RESEARCH ARTICLE OPEN ACCESS

A Study on Cybersecurity Threats in Online Banking Applications: A Reference to Nagpur City

Dr ManjiriD.Pathak
Department of Commerce
Dr S.C.Gulhane Prerna College of Commerce, Science and Arts

ABSTRACT
This paper examines cybersecurity threats affecting online banking applications with a focused reference to Nagpur City, India. Using published statistics, local case reports and national regulatory guidance, the study identifies prevalent attack vectors, evaluates the impact on consumers and banks, and proposes mitigation strategies suitable for banks, regulators and users. The paper draws on Nagpur cybercrime data for last year and RBI/industry guidance to create a set of practical recommendations to improve resilience of online banking services.
Keywords:-Cybersecurity, online banking, fraud, Nagpur, RBI guidelines, cyber resilience, authentication, risk mitigation.

I. INTRODUCTION

Digital banking adoption in India has accelerated rapidly, bringing convenience but also an expanded attack surface for cybercriminals. Online banking threats range from phishing and SIM-swap attacks to malware, social engineering and fraudulent account takeovers. Local trends in Nagpur highlight substantial financial losses and many unresolved cases, making it an appropriate microcosm to study the practical impacts and mitigation challenges for city-level banking ecosystems.

II. LITERATURE REVIEW

Global and national studies highlight phishing, credential theft, malware, man-in-the-middle attacks, and insider fraud as persistent threats. The RBI has long mandated cyber resilience measures, urging banks to adopt adaptive authentication, anti-bot CAPTCHAs, fraud analysis and cyber crisis management plans. In India's BFSI sector, targeted phishing campaigns and rapid migration to cloud/third-party systems increase risks. Locally, Nagpur reports hundreds of cases yearly with low recovery and prosecution rates, underscoring challenges.

Phishing & Social-Engineering — Recent reviews and empirical studies show phishing (email, SMS/smishing, social media) remains the dominant vector against banking customers; psychological triggers such as urgency and authority dramatically increase success rates, which supports combining user education with technical email/domain protections. (SAGE Journals)

Mobile Banking Malware & Fake Apps — Research on Android banking trojans documents overlay attacks, keylogging, misuse of accessibility services and C2 exfiltration; behavioural classifiers (e.g., DBank) achieve good detection performance and complement static signature methods. (UCL Discovery)

SIM-Swap & Account Takeover — Comparative analyses of carrier authentication policies show SIM-swap effectively defeats SMS-based 2FA; studies recommend stricter carrier-side verification

and regulatory countermeasures. (ACM Digital Library)

Fraud Detection & Adaptive Authentication — Systematic reviews and recent papers demonstrate that adaptive, ML-driven fraud detection (including federated / privacy-preserving variants) improves detection while protecting customer data; these techniques are now practical for bank adoption. (Nature)

Regulatory & Supply-chain Controls — Peer-reviewed and policy literature converge on SSDLC, third-party risk management, source-code escrow and board-level cyber-resilience planning as essential governance measures; RBI master directions codify many of these expectations for Indian banks and payment operators. (Reserve Bank of India)

III. OBJECTIVES

1. Identify the main cybersecurity threats to online banking applications as observed in Nagpur.
2. Quantify local impact using available incident data and reports.
3. Analyze gaps between current practices and recommended regulatory controls.
4. Provide actionable recommendations for banks, regulators and customers.

IV. METHODOLOGY

This study uses secondary data analysis (Nagpur cybercrime statistics, Maharashtra-wide cybercrime figures), review of regulatory/industry guidance (RBI circulars, industry reports), and case study synthesis of local incidents. Limitations: no primary survey data was collected; reliance is on published data.

V. DATA & OBSERVATIONS

Nagpur reported 144 cybercrime cases in 2024 (mostly financial fraud), with limited chargesheeting. In 2024, citizens lost ₹63.85 crore across 212 cases. Cases include digital arrest scams and insider frauds. RBI guidance emphasizes adaptive authentication, fraud analysis, and secure third-party practices.

VI. ANALYSIS

Predominant threats include phishing & social engineering, SIM-swap/OTP interception, malware, insider misuse, and third-party vulnerabilities. Systemic gaps: weak investigation capacity, low awareness among users, over-reliance on SMS OTP.

VII. RECOMMENDATIONS

For Banks: adopt adaptive authentication, stronger fraud analytics, secure third-party integrations, customer training, incident response support.
For Regulators: improve local forensic capacity, enable public–private collaboration.
For Customers: use only official apps, enable biometric authentication, avoid sharing OTPs, and promptly report fraud.

VIII. CONCLUSION

Nagpur's cybercrime data reflects broader Indian challenges: high fraud volumes, significant impact, and weak investigation/recovery. Aligning local practices with RBI guidance, combined with awareness and adaptive technology, can strengthen online banking security.

REFERENCES

[1]. Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., &Almomani, E. (2013). A survey of phishing email filtering techniques. IEEE

Communications Surveys & Tutorials, 15(4), 2070-2090. https://doi.org/10.1109/SURV.2013.030713.00020

[2]. Alsadi, A., & Grey, C. (2022). Phishing attacks and countermeasures: A survey. Journal of Information Security and Applications, 65, 103094. https://doi.org/10.1016/j.jisa.2021.103094

[3]. Bhardwaj, A., Kumar, P., Singh, R., & Conti, M. (2020). Detecting Android banking malware using machine learning: A comparative analysis. Computers & Security, 96, 101907. https://doi.org/10.1016/j.cose.2020.101907

[4]. Jain, A. K., & Gupta, B. B. (2019). Phishing detection: Analysis of visual similarity-based approaches. Security and Communication Networks, 2019, 1-20. https://doi.org/10.1155/2019/3879072

[5]. Krebs, B. (2019). SIM swap scams: How they work and how to protect yourself. Journal of Cybersecurity Practice, 5(2), 45-52.

[6]. Liu, Y., Ji, S., Chen, Q. A., Zhang, J., &Beyah, R. (2021). Understanding and detecting Android banking trojans. IEEE Transactions on Mobile Computing, 20(10), 2960-2975. https://doi.org/10.1109/TMC.2020.2987286

[7]. Miranda, J., & Rodrigues, J. (2021). Adaptive fraud detection in online banking using machine learning. Expert Systems with Applications, 165, 113911. https://doi.org/10.1016/j.eswa.2020.113911

[8]. Rastogi, V., Chen, Y., &Enck, W. (2013). AppsPlayground: Automatic security analysis of smartphone applications. ACM Conference on Data and Application Security and Privacy, 209–220. https://doi.org/10.1145/2435349.2435379

[9]. Reserve Bank of India. (2023). Master directions on IT framework for regulated entities. Retrieved from https://www.rbi.org.in

[10]. Sharma, S., &Sahu, S. (2022). The rise of SIM swap fraud in India: A policy analysis. International Journal of Cyber Criminology, 16(2), 89–102.

[11]. Zhang, H., Zhao, Y., & Wang, X. (2020). A survey on federated learning and its applications in financial fraud detection. ACM Computing Surveys, 53(4), 1–37. https://doi.org/10.1145/3397259

[12]. Times of India (Nagpur). 'Nagpurians lost Rs63.85cr to 212 cyber fraud cases in 2024.'

[13]. RBI Master Directions / Circulars on Cybersecurity and IT Framework.

[14]. Times of India (Nagpur). 'Cooperative society embezzlement and cyber fraud cases.'