WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Emerging Trends in Digital Banking Fraud: A Case Analysis

Mr. Karthik Pai H[1], Ms. Niriksha Y M[2], Dr. Yathish Kumar[3]

[1]Research Scholar and Faculty, Dept. of Commerce, University College, Mangalore.
[2]LLM Student, CMR College, Dodda Banaswadi, Bengaluru.
[3]Professor and Research Guide, Department of Commerce, University College, Mangalore.

ABSTRACT

Banking is rightly considered as one of the most widely transacted service-based sectors meeting the diverse financial needs of customers across the globe. The rapid digitalisation of banking services has led to the uninterrupted accessibility to financial services, enhanced customer experience and a greater financial inclusion. However, with the extensive advancement of technology and Artificial Intelligence in modern banking, the incidence of unpleasant digital scams and fraud cases have been detected significantly posing serious threats to financial institutions and customers seamlessly. Digital Banking frauds cover a wide range of illegal acts using weaknesses in Cybersecurity systems, Human Psychology, and Technology. Digital fraud results in loss of money and the exposure of individual's privacy details, eroding public trust/confidence on the digital initiatives of the Government within the banking framework.

In this regard, this research study attempts to examine the distinct types of fraud prevalent in the contemporary society, the role of IT in both promoting and mitigating fraudulent activities and various strategies to curb such risks. A detailed case analysis of real-world banking fraud incidents, common vulnerabilities and associated risks are discussed to create awareness among the readers as regards the nature and forms of digital banking swindles. Additionally, the study presents essential safety measures to overcome cyber-crimes and enhance security in digital banking operations.

Keywords: Artificial Intelligence, Digital Banking, Emerging Trends and Frauds.

INTRODUCTION

The COVID-19 epidemic accelerated the shift to digital banking with an increase in electronic transactions. While this shift has greatly enhanced customer convenience, it has also created new opportunities for cybercriminals. Most of the users have become prime targets for scams due to their lack of familiarity with digital banking security rules. Fraudsters utilized this vulnerability by applying social engineering techniques such as impersonation fraud and phone spoofing to deceive individuals into disclosing confidential information, including one-time passwords (OTPs) and banking credentials. Regulatory bodies and Government all over the world have taken considerable steps to combat digital banking fraud. Financial institutions have enforced latest security measures such as biometric authentication, multi-factor authentication and real-time fraud detection. Despite these advancements, fraudsters design new strategies and tactics to bypass security protocols, exhibiting a battle between cybercriminals and security experts.

According to a survey report from the Financial Crimes Enforcement Network (FinCEN); the cybercrime in the banking industry has increased by 150% over the last 5 years. Regulatory bodies and Governments have implemented various measures to reduce digital banking fraud. The Reserve Bank of India (RBI), for instance, has mandated multi-factor authentication and transaction monitoring systems to achieve security (RBI, 2022). Similarly, the European Banking Authority (EBA) has introduced the Revised Payment Services Directive (PSD2) to enforce strong customer authentication (EBA, 2021). Despite these efforts, scammers continue to adapt, highlighting the need for continuous innovation in fraud detection and prevention.

OBJECTIVES

1. Examine the incidence of Banking Fraud and identify various techniques and emerging trends used in digital scams in the banking system.
2. Analyse the impact of digital fraud on banking customers and financial services.
3. Investigate the case studies related to recent E-Banking fraud incidents.
4. Evaluate the regulatory frameworks and control measures adopted to tackle digital banking frauds.

RESEARCH METHODOLOGY

- **Research Design:** The study follows a descriptive and conceptual research design, highlighting the emerging trends in digital banking frauds through some case study analysis. The research employs a qualitative approach, utilizing secondary based information to bring out the various fraud techniques, their implications, and emerging online security measures.
- **Data Collection Methods:** The article is designed by extracting information from research papers, news articles, case studies, industry reports, official reports and publications of regulatory bodies, financial institutions such as RBI, SEC, and Cybersecurity agencies.

EMERGING TRENDS IN DIGITAL BANKING FRAUDS

1. **Phishing:** Phishing is a type of cyberattack in which scammers send emails through phone in the name of a reputable financial institution/Bank. Frequently, these emails include links to websites that mimic legitimate financial gateways. Customers' login credentials are stolen by the attackers, who then have unauthorised access to their accounts. For example, A consumer gets an email pretending to be from their bank warning them that if they do not update their information, their account would be blocked. Clicking on the link redirects them to a fake banking page where they unknowingly enter their username, password, and OTP, allowing fraudsters to access their bank account.
2. **SIM Swap Fraud:** In SIM Swap Fraud, thieves obtain a fake SIM card from the telecom operator to take control of a victim's mobile number. After obtaining the SIM, they can reset passwords and gain access to the victim's bank accounts. For Example, using fictitious identification, a scammer contacts the cell service provider pretending to be the victim and asks for a replacement SIM card. Once engaged, all bank notifications and OTPs are sent to the fraudster, who uses them to carry out fraudulent activities without the victim's knowledge.

3. **UPI Frauds & QR Code Scams**: Scammers use fictitious payment requests or QR codes to fool victims into authorising fraudulent transactions over the Unified Payments Interface (UPI). In online marketplaces, scammers frequently pretend to be purchasers and send QR codes, claiming they need them to "receive" money. However, scanning the code takes money out of the victim's account. Example: Example: A scammer impersonating a buyer sends a QR code after a seller offers an item on OLX, stating it is for payment receipt. By scanning it, the vendor unintentionally approves a debit transaction rather than a credit one, resulting in the loss of money.
4. **Remote Access Scams:** Fraudsters utilise remote access programs like AnyDesk, TeamViewer, or QuickSupport to trick victims into installing them which may remotely control their equipment. Once installed, scammers can access financial apps, steal login information, and carry out illegal activities. For instance, a victim receives a call from a person posing as a customer service representative from a bank. In order to resolve a "security issue" with the bank app, they request the user to install AnyDesk. After installation, the fraudster gains control of the device and withdraws funds from the victim's bank account.
5. **Banking Malware & Trojans:** To obtain sensitive financial information, fraudsters use trojans and malicious software (malware) to infiltrate a user's computer, smartphone, or banking app. These malicious apps have the ability to override two-factor authentication, log login credentials, and record keystrokes. For instance, a user installs a fraudulent app from an unreliable source, believing it to be a legitimate banking app. After installation, the malware records the user's OTPs and login information, enabling hackers to access the account and drain it.

NOTABLE CASE STUDIES ON DIGITAL BANKING FRAUDS

1. The Yes Bank Phishing Scam (India, 2021):

In the year 2021, Securities and Exchange Board of India (SEBI) scrutinised YES bank for fraudulent realisation of Additional Tier-1 (AT1) Bonds. A penalty of ₹250 million was imposed on Yes Bank, declaring that the bank had misguided the retail investors to invest on these high-risk bonds as low-risk investments including senior citizens, without disclosing the risks associated with these investments. This misrepresentation resulted in significant financial losses for several investors when the bank used these bonds to stabilize their financial position.

In addition to this, Yes Bank has cautioned its customers regarding voice phishing scams, where fraudsters impersonate bank officials over the phone to obtain financial and personal details.

2. The Rise of UPI-Based Phishing Scams in India:

(UPI) Unified Payments Interface has revolutionized internet banking in the country, facilitating real-time transactions among the users. However, with its rapid usage, deceivers have adopted advanced techniques to exploit customers. Phishing attempts, which target people through fake UPI links and fraudulent customer support calls, are the most common scams. For instance, Mr. Rajesh Sharma, a working professional stationed in Mumbai, received a call from a person claiming to be a bank official. The fraudster informed him that his KYC (Know Your Customer) information required to be updated immediately to prevent account cancellation. The caller sent a UPI collect request and directed Rajesh to approve it, stating it was a verification step. Trusting the caller, Rajesh approved the request link, unknowingly transferring ₹50,000 from his bank account.

3. The Punjab National Bank (PNB) Scam (The case of Nirav Modi and Mehul Choksi):

One of the biggest banking scams in India was the Punjab National Bank (PNB) affair, which was made public in 2018. It involved about $1.8 billion (₹14,000 crore). In cooperation with some PNB officials, Nirav Modi and his uncle Mehul Choksi, proprietors of high-end jewellery brands, planned the scam. The illegal issuance of Letters of Undertaking (LOUs), which are bank guarantees that enable businesses to raise money from foreign banks, was at the centre of the scam. Based on fictitious LOUs issued by PNB's Brady House branch in Mumbai, Modi's companies were able to obtain loans from overseas branches of Indian Banks without having to provide the required collateral. As PNB's Core Banking System (CBS) was not integrated with the SWIFT (Society for Worldwide Interbank Financial Telecommunications) network, which enabled these unauthorised transactions, the fraud was undiscovered for several years. In January 2018, PNB officials discovered inconsistencies in their records, which led to the discovery of the scam. The Enforcement Directorate (ED) and Central Bureau of Investigation (CBI) then began their investigations, which resulted in several arrests and asset seizures. Owing to the exposure of significant weaknesses in internal control and banking, the Reserve Bank of India (RBI) strengthened trade finance laws after this scam.

4. The Cosmos Bank Cyber-attack (2018):

Cosmos Bank, a Cooperative Bank with its headquarters in Pune, suffered a sophisticated cyberattack in August 2018 that costs ₹94 crore. Through malware, hackers were able to access the bank's SWIFT (Society for Worldwide Interbank Financial Telecommunications) network by intruding its internal systems. Cybercriminals used cloned debit cards to withdraw substantial amounts of money over the period of 2 days from ATMs in 28 different countries. Additionally, fraudulent SWIFT transactions were used to transfer ₹13.92 crore to a Hong Kong bank. Banks throughout India tightened their transaction monitoring procedures strengthened their cybersecurity frameworks in the wake of the incident to avoid similar attacks in the future.

SUGGESTIONS:

- Banks need to actively educate their customers as regards the growing risks of banking frauds through the conduct of regular awareness campaigns via SMS, e-mails and social media.
- Customers should be informed not to share any OTPs, Passwords, or PINs with anyone, as Banks do not demand the same.
- Users need to download Banking Apps from official sources like Google Play Store or Apple App Store.
- Banks should advise the customers to enable two-factor authentication and transaction alerts to monitor account activity and avoid clicking on suspicious links received in emails, SMS, or WhatsApp messages.

CONCLUSION

To sum up, disseminating knowledge and raising awareness on digital fraud is essential to protect the interests of banking clients in this modern world. To safeguard consumers from online dangers, Banks must be proactive in educating the public, running awareness programs, and implementing secure banking practices. Financial institutions may drastically lower fraud incidents and increase consumer trust by encouraging vigilant and responsible digital behaviour. A collaborative effort between regulatory authorities, banks, and customers is essential to build a safer digital banking environment.

BIBLIOGRAPHY

- Kaur, P., & Sharma, R. (2021). The rise of digital banking frauds: Trends, challenges, and preventive measures. *Journal of Financial Crime, 28*(4), 123-145.
- Singh, A., & Jain, R. (2023). Artificial intelligence in banking fraud detection: Opportunities and risks. *Cybersecurity Review, 15*(2), 87-102.
- Smith, J. (2023). *Cybercrime in the digital banking era: Prevention and risk management.* Oxford University Press.
- Cybersecurity & Infrastructure Security Agency (CISA). (2023, September 10). *How AI is transforming digital fraud techniques.* https://www.cisa.gov/xxxxx
- Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A systematic literature review of e-banking frauds: Current scenario and security techniques. *Linguistica Antverpiensia, 2021*(2), 3509–3517.
- Mehta, A. (2024). Impact of technological advancements on banking frauds: A case study of Indian banks. *International Journal of Research in Finance and Management, 7*(1), 261–266.
- Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management, 26*(1), a1763.
- Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economic Surveys, 32*(5), 1292–1325.