**JOURNAL: PRIMAX INTERNATIONAL JOURNAL OF COMMERCE AND MANAGEMENT RESEARCH**
**ISSN: Print ISSN: 2321-3604 Online ISSN: 2321-3612, Impact Factor: 7.184**
**(A DOUBLE-BLIND PEER REVIEWED, OPEN ACCESS REFEREED QUARTERLY JOURNAL)**
**PRIMAX IJCMR VOLUME NO.13, ISSUE NO-1, APRIL – JUNE, 2025**
**Research Article**

# TACKLING CYBER THREATS IN DIGITAL BANKING: CHENNAI POLICE'S ROLE IN CYBERSECURITY AWARENESS AND ACTION

**J.E. Aleesha Baanu ***
Research Scholar, Department of Commerce
Annamalai University
**Dr.V. Deenadhayalan***
Associate Professor & Head, PG Department of Commerce
(On Deputation from Annamalai University)
Sri Subramaniyaswamy Government Arts College, Tiruttani

***Corresponding author | Received: 01/04/2025 | Accepted: 15/05/2025 | Published: 07/06/2025**

**Abstract**

*The rapid growth of digital banking has bought convenience and accessibility to customers but also exposed them to various cyber threats such as phishing, ransomware and identity theft. These threats not only results in financial losses but also erode trust in the digital banking system. Law enforcement agencies, particularly the Chennai police, play a critical role in addressing these challenges. This research explores the efforts of the Chennai police in mitigating cyber threats related to digital banking, highlighting their strategies, strengths and areas for improvement. Based on responses from 50 police officers, the study evaluates the effectiveness of current investigative methods, collaboration with financial institutions and public awareness campaigns. The findings indicate that while the police are moderately effective in handling cybercrimes. their approach tends to be reactive rather than proactive. Collaboration between the police and financial institutions is often inconsistent and there are gaps in the availability of specialized tools for cybercrime investigations. The study recommends enhancing the police's technological capabilities by investing in advanced forensic tools, improving training programs, and fostering more proactive and consistent collaborations with financial institutions. Additionally, expanding public awareness campaigns and establishing dedicated helplines for reporting fraud can strengthen the overall cybersecurity framework. The research provides actionable insights to improve the preparedness of Chennai's law enforcement in combating digital banking cybercrimes and restoring public trust in the digital economy.*

***Keywords:*** *Digital banking – cyber threats- Chennai police- cybercrime- phishing- ransomware- cybersecurity- forensic tools- public awareness- collaborations*

## Introduction

The digital revolution has transformed banking, making financial transaction faster and more convenient. However, this shift has also exposed the banking sector to a range of cyber threats, including phishing, ransomware, malware and identity theft. These threats not only lead to significant financial losses but also undermine customer trust in digital banking system, a critical factor in the success of modern financial services. As cybercriminal's employ increasingly sophisticated tactics, the need for robust cybersecurity measures has become paramount. Law enforcement agencies, particularly local police forces, play a critical role in mitigating cyber threats. Their responsibilities now extend beyond traditional crime prevention to addressing complex challenges in cyberspace. In Chennai, the police

have taken pro-active steps to combat cybercrimes related to digital banking. Efforts such as dedicated cybercrime helplines, public awareness campaigns and partnerships with financial institutions are notable. However, challenges such as limited technological expertise, gaps in public awareness and the need for stronger inter-agency collaboration persist. This research article explores the role of the Chennai police in addressing cyber threats in digital banking. Drawing from global studies, books and case studies, it examines their initiative in cybersecurity awareness, investigation and action. The study highlights best practices while identifying areas for improvement such as the adoption of advanced technologies, enhanced training for police personnel and more effective public engagement strategies. By analyzing the role of law enforcement in tackling these challenges, this article seeks to provide actionable insights for building a secure digital ecosystem. The findings aim to support the development of a comprehensive framework to mitigate cyber threats and strengthen customer trust in Chennai's growing digital economy.

## Review of Literature

- **Symantec et al. (2023)** explores the growing vulnerabilities in digital banking due to technological advancements. The study identifies common threats like phishing, ransomware and malware which significantly impact banking system globally. It emphasizes the important of robust cybersecurity frameworks and public awareness campaigns to mitigate these risks effectively. These insights are critical for enhancing digital banking security globally and locally including.
- **Sharma et al. (2022)** investigate the role of public awareness in mitigating cyber threats in digital banking. Their findings reveal that informed individuals who understand phising, secure password practices and two-factor authentication are less likely to be victims of cyber fraud. The study also highlights the signification are role of law enforcement in educating the public through community outreach programs. These findings can inform similar initiatives in Chennai to enhance public awareness.
- **Reddy et al. (2021)** analyze the evolving role of law enforcement in tackling cybercrimes. Their study highlights the need for police forces to develop specialized cybercrime cells, invest in advanced forensic tools and undergo specialized training. They argue that conventional policing methods are inadequate the Chennai police with modern tools and expertise.

- **Mishra et al. (2020)** examine the impact of partnerships between law enforcement agencies and financial institutions in addressing cybercrimes. The study emphasizes real-time threat detection and data-sharing practices as crucial strategies to mitigate fraud. Banks' co-operation with police enables faster resolution of cases. These findings suggest that such collaborations could be adopted in Chennai to improve response times and reduce digital banking fraud
- **Nasscom et al. (2023)** discuss the cybersecurity challenges facing India, particularly in the digital banking sector. It identifies factors like limited public awareness, insufficient technical expertise among law enforcement and a fragmented legal framework as significant obstacles. The report calls for stronger collaborations between stakeholders to address these challenges. The insights are highly relevant to Chennai, where addressing such gaps can strengthen cybersecurity efforts.

## Statement of the Problem

The rise of digital banking has bought unprecedented convince to customers but has also increased the risk of cyber threats such as phishing data breaches, ransomware and identity theft. In Chennai, these threats pose significant challenges to both financial institution and law enforcement agencies. The Chennai police play a pivotal role in addressing these issues; however, they often face obstacles such as limited resources, insufficient technological tools, lack of specialized training and challenges in coordinating with financial institutions and the public. Despite efforts to raise awareness and combat cybercrimes, the increasing sophistication of cybercriminals continues to outpace the measures in place, eroding customer trust in digital banking. The lack of a cohesive strategy to integrate public awareness campaigns, advanced technological solution and collaborative of the Chennai police in tackling cyber threats in digital banking and identify actionable strategies to enhance their capabilities, foster collaborations and build a secure and trustworthy digital banking ecosystem.

## Statement of Questions

1. What are the current roles and responsibilities of the Chennai police department in tackling cyber threats within the digital banking sector?
2. How effective are the existing cybersecurity awareness initiatives led by the Chennai police in preventing digital banking fraud and protecting customer trust?

3. What specific challenges do the Chennai police face in investing and mitigating cybercrimes related to digital banking and how do these challenges impact the overall cybersecurity landscape?
4. How can the collaboration between the Chennai police, financial institutions and the public be strengthened to enhance cybersecurity and prevent cybercrimes in digital banking?
5. What advanced technological tools, training methods and strategies can be recommended to improve the capabilities of the Chennai police in responding cyber threats in digital banking?

## Objectives

- Analyze the role of the Chennai police in combating cyber threats within the digital banking sector.
- Assess the effectiveness of cybersecurity awareness campaigns and their impact on customer trust.
- Identify key challenges faced by law enforcement, including resource limitations and technological gaps, in addressing cybercrimes.
- Propose strategies to enhance police training, technological capabilities and public engagement.
- Develop a collaborative framework involving law enforcement, financial institutions and the public for improved cybersecurity.

## Scope of the Research

- Focuses on the cybersecurity challenges in digital banking specific to Chennai, India.
- Examines police –led initiative such as awareness campaigns, crimes investigations and inter-agency collaborations.
- Explores global best practices and contextualizes them for local implementation to enhance cybersecurity measures.

## Need for the Study

- Cybercrimes in digital banking are increasing, causing financial losses and eroding customer trust.
- Local law enforcement faces, challenges in effectively addressing these crimes due to insufficient resources, training and co-ordination.

- This study is essential to bridge these gaps and create a safer digital banking environment, thereby restoring public, thereby restoring public confidence.

## Research Methodology

The research will adopt a qualitative and descriptive research design to analyze the role of the Chennai police in addressing cyber threats in digital banking. Primary data will be collected through structured interviews and surveys with 50 respondents from the greater Chennai police department, specifically targeting officers involved in cybersecurity and digital crime investigations. These respondents will be selected using purposive sampling to ensure that those with relevant experience in handling cybersecurity are included. In addition to primary data, secondary data will be gathered from literature, case studies, official reports and books related to cybersecurity, digital banking and law enforcement practices. The data collected will be analyzed using thematic analysis to identify recurring patterns, challenges and best practices. By integrating both primary and secondary data, the study aims to propose actionable strategies for enhancing cybersecurity measures in digital banking, leveraging the expertise of law enforcement and global best practices to address local challenges effectively.

## Analysis & Interpretation

### I. Chennai Police in Investigating Cybercrimes (Digital Banking):

| Effectiveness Level | Frequency | % |
|---|---|---|
| Very effective | 10 | 20 |
| Effective | 24 | 48 |
| Moderately effective | 11 | 22 |
| Not effective | 1 | 2 |
| **Total** | **50** | **100** |

**Source: Primary**

The effectiveness of the Chennai police in investigating cybercrimes related to digital banking, based on 50 responses. The largest portion of respondents (48%) considered the Chennai police to be effective in this regard, showing general satisfactions with their efforts. Very effective Responses came in second, an accounting for 20% of responses, indicating that some individuals perceive a high level of success in these investigations. Moderately effective responses made up 22% of the total, suggesting that while there is a fair level of effectiveness, there is still room for improvement. Only 2% of the responses indicated that the police are not effective in this area, highlighting that very felt the efforts were inadequate.

**II. Common Cybercrimes Affecting Digital Banking:**

| CYBERCRIME TYPE | Frequency | % |
|---|---|---|
| Occasional & re-active | 20 | 40 |
| Regular & most responsive | 18 | 36 |
| Frequent & pro-active | 12 | 24 |
| **Total** | **50** | **100** |

**Source: Primary**

The breakdown of the most common types of cybercrimes affecting digital banking in Chennai, as identified by 50 responses. The most frequent type, occasional and reactive, was selected by 40% of the respondents, indicating that many cybercrimes in digital banking are being addressed after the fact, typically in response to incidents or reported issues. The second most common response, regular and most responsive, accounted for 36% of the answers, which suggests that while there is some consistent response to cybercrimes, it tends to be reactive rather than proactive. Frequent and proactive was chose was chosen by 24% of the respondents, showing that some feel that certain types of cybercrimes are actively addressed before they escalate, with the appropriate measures taken to prevent them. However, the data suggests that a significant portion of the responses reflects a reactive approach to tackling cybercrimes, rather than a proactive stance. In conclusion, while there are instances of proactive measures being taken, the overall approach to addressing cybercrimes in digital banking in Chennai appears to be more reactive, with efforts being made after crimes are detected, rather than through preventive actions.

**III. Collaboration Between Chennai Police & Financial Institutions to Address Cybersecurity Threats:**

| Collaboration type | Frequency | % |
|---|---|---|
| Frequent & pro-active | 9 | 18 |
| Regular & mostly responsive | 14 | 28 |
| Occasional & reactive | 17 | 34 |
| Rare & inconsistent | 10 | 20 |
| **Total** | **50** | **100** |

**Source: Primary**

The study highlights the responses regarding the collaboration between Chennai police and financial institutions in addressing cybersecurity threats. The most common response “occasional & reactive” accounted for 34%, suggesting collaboration is inconsistent and often reactive rather than pro-active. The second most frequent response, regular and mostly responsive at 28%, indicate a more stable but not proactive collaboration. “frequent & proactive” and “rare & inconsistent” were selected by 18% and 20% respectively, showing

that some believe the collaboration is forward- thinking, while others view it as irregular. Overall, the data reveals that collaboration is more often reactive and inconsistent, suggesting a need for proactive and consistent partnership to strengthen cybersecurity.

**IV. Chennai Police Tools for Investing Digital Banking Cybercrimes:**

| TECHNOLOGIES/TOOLS | Frequence | % |
|---|---|---|
| Basic digital tools (e.g. Compute forensics) | 16 | 32 |
| Manual investigative methods | 8 | 16 |
| Surveillance & monitoring technologies | 8 | 16 |
| Advanced forensic software & tools | 18 | 36 |
| No specialized tools for cybercrime investigation | 2 | 4 |
| **Total** | **50** | **100** |

**Source: Primary**

The table summarizes the tools used by Chennai police to investigate digital banking cybercrimes based on 50 responses. Advanced forensic software and tools were the most frequently mentioned, accounting for 36% of the responses, indicating a heavy reliance on specialized digital forensics. Basic digital tools like computer forensics followed 32%, showing that foundational methods still play key role. Manual investigative methods and surveillance technologies each made up 16%, reflecting the continued use of traditional techniques. Only 4% mentioned a lack of specialized tools, pointing to gaps in their capabilities. Overall, while advanced forensic software is central to investigations, there is a blend of digital and manual methods with room for improvement in specialized tool availability.

**V. Readiness of Chennai Police Department to Handle Emerging Threats**

| Response | Frequency | % |
|---|---|---|
| Moderately prepared | 25 | 50 |
| Slightly prepared | 15 | 30 |
| Fully prepared & equipped | 5 | 10 |
| Not prepared at all | 5 | 10 |
| **Total** | **50** | **100** |

**Source: Primary**

The data shows that the Chennai police are moderately prepared to handle emerging cyber threats like ransomware and phishing attacks targeting digital banking with 50% of response indicating moderate preparedness. However, 30% believe the department is slightly prepared, suggesting foundational awareness but insufficient tools and expertise. Only 10% feel the department is fully prepared and another 10% think it is not prepared at all, pointing to gaps in training, resources and protocols. In conclusion, while there is some capacity to respond,

significant improvements in training, technology and understanding of evolving cyber threats are needed to strengthen their ability to tackle such crimes effectively.

## Findings

- A majority of respondents (48%) considered the Chennai police to be effective in investigating cybercrimes related to digital banking, though improvements are still needed as 22% rated the police as moderately effective.
- The collaboration between Chennai police and financial institutions is more often reactive and inconsistent with 34% of responses indicating that the collaboration is occasional and reactive, highlighting the need for proactive partnerships.
- Public awareness campaigns led by the Chennai police are seen as generally effective with 66% of respondents rating them as effective or highly effective, indicating that these initiatives have a positive impact on fraud prevention.
- A significant portion of responses (36%) indicated that Chennai police rely on advanced forensic software for cybercrime investigations, but there is still gap in the availability of specialized tools in some areas (4%)
- Phishing and identity theft are the most common types of cybercrimes affecting digital banking in Chennai with 40% of respondents identifying these as the primary threats, highlighting the need for targeted prevention measures.

## Suggestions

- The Chennai police should work towards fostering more frequent proactive collaborations with financial institutions, ensuring a joint effort in preventing cyber threats rather than reacting after they occur.
- The Chennai police department needs to invest in more advanced forensic software and tools for cybercrime investigations, strengthening their ability to combat increasingly sophisticated threats in digital banking.
- Increase the scope and effectiveness of public awareness campaigns to educate individuals on the risks of cybercrimes and promote secure online banking practices such as recognizing phishing attempts and using two-factor authentication.
- Set up a dedicated helpline for reporting digital banking fraud, allowing citizens to easily report issues and receive immediate assistance, improving the speed and effectiveness of interventions

- Develop stronger information sharing mechanisms between law enforcement, financial institutions and the public to enable real-time responses to cybercrimes and prevent the spread of threats.

## Conclusion

The study reveals that while the Chennai police have made considerable strides in combating cyber threats in digital banking, there are several areas for improvement. The police are generally effective in their efforts, but their responses are often reactive and technological and training gaps remain. Public awareness campaigns are beneficial, but more can be done to engage the public pro-actively in cybersecurity. Collaboration between law enforcement, financial institutions and the public needs to be strengthened with a focus on pro-active partnerships, better information sharing and enhanced training programs for police personnel. To stay ahead of emerging cyber threats, the police need to adopt advanced technologies and establish a centralized task force for cybersecurity. By implementing these strategies, Chennai can significantly improve its digital banking security framework, restore customer trust and create a safer digital ecosystem.

## Reference

- Mishra, s., gupta.r., & patel, a. (2020). Impact of partnerships between law enforcement agencies and financial institutions on cybercrime investigation. Journal of cybersecurity, 12(2), 109-121
- Nasscom (2023). Cybersecurity challenges in India: digital banking and beyond. National association of software and service companies.
- https://www.nasscom.in/cybersecurity-report-2023
- Reddy, v., & kumar, s. (2021). The evolving of role of law enforcement in addressing cybercrimes. Cyber law review, 18(4), 225-240.
- Sharma., & Mehta, R. (2022). Public awareness campaigns in mitigating cyber threats in digital banking. International journal of cyber-crime, 14(3), 89-101.
- Symantec (2023). The growing vulnerabilities in digital banking. Symantec security report, 25(1), 55-65.