International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Curbing Digital Technology in Bank Fraud and Theft

Sahanunu Dahiru[1], Zainab Sulaiman Abdullahi[2], Shamsuddeen Abdullahi[3]
[1, 3]Department of Computer Engineering Jigawa State Polytechnic for Information and Communication Technology, Kazaure
[2]Department of Computer Engineering Hussaini Adamu Federal Polytechnic Kazaure
Email address: sdahiru2@gmail.com, zeeshahzahm05@gmail.com, engrjigawa@gmail.com

Abstract— *The rapid evolution of digital technologies has transformed the banking industry, enhancing efficiency, accessibility, and user experience. However, it has also exposed financial institutions and their customers to a surge in sophisticated fraud and theft tactics. This paper explores the pressing need for robust strategies to curb the misuse of digital technology in bank fraud and theft. Key methods include the deployment of advanced cybersecurity measures such as artificial intelligence (AI)-driven anomaly detection, blockchain-based transaction verification, and multi-factor authentication systems. The study emphasizes the importance of real-time monitoring tools, customer education, and collaboration between financial institutions and regulatory bodies to mitigate risks. Additionally, legal frameworks must evolve to address emerging threats, such as deepfake scams and ransomware attacks targeting banking systems. The findings highlight the critical balance between leveraging technological innovation and ensuring security, advocating for a proactive and adaptive approach to safeguard digital banking ecosystems against fraud and theft. This research concludes that a comprehensive, multi-layered security strategy, supported by continuous technological and procedural advancements, is vital to protecting the integrity of modern financial systems in the face of evolving cyber threats*.

Keywords— *Digital Technology, Bank fraud and Theft*.

I. INTRODUCTION

The rapid adoption of digital technology in the banking sector has revolutionized financial transactions, making them faster, more convenient, and globally accessible. However, this evolution has also opened avenues for cybercriminals to exploit technological vulnerabilities, leading to increased incidents of fraud and theft. The global cost of financial cybercrime is projected to rise, with banks being primary targets due to the high-value assets they manage (Anderson et al., 2021). Most of these cases arise as a result of access to confidential banking information either through phone calls, facebook hacking, whatsapp hacking, ATM swap, and any form of crime that involve physical attack to snatch somebody's smartphone. Addressing this challenge requires a multi-faceted approach combining technology, regulation, and awareness.

II. CYBERCRIME

Cybercrime refers to any criminal activity that involves a computer, networked device, or a network. It includes offenses such as hacking, identity theft, phishing, fraud, and other forms of illegal digital activities that target individuals, businesses, or governments (Interpol, n.d.).

2.1 Cyber security

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, unauthorized access, or damage. These cyberattacks are often aimed at accessing, altering, or destroying sensitive information, interrupting normal operations, or extorting money from users (Kaspersky, n.d.).

2.2 Information access in bank fraud

Information access in bank fraud refers to unauthorized access to sensitive financial data, including account details, passwords, and transaction records, which is exploited to commit fraudulent activities. Criminals often use methods such as phishing, malware, or social engineering to gain access to this information and manipulate banking systems to siphon funds or steal identities (Asha & Sridhar, 2015).

2.3 The Evolution of Cybercrime in Banking

The digital transformation of the financial sector has provided cybercriminals with new opportunities. Traditional methods of bank robbery and theft have been replaced by digital fraud tactics, such as phishing, malware, ransomware, and social engineering. As financial institutions integrate more advanced technologies, cybercriminals have adapted their techniques to exploit vulnerabilities within these systems.

2.4 Electronic Funds Transfer Fraud

Electronic funds transfer systems have started to multiply, and with this comes the increased risk that these transactions might be intercepted and redirected. Legitimate credit card numbers can be captured electronically, as well as in person; the digital data held on a card can be replicated. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy. Computer-related crime may be compound in nature, combining two or more of the generic forms outlined below.

2.4.1 Phishing and Social Engineering

Phishing remains one of the most common techniques used by cybercriminals to steal individuals' funds. In phishing attacks, cybercriminals masquerade as legitimate institutions (e.g., banks or financial services) and trick victims into divulging personal information such as login credentials or financial account details. These attacks are increasingly sophisticated, with emails, websites, and phone calls designed to mimic real bank communications, making them hard for users to distinguish from legitimate messages.

2.4.2 Malware and Keyloggers

Another prevalent technique involves malware infections. Cybercriminals use malicious software to infiltrate a victim's computer or mobile device, often without their knowledge.

Sahanunu Dahiru and Zainab Sulaiman Abdullahi, "Curbing Digital Technology in Bank Fraud and Theft," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 18-20, 2025.

These programs can track keystrokes (keyloggers), capture screenshots, and record sensitive information such as login credentials. The malware can be delivered via email attachments, infected websites, or malicious apps.

2.4.3 SIM Swapping and Account Takeover

SIM swapping is a method in which cybercriminals gain control over a victim's phone number by convincing the victim's telecom provider to transfer the number to a SIM card in the attacker's possession. Once the criminal has control of the victim's phone number, they can intercept two-factor authentication codes, gaining access to online bank accounts and draining funds.

2.4.5 Insider Threats and Third-party Breaches

In some cases, cybercriminals may exploit weaknesses within organizations. Insider threats, where an employee or contractor with access to sensitive information steals funds or assists criminals. Additionally, breaches in third-party service providers, such as payment processors or cloud services, can expose personal financial data that criminals can use to execute fraudulent transactions.

2.5 Challenges in Digital Banking Security

1. Cyber Threat Landscape Financial institutions face a variety of cyber threats, including phishing, ransomware, insider fraud, and account takeovers. The sophistication of these attacks is growing, leveraging artificial intelligence (AI) and machine learning to breach defenses (Kshetri, 2020).
2. Weak Authentication Systems Many banking systems still rely on traditional authentication methods such as passwords and PINs, which are susceptible to breaches. Multi-factor authentication (MFA) adoption remains inconsistent, leaving significant gaps in security.
3. Human Error and Insider Threats Employees and customers often inadvertently enable fraud by falling victim to social engineering tactics or failing to follow security protocols. Insider threats also pose a significant risk, with malicious actors exploiting their access to sensitive systems (Pwc, 2022).
4. Regulatory and Compliance Gaps Despite advancements, regulatory frameworks in some regions lag behind the rapidly evolving threat landscape. A lack of uniform international standards exacerbates vulnerabilities in cross-border banking transactions (Basel Committee on Banking Supervision, 2022).

2.6 Impact of Digital Theft on Individuals

The consequences of digital theft are far-reaching and often devastating. For individuals, losing access to their bank accounts or having funds stolen can result in significant financial hardship. Victims may experience:

- Immediate Financial Loss: Direct theft of funds can leave individuals unable to meet immediate financial obligations, such as paying bills, mortgages, or healthcare costs.
- Psychological Effects: Being a victim of digital theft often leads to feelings of helplessness, embarrassment, and stress. The fear of further theft can cause long-term anxiety and a loss of trust in digital banking systems.
- Long-term Financial Implications: Recovery from financial theft can be prolonged and expensive. Victims often face challenges in reclaiming stolen funds, and the process can involve legal and bureaucratic hurdles. Additionally, their credit scores may be negatively impacted, affecting their ability to obtain loans or mortgages.

III. Solutions and Measures to Curb Cybercrime in Digital Banking

To curb the persistent threat of digital theft from bank accounts, a multifaceted approach involving individuals, financial institutions, and governments is required. The following strategies can help mitigate the risks:

1. Stronger Authentication Methods: Banks and financial institutions must prioritize the implementation of stronger authentication mechanisms to protect customers' accounts. While two-factor authentication (2FA) has become a standard security measure, criminals have developed ways to bypass it (e.g., through SIM swapping). Multi-factor authentication (MFA), incorporating biometrics such as fingerprints or facial recognition, can provide an added layer of security that is more difficult for criminals to bypass.

2. Customer and Employee Education

- Awareness Campaigns: Regular training for customers on recognizing phishing attempts and secure online behavior can reduce susceptibility to scams.
- Employee Training: Employees should undergo continuous training on cybersecurity protocols and fraud detection techniques.

3. Regulatory Enhancements Governments and international bodies must update regulations to address emerging threats. The General Data Protection Regulation (GDPR) in the EU serves as an example of robust data protection standards. Financial institutions should also comply with the Basel Framework's risk management principles.

4. Collaboration and Intelligence Sharing Financial institutions must collaborate to share threat intelligence. Industry-wide platforms, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), enable proactive defense measures by pooling resources and knowledge (FS-ISAC, 2023).

5. Enhanced Security Technologies

- AI and Machine Learning: Leveraging AI for anomaly detection can help identify fraudulent transactions in real time. Predictive analytics is capable of foreseeing and mitigating threats prior to their occurrence (Nguyen et al., 2021).
- Biometric Authentication: Implementing biometrics, such as fingerprint and facial recognition, provides a stronger layer of security compared to traditional methods.
- Blockchain Technology: Blockchain's decentralized nature ensures secure and transparent transactions, reducing opportunities for fraud in digital payments (Gupta & Bose, 2019).

Sahanunu Dahiru and Zainab Sulaiman Abdullahi, "Curbing Digital Technology in Bank Fraud and Theft," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 1, pp. 18-20, 2025.

IV. Conclusion

The rise of digital banking and online financial transactions has undoubtedly brought convenience and efficiency, but it has also made individuals more vulnerable to cybercriminal activities. The techniques used by criminals to steal funds from bank accounts are becoming more sophisticated, requiring a concerted effort from individuals, financial institutions, and governments to address the growing threat. By strengthening security measures, raising awareness, improving regulatory frameworks, and promoting collaboration between stakeholders, we can work together to curb the persistent techniques employed in stealing individual funds. It is imperative that all parties remain vigilant and proactive in safeguarding digital banking environments to protect consumers and preserve the integrity of financial systems worldwide

References

1. Anderson, R., Barton, C., Bohme, R., Clayton, R., & van Eeten, M. (2021). *The Economics of Cybercrime*. Cambridge University Press.
2. Asha, S., & Sridhar, M. (2015). *Cyber Crimes and Security Issues in Banking Sector*. International Journal of Research in Engineering and Technology, 4(3), 306–310.
3. Basel Committee on Banking Supervision. (2022). *Principles for Operational Resilience*. Bank for International Settlements.
4. FS-ISAC. (2023). *Cyber Threat Intelligence Sharing in the Financial Sector*. Retrieved from fs-isac.com.
5. Gupta, M., & Bose, S. (2019). "Blockchain in Banking". *Journal of Financial Innovation*, 12(3), 45-58.
6. Interpol. (n.d.). *Cybercrime*. Retrieved from https://www.interpol.int/Crimes/Cybercrime.
7. Kaspersky. (n.d.). *What is Cybersecurity?* Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.
8. Kshetri, N. (2020). "Cybersecurity Challenges in Financial Services". *Journal of Cybersecurity*, 6(2), 89-102.
9. Nguyen, T., et al. (2021). "AI Applications in Fraud Detection". *Artificial Intelligence Review*, 53(4), 1075-1101.
10. PwC. (2022). *Global Economic Crime and Fraud Survey*. PricewaterhouseCoopers.
11. Forbes. (2022). "How JPMorgan is Fighting Fraud with AI". Retrieved from forbes.com.
12. Financial Times. (2023). "HSBC's Technological Leap in Customer Security". Retrieved from ft.com.