

American Journal of Economics and Business Management

Vol. 9 Issue 7 | **pp.** 305-309 | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Digital Transformation and Institutional Voids: An Empirical Analysis of Social Engineering Tactics in Uzbekistan's Banking Sector

Feruza Nabieva[*1]

1. Researcher at Tashkent State University of Economics

* Correspondence: feruzanabievaal@gmail.com

Citation: Nabieva F. Digital Transformation and Institutional Voids: An Empirical Analysis of Social Engineering Tactics in Uzbekistan's Banking Sector. American Journal of Economics and Business Management 2026, 9(7), 305-309.

Received: 22nd Apr 2026
Revised: 14th May 2026
Accepted: 08th Jun 2026
Published: 10th Jul 2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

Abstract: The rapid digitalization of Uzbekistan's financial sector has created a profound paradox: while a "fintech boom" has accelerated economic growth, it has also fostered "institutional voids" in cybersecurity. This study investigates the adaptation of social engineering tactics to the local linguistic and cultural context of Uzbekistan, a research area that remains significantly under-explored in Central Asia. Utilizing a mixed-methods approach, the researchers conducted a content analysis of 1,252 primary incident reports recorded in January 2025 by the internal affairs authorities of Uzbekistan. The methodology of this research is thematic coding to classify fraudulent tactics such as vishing, phishing, and pretexting, while cross-tabulating these with victim demographics. The results indicate that 98% of fraud cases involved unauthorized remote transfers, with vishing via phone calls emerging as the dominant channel (58%). A critical finding is the correlation between age and financial loss: while younger victims (ages 20–45) experienced a higher frequency of attacks with lower average losses, the older demographic (ages 45–70) suffered critical financial damage due to high levels of trust and lower technical adaptability. To address these vulnerabilities, the study proposes the "Guardian" Adaptive Security Protocol, incorporating measures such as trusted delegate verification and call-state awareness. These findings emphasize that mitigating cybercrime in emerging digital economies requires specialized socio-technical safeguards to protect vulnerable populations and maintain systemic trust.

Keywords: Digital Transformation in Uzbekistan, Social Engineering, Financial Fraud, Institutional Voids.

1. Introduction

The current stage of development in Uzbekistan's financial sector is characterized by a profound paradox: rapid digital transformation and an unprecedented "fintech boom" have created unique opportunities for economic growth while simultaneously fostering dangerous "institutional voids" within the cybersecurity framework [1].

The widespread adoption of instant payment systems and digital banking has significantly outpaced both the evolution of regulatory protective mechanisms and the level of public digital literacy. In this context, financial fraud must be viewed not merely as a series of individual thefts but as a fundamental threat to trust in the country's burgeoning digital economy [2].

Global statistics underscore the magnitude of this challenge: annual worldwide losses from fraudulent transactions escalated from $9.84 billion in 2011 to over $32 billion by 2020. According to ACFE, the total cost of fraud accounts for approximately 5% of global business revenue, translating to an annual loss of $4 trillion. Uzbekistan is deeply embedded in these global trends; in Tashkent alone, 20,518 IT-related criminal complaints were recorded in 2024, resulting in damages exceeding 4.4 billion soums [3].

However, despite the evident surge in cybercrime across Central Asia, the mechanisms by which social engineering adapts to the local linguistic and cultural context remain poorly understood. Existing research predominantly focuses on Western or East Asian markets, often overlooking the specific deception scenarios tailored to the unique socio-economic realities of Uzbekistan [4]. This paper aims to bridge this research gap through an empirical analysis of social engineering tactics and their impact on various age demographics amidst the rapid digitalization of the republic's banking sector. The "institutional voids" in Uzbekistan's cybersecurity framework refer to a regulatory lag, where the rapid deployment of instant payment systems has surpassed the government's ability to implement comprehensive fraud prevention laws. An institutional void exists where there is a lack of systematic public education regarding digital hygiene, leaving the elderly demographic particularly vulnerable to sophisticated social engineering tactics [5].

2. Materials and Methods

The methodology of this study is based on a mixed-methods approach, integrating quantitative statistical analysis with qualitative content analysis of primary data. The empirical foundation consists of 1,252 incident reports (case descriptions) involving bank card fraud submitted to the internal affairs authorities of the Republic of Uzbekistan in January 2025 [6].

Content Analysis and Coding Process. The analysis was conducted in three distinct stages:

1. Preliminary Screening: Systematic review of case descriptions to identify recurring patterns of interaction between the fraudster and the victim.
2. Thematic Coding: Each report was categorized based on the specific social engineering tactic employed (e.g., phishing, vishing, pretexting) and the communication channel used (phone calls, instant messengers, social networks) [7].
3. Cross-tabulation: Correlating the age demographics of victims with the magnitude of financial loss to identify vulnerability trends.

Inclusion and Exclusion Criteria To ensure the robustness of the sample, the following criteria were applied:

1. Inclusion Criteria: Incidents involving unauthorized fund transfers from bank cards or involuntary credit applications via digital channels; cases where psychological manipulation or social engineering was the primary mechanism of the crime [8].
2. Exclusion Criteria: Technical failures of banking systems unrelated to fraudulent activity; physical theft of cards without the use of social engineering; and reports with critically insufficient data that precluded the reconstruction of the incident sequence.

Refining the "Unknown reasons" Category (51.4%) During the study, the "Unknown reasons" category, which accounted for 51.4% (643 cases) of the sample, underwent further qualitative scrutiny. It was determined that this group primarily comprises scenarios characterized by pure psychological pressure without the use of specific digital links or malware. Typical scenarios identified through qualitative analysis include [9].

Direct psychological manipulation during phone calls (vishing), where the victim voluntarily discloses OTP codes under conditions of induced stress or urgency. Social engineering tactics conducted through transient communication channels that were not preserved in the initial case documentation. The application of "pretexting" techniques,

where the perpetrator creates a fabricated crisis (e.g., “emergency assistance for a relative”), leaving no explicit digital footprint that could be categorized as standard phishing or e-commerce fraud [10].

3. Results

The Table 1. analysis of 1,252 incident reports recorded in January 2025 revealed key patterns in the structure of digital fraud within Uzbekistan. The study found that in 98% of cases (1,222 incidents), funds were misappropriated through unauthorized remote transfers, while 2% (30 cases) involved fraudulent or coerced credit applications in the victim's name [11].

Table 1. Fraud incident reports recorded by the Internal Affairs Authority of Uzbekistan.

Month	Total	Phishing link	Trading	E-commerce fraud	Employee of banking or payment systems	Renting	Down payment for a phone	Purchasing online game accounts	Job offering	Unknown reasons	Impersonating a state security officer	Other
In %		*0,7*	*13,1*	*8,3*	*3,5*	*2,2*	*4,2*	*1,4*	*1,8*	*51,4*	*0,6*	*13,3*
Jan	1252	9	164	104	44	27	52	18	23	643	1	167

Figure 1. Phone calls emerged as the dominant communication channel (58%), highlighting the high efficacy of vishing methods in the region. Social media and messaging platforms, such as Telegram (21%) and Instagram (9%), are also extensively utilized to execute phishing attacks and e-commerce fraud schemes (8.3%) [12].

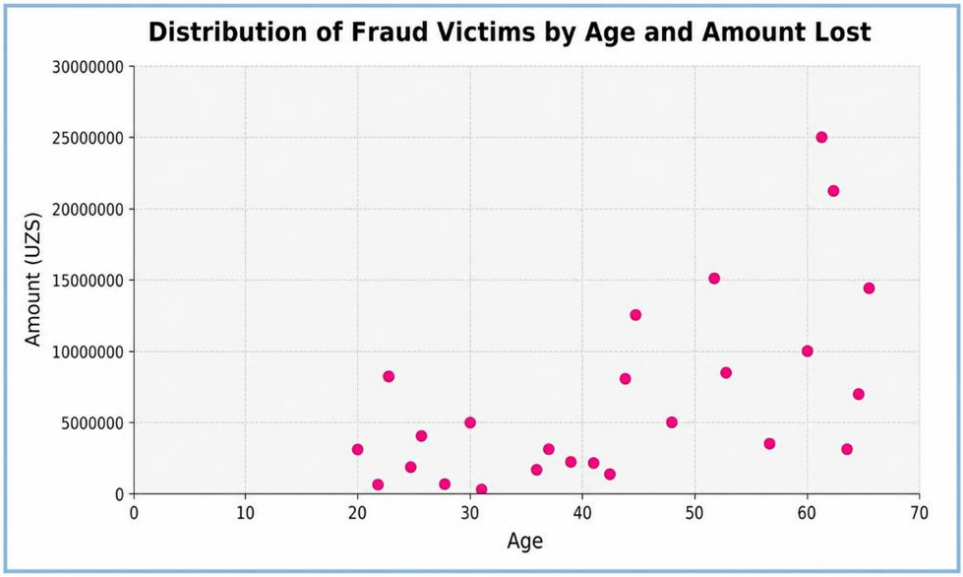


Figure 1. Distribution of fraud victims by age and amount lost.

A significant correlation was observed between the age of the victims and the nature of their financial losses. The empirical data confirm that digital literacy among youth (20–45 years old) reduces the average amount stolen, while a high level of trust and low technical adaptability among the older generation (45–70 years old) lead to significant financial losses. In the 20–45 age group, there is a high frequency of incidents; however, the stolen amounts remain relatively low due to the victims' ability to rapidly identify the threat. In contrast, the 45–70 age group experiences fewer incidents, but each successful social engineering act results in substantial financial damage, often involving the total loss of savings or the incurrence of significant debt [13].

4. Discussion

The study results confirm that the identified age paradox warrants specific academic scrutiny. While younger demographics (ages 20–45) face frequent but low-value thefts, the 45–70 age group is targeted for "high-ticket" attacks resulting in critical financial damage. This vulnerability stems not only from a lack of digital hygiene but also from a systemic absence of "impulse-control" safeguards in banking interfaces that could counteract psychological pressure.

Proposed Model: The "Guardian" Adaptive Security Protocol

1. Based on the empirical evidence regarding critical losses among older citizens, we propose a specialized Multi-Factor Authentication (MFA) model and an adaptive limit system:
2. Trusted Delegate Verification: For users aged 55 and above, any transaction to a previously unknown recipient exceeding a specific threshold (e.g., 20% of the average monthly turnover) must be authorized by a "Trusted Contact" (e.g., a family member) via a synchronized push notification [14].
3. Call-State-Aware Authentication: The mobile banking application should detect an active voice call. If a transfer is attempted during a call, the system must either trigger mandatory secondary biometrics (Face ID/Retinal scan) or enforce a mandatory 15-minute cooling-off period. This serves as a direct technical barrier against vishing maneuvers.
4. Mutual Authentication (Safe-Word System): To verify the legitimacy of a bank representative, the user's app should generate a unique, time-sensitive code that the caller must recite first. Failure to provide this code immediately identifies the caller as a fraudster.

The implementation of these measures would address the "institutional voids" identified in the introduction and significantly mitigate the risk of total asset depletion for the most vulnerable segments of society [15].

5. Conclusions

This study has provided an empirical analysis of the social engineering landscape within Uzbekistan's rapidly evolving banking sector, specifically addressing the "institutional voids" created by the nation's accelerated fintech boom. By examining 1,252 incident reports from January 2025, the research highlights that while digital transformation has enhanced financial accessibility, it has simultaneously introduced sophisticated risks that exploit human psychology rather than technical vulnerabilities. The findings confirm that vishing (58%) is the primary mechanism for financial fraud in the region, leveraging local cultural tendencies toward trust in authority and verbal communication. A critical contribution of this research is the identification of a clear demographic divergence in digital vulnerability: while younger populations (ages 20–40) exhibit higher resilience and lower average financial losses due to superior digital literacy,

the older generation (ages 45–70) remains highly susceptible to "high-ticket" fraud, often resulting in the total depletion of personal savings.

To address these systemic weaknesses, this paper proposes the "Guardian" Adaptive Security Protocol. This multi-layered framework—comprising Trusted Delegate Verification, Call-State Awareness, and Mutual Authentication systems—is designed to provide a technical safety net for the most vulnerable users. Implementing such socio-technical safeguards is not merely a matter of bank policy but a fundamental requirement for maintaining public trust in the digital economy. Ultimately, bridging the gap between technological advancement and user protection is essential for the sustainable growth of Uzbekistan's financial ecosystem. Future research should focus on the long-term efficacy of these adaptive MFA models and the impact of national digital literacy campaigns on reducing the success rates of cross-border social engineering tactics.

REFERENCES

[1] B. Musa, A. Bahago, N. A. M. Nasir, and F. Jamal, "Emerging trends in phishing: A look at smishing, vishing, quishing," *International Journal of Technology & Emerging Research*, vol. 1, 2025, doi: 10.64823/ijter.2503033.

[2] P. V. Falade, "Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2023, doi: 10.32628/CSEIT2390533.

[3] A. A. Abubaker, D. Eleyan, A. Eleyan, T. Bejaoui, N. Katuk, and M. Al-Khalidi, "Social engineering in social network: A systematic literature review," Manchester Metropolitan University, 2023. [Online]. Available: https://hdl.handle.net/10779/mmu.32484582.v1

[4] S. Gupta, M. Pritwani, A. Shrivastava, M. Mohana, M. Moharir, and A. R. Kumar, "A comprehensive analysis of social engineering attacks: From phishing to prevention—Tools, techniques and strategies," in *Proc. ICoICI*, 2024, pp. 1–8, doi: 10.1109/ICoICI62503.2024.10696444.

[5] M. Zaoui, Y. Belfaik, Y. Sadqi, M. Yassine, and K. Ouazzane, "A comprehensive taxonomy of social engineering attacks and defense mechanisms: Toward effective mitigation strategies," *IEEE Access*, vol. 12, pp. 72224–72241, 2024, doi: 10.1109/ACCESS.2024.3403197.

[6] M. Kamilova *et al.*, "Impact of the pandemic on fintech adoption by developing countries," in *ACM Int. Conf. Proc. Series*, 2022, pp. 178–181. [Online]. Available: https://dl.acm.org/doi/10.1145/3584202.3584229

[7] K. Ramachandran, K. Kayathwal, H. Wadhwa, and G. Dhama, "FraudAmmo: Large scale synthetic transactional dataset for payment fraud detection," in *Proc. Int. Joint Conf. Neural Networks (IJCNN)*, Gold Coast, Australia, Jun. 2023.

[8] D. Choi and K. Lee, "An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation," *Security and Communication Networks*, vol. 2018, Art. no. 5483472, 2018.

[9] J. Barnes, "Fraud detection: Forensic accounting education and CFE designation impact on auditor's confidence levels," *Journal of Accounting and Finance*, vol. 20, no. 4, pp. 62–75, 2020.

[10] D. L. Johnson, "Demystifying the elusive quest for cyber insurance protection: The need for new contract language," *Cardozo Law Review*, vol. 44, pp. 2361–2385, 2022.

[11] J. Abolarin, *Banking Law and Financial Regulations: The Imperatives for Managing Stability in the Banking Sector*, 2025. [Online]. Available: https://books.google.com

[12] X. Zhu, X. Ao, Z. Qin, Y. Chang, Y. Liu, Q. He, and J. Li, "Intelligent financial fraud detection practices in the post-pandemic era," *Innovation*, vol. 2, no. 4, Art. no. 100176, 2021.

[13] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[14] C. C. Aggarwal, *Outlier Analysis*, 2nd ed. Cham, Switzerland: Springer, 2017.

[15] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.