



Digital Banking in Uzbekistan: Enhancing Customer Trust and Addressing Cybersecurity Challenges

Norqo'zиеva Madina Ulug'bek qizi
Tashkent State University of Economics
Email: madinanorkuzieva@gmail.com

Submitted: 30-Mar, 2026

Accepted: 17-Apr, 2026

Published: 03-May, 2026

Vol. 3, No. 2, 2026. Sociometrics.us

Journal of Community, Law and
Diplomacy Sciences

***Corresponding author:**

Norqo'zиеva Madina Ulug'bek
qizi

Copyright © 2026 by author(s) and
Scientific Research Publishing Inc. This
work is licensed under the Creative
Commons Attribution International
License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The rapid digital transformation of the banking sector has significantly reshaped the delivery of financial services, turning mobile applications into comprehensive financial platforms accessible 24/7. In Uzbekistan, the expansion of digital banking has enhanced convenience and financial inclusion, while simultaneously raising concerns regarding cybersecurity and customer trust.

This study examines the relationship between the development of digital banking services, the level of customer trust, and emerging cybersecurity challenges. The research is based on a systematic analysis of scientific literature and statistical data reflecting the growth of digital payment systems. Particular attention is given to modern cyber threats, including phishing, social engineering, artificial intelligence-based attacks, and vulnerabilities in banking application programming interfaces (APIs).

The findings indicate that customer trust is a critical determinant of the sustainable development of digital banking. Trust is influenced by multiple factors, including service reliability, data protection, and transparency of financial operations. At the same time, increasing digitalization expands the attack surface, requiring banks to implement advanced security measures such as multi-factor authentication, encryption, and AI-driven fraud detection systems.

The study concludes that achieving a balance between user convenience and robust cybersecurity is essential for maintaining customer trust and ensuring the long-term stability of the banking sector. Strengthening cybersecurity frameworks and promoting user awareness are identified as key priorities for the continued development of digital financial services in Uzbekistan.

Keywords: Digital banking, cybersecurity, data protection, payment systems, risks, AI-based attacks, digital payment systems

Introduction

In recent years, the rapid advancement of digital technologies has fundamentally transformed the global banking sector. Mobile banking applications have evolved from simple tools for money transfers into comprehensive financial platforms that provide a wide range of services, including payments, lending, savings, and investment management, all accessible in real time. This shift has significantly enhanced the convenience

and accessibility of financial services for customers.[1]

In Uzbekistan, the digital transformation of the banking system has accelerated considerably, driven by regulatory reforms and the active adoption of financial technologies. As a result, customers have become increasingly reliant on digital channels for their daily financial activities, leading to a substantial increase in the volume of online transactions and the use of mobile banking applications.[2][3]

However, alongside these benefits, the expansion of digital banking services has introduced new challenges, particularly in the area of cybersecurity. The growing dependence on digital platforms has increased exposure to various cyber threats, including phishing attacks, social engineering, data breaches, and more sophisticated threats enabled by artificial intelligence. These risks raise critical concerns about the security of financial transactions and the protection of sensitive customer data.[4]

In this context, customer trust has emerged as a key factor in the sustainable development of digital banking. As technological differences between banks become less pronounced, the ability to ensure a secure and reliable digital environment becomes a primary competitive advantage. Customers are increasingly concerned not only with the functionality of banking applications but also with the level of security and protection provided.[5]

Therefore, the purpose of this study is to examine the relationship between digital banking development, cybersecurity challenges, and customer trust in Uzbekistan. The research aims to identify the key factors influencing trust in digital financial services and to analyze how banks can balance user convenience with effective cybersecurity measures in order to ensure long-term stability and growth.[6][7]

Related literature and research gaps

The development of digital banking has been widely discussed in the works of Mbama CI and Ezepe PO works, particularly in relation to customer trust and cybersecurity.[8]

Studies show that digital technologies have improved the accessibility and efficiency of financial services, but have also increased exposure to cyber risks.

Customer trust is identified as a key factor influencing the adoption of digital banking. It is largely determined by perceived security, data protection, and the reliability of services. Research indicates that security breaches and fraud incidents can significantly reduce user confidence and limit the use of digital platforms.

At the same time, the growing complexity of cyber threats – including phishing, malware, and AI-based attacks – has made cybersecurity a critical priority for banks. To address these challenges, financial institutions increasingly implement advanced solutions such as multi-factor authentication, encryption, and AI-driven fraud detection systems.

Overall, the literature highlights the need to balance strong security measures with user convenience, especially in the context of rapidly developing digital banking markets.[9]

Methodology

This study employs a complex approach based on a systems perspective to analyze digital banking services, customer trust, and cybersecurity challenges. The research combines qualitative and quantitative methods to ensure a comprehensive understanding of the topic.

The theoretical foundation is based on the analysis and synthesis of existing academic literature related to digital banking, trust formation, and cybersecurity. In addition, statistical data on digital payment systems are used to identify key trends in the development of digital financial services.

Comparative and analytical methods are applied to examine different cybersecurity approaches, including multi-factor authentication, encryption, and artificial intelligence-based fraud detection. Methods of classification and generalization are also used to identify key factors influencing customer trust.[10]

Results and Discussion

The practical application of this study focuses on examining the real-world implications of digital banking development in Uzbekistan, particularly in the context of customer trust and cybersecurity. The findings demonstrate that the widespread adoption of mobile banking and digital payment systems has significantly transformed financial behavior, enabling users to access a broad range of services with greater speed, efficiency, and convenience.[11]

The analysis reveals a consistent upward trend in the use of digital financial services, indicating a high level of user engagement and increasing reliance on online banking platforms. This expansion reflects not only technological progress but also the growing acceptance of digital solutions among customers. However, the results also highlight that this rapid growth is accompanied by an increased exposure to cyber risks.[12]

The study identifies that evolving cyber threats, including phishing schemes, social engineering, and AI-driven attacks, present substantial challenges to the security of digital banking systems. As a result, financial institutions are compelled to strengthen their cybersecurity frameworks and adopt more sophisticated protective measures. The implementation of advanced tools such as multi-factor authentication, encryption technologies, and intelligent fraud detection systems has proven to be essential in mitigating these risks.[13]

Furthermore, the results indicate that customer trust is closely linked to the perceived level of security and reliability of digital services. Users are more likely to engage with platforms that ensure data protection, transparency, and consistent performance. Conversely, any indication of vulnerability or security failure can negatively affect user confidence and reduce the adoption of digital banking solutions.[14]

In addition, the application of modern technologies, particularly artificial intelligence and machine learning, has enhanced the ability of banks to monitor transactions and detect suspicious activities in real time. These innovations contribute to faster response times and more effective prevention of financial fraud.

Overall, the findings suggest that the successful development of digital banking depends on the ability of financial institutions to integrate user-friendly services with robust cybersecurity mechanisms. Achieving this balance is critical for maintaining customer trust and ensuring the long-term sustainability of digital financial ecosystems.[15]

Conclusion

In conclusion, the study demonstrates that digital banking has become an essential component of the modern financial system, significantly enhancing the accessibility and efficiency of financial services. In Uzbekistan, the rapid adoption of digital technologies has increased customer engagement, while simultaneously raising important concerns related to cybersecurity.

The findings confirm that customer trust is a critical factor for the sustainable development of digital banking. This trust largely depends on the ability of financial institutions to ensure data security, protect users from cyber threats, and provide reliable services.

Therefore, achieving a balance between convenience and strong cybersecurity measures is essential. Strengthening security frameworks, implementing advanced technologies, and increasing user awareness will play a key role in maintaining trust and supporting the long-term growth of the banking sector.

References

- [1] C. I. Mbama and P. O. Ezepeue, "Digital banking, customer experience and bank financial performance: UK customers' perceptions," *Int. J. Bank Mark.*, vol. 36, pp. 230–255, 2018.
- [2] F. N. Mahmadi, Z. F. Zaaba, and A. Osman, "Computer security issues in online banking: An assessment

- from the context of usable security,” IOP Conf. Ser.: Mater. Sci. Eng., vol. 160, p. 012107, 2016.
- [3] M. S. Alam and M. A. Alam, “Cybersecurity in online banking: Challenges and solutions,” iCommerce Central, 2025. [Online]. Available: <https://www.icommercecentral.com/open-access/cybersecurity-in-online-banking-challenges-and-solutions.pdf>. [Accessed: Apr. 30, 2026].
- [4] UZCERT, “Forecast of major cyber threats in Uzbekistan for 2025,” [Online]. Available: <https://uzcert.uz/en/forecast-of-major-cyber-threats-in-uzbekistan-for-2025/>. [Accessed: Apr. 30, 2026].
- [5] S. Wang et al., “Data privacy and cybersecurity challenges in the digital banking sector,” Computers & Security, 2024.
- [6] Central Bank of the Republic of Uzbekistan, “About the CERT-CBU cybersecurity center of the Central Bank,” [Online]. Available: <https://cbu.uz/uz/cert/about/>. [Accessed: Apr. 30, 2026].
- [7] LEX.UZ, “Regulation on ensuring information security and cybersecurity in the payment systems of payment system operators and payment service providers,” No. 3513, May 21, 2024. [Online]. Available: <https://lex.uz/docs/-6933268>. [Accessed: Apr. 30, 2026].
- [8] LEX.UZ, “Regulation on minimum information security and cybersecurity requirements for commercial banks of the Republic of Uzbekistan,” No. 3669, Aug. 18, 2025. [Online]. Available: <https://lex.uz/uz/docs/-7689673>. [Accessed: Apr. 30, 2026].
- [9] J. A. Jafri et al., “A systematic literature review of the role of trust and security in FinTech and banking adoption,” 2023.
- [10] Y. Hanif et al., “Security factors on the intention to use mobile banking applications,” 2021.
- [11] S. C. Shin, J. W. Ho, and V. Y. Pak, “Digital transformation through e-Government innovation in Uzbekistan,” in Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT), 2020, pp. 632–639.
- [12] J. Ure, Digital solutions centre in Central Asia, 2021.
- [13] Z. Mamadiyarov, “Analysis of factors affecting remote banking services in the process of bank transformation in Uzbekistan,” Financial and Credit Activity Problems of Theory and Practice, vol. 1, no. 36, pp. 14–26, 2021.
- [14] A. M. Nurgazina, R. D. Doszhan, and A. Sabidullina, “New financial technologies: New opportunities and new challenges of the XXI century,” Khabarshy, vol. 33, 2021.
- [15] H. Yaseen et al., “Adoption of artificial intelligence-driven fraud detection in banking,” 2025.