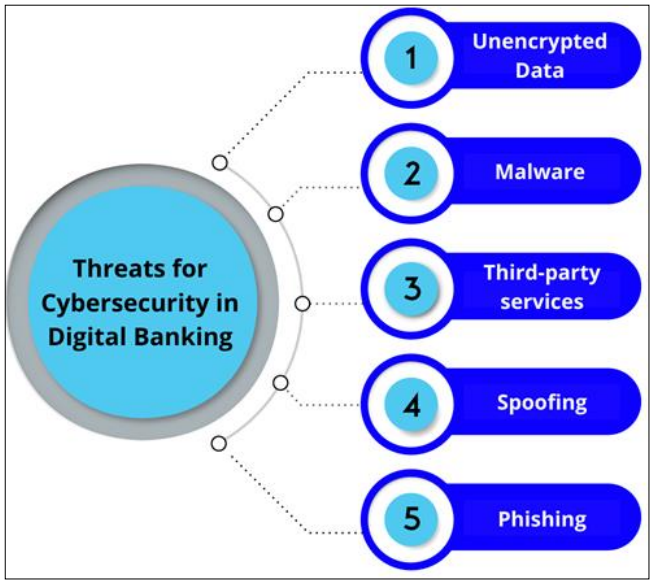
- **Intellectual Property Crimes:** Intellectual property consists of a person's creations such as articles, books, paintings, photos or any such intellectual content. Any unlawful act by which on owner of such intellectual property is deprived completely or partially of his rights is an offence and this is known as intellectual property crime. The common form of IPR violation/crime may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's Internet Service Provider given user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the person's knowledge.

- **Phishing:** It is an attempt to 'fish' for your banking details. Phishing could be an e-mail that appears to be from a known institution Uke banks / a populor website. Please note that banks will never ask for

confidential data like login and transaction password, One Time Password (OTP) etc.

- **Voice Phishing:** The term is a combination of "voice" and "phishing". Voice phishing is used to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.



Summing-up

The risk of fraud is rising daily along with the use of internet banking. People today are more educated than in the past, therefore their lives are more machine-oriented and they have less time than ever before to visit a bank branch. When a consumer has access to an internet-connected computer, they can do their business without having to go to a bank branch. Simply put, if they have an internet connection, they can transact anytime, anyplace. Customers can obtain a range of services, such as a request for a cheque book or a balance query, by dialling the telebanking number. While a significant portion of fraud cases were advance-related, approximately 65% of all fraud cases reported by banks were technology- related frauds (covering frauds committed through ATMs, internet banking channels, and other payment channels like credit, debit, and prepaid cards). Due to these factors, it is imperative that one studies the risks associated with online banking. These include negligent bank management, fraud using a QR code. The main causes are attacks involving phishing, smishing, or vishing. One must be aware of these issues and act as soon as possible to combat fraud and awareness. To do this, one must conduct training programmes for fraud awareness improvements in policies. Without the survey, it would be impossible to identify the full scope of the online banking fad, which is why it is important. Finding the cause of various types of fraud allows one to take action to manage or prevent them. Consequently, it is vital to thoroughly research Online Banking Fraud Risk and Awareness.

Security, as well as privacy issues, could be dealt with to a greater extent by the use of global counters, global analysis, and differential analysis. The likelihood of fraudsters accessing the portal could also be detected beforehand and the overall threat could be minimized. Other mechanisms can be adapted along with data mining principles namely pattern mining, neural networks, and decision forest. This proves that if IT brings to us cybercrimes, it also brings us the prevention tactics for securing ourselves from such crimes. Finally, technology administration risks tend to decrease with organizational flexibility, staff training and awareness, and support from the top officials to provide a transparent, satisfying working environment based on legal and ethical values. These are perceived inputs for reducing collision among employees so as to reduce banking frauds.

References

1. Chaturvedi SK, Baranwal S. Cyber Crimes: Issues, Policy, Regulations and Developments. Satyam Law International, New Delhi, 2023.
2. Gupta R, Das S. Insider Fraud in Indian Banks: A Critical Analysis. International Journal of Banking Studies,2020:4(1):33-48.
3. Mallesha C, Govardhan M. A Study of Cyber Crime on Banking Sector in India. International Journal of Innovative Research in Technology,2024:11(2):2076-2082.
4. Nainta RP. Banking System, Frauds and Legal Control. Deep and Deep Publications Pvt. Ltd., New Delhi, 2005.
5. Patel AD. New Challenges in Banking Fraud: A Social-legal Analysis in India. Sarvalokum-Law and Society,2024:1(1):1-14.
6. Saroja AVBNH, Radhika R. A Study on Cyber Frauds in India Banking Sector. International Journal of Applied and Advanced Scientific Research,2018:3(1):315-321.
7. Sharma A. Cyber Fraud in Indian Banking: Challenges and Solutions. Journal of Financial Security,2019:7(2):145-162.
8. Sharma BR. Bank Frauds: Prevention and Detection. Lexis, Gurgaon, 2016.
9. Singh V. Regulatory Reforms in Indian Banking: Towards Combating Frauds. Journal of Economic and Legal Regulations,2021:18(4):87-104.
10. Soni L, Mangala D. A Thorough Analysis of the Literature on Banking Sector Frauds. Journal of Financial Crime,2023:30(1):285-301.
11. www.acfe.com
12. www.iibf.org.in
13. www.legalserviceindia.com
14. www.rbi.org.in
15. www.voiceofresearch.org