المجلة الدولية للأداء الاقتصادي
International journal of economic performance
ISSN: 2661-7161 EISSN:2716-9073
Publications are Open Access in this journal
journal home page : https://ijep.dz/index.php/IJEP/index

Cyber Security Measures as Determinants of Customers' Loyalty: Evidence from the Nigerian Banking Industry

Olota oluwayomi omotayo *

olotaoluwayomi@gmail.com, Department of Financial Intelligence, College of Accounting Sciences, University of South Africa (South Africa)

ARTICLE INFO

Article history:
Received : 22/04/2026
Accepted : 31/05/2026
Published: 30/06/2026

Keywords:
Cyber-Security Measures; Customer Loyalty; Banking Industry; Biometric Verification; Multi-Factor Authentication; Security Awareness Campaigns.

Jel Codes:
G21; M15; O33; D83.

ABSTRACT

With the expansion of the digital presence of financial institutions, the complexity and intensity of cybercrime has increased, forcing banks to implement more resilient security systems to protect confidential information of their customers and maintain the confidence level among the participants of the financial ecosystem. Hence, cyber security measures as determinants of customers' loyalty: evidence from the Nigerian banking industry was investigated. Specifically, it examined the effect of biometric verification, multi-factor authentication, security awareness campaigns on customer loyalty in Nigeria banking industry. Descriptive survey was adopted using questionnaire to examine a sample of 377 active customers of the selected five banks in Kwara State. The obtained data was analyzed using PLS-SEM through SmartPLS. Findings revealed that multi-factor authentication has the strongest effect on customer loyalty ($\beta = 0.385$, $t = 10.312$, $p < 0.001$), followed by security awareness campaigns ($\beta = 0.288$, $t = 5.036$, $p < 0.001$), and biometric verification ($\beta = 0.256$, $t = 4.333$, $p = 0.001$). It concluded that cyber-security measures is significantly vital for customer loyalty in Nigerian banking industry. It therefore strongly recommended that Nigerian banks should prioritize cybersecurity especially by focusing strongly on multi-factor authentication as the cornerstone of its cybersecurity strategy. This should include implementing tokenized access and adaptive authentication systems bank-wide.

* *Corresponding author, E-mail address: olotaoluwayomi@gmail.com*

1. Introduction

The electronic revolution in the banking sector of Nigeria has created significant improvements in the delivery of its services, but it has resulted in multifaceted security issues, which require continuous consideration. With the expansion of the digital presence of financial institutions, the complexity and intensity of cybercrime has increased, forcing banks to implement more resilient security systems to protect confidential information of their customers and maintain the confidence level among the participants of the financial ecosystem (Hassan et al., 2024). Unfortunately, the dynamic character of such threats as phishing, malware, and social engineering has made the necessity to invest in sophisticated technical systems and promote the culture of security awareness and advocacy among employees and clients (Mustapha and Sinha, 2024; Reis et al., 2024).

To address these struggles, the Nigerian banks have adopted various measures, including multi-factor authentication, regular security audits, and cooperation with regulatory agencies, to help them to be better prepared to counter cyberattacks (Fatoki, 2023). These are technical, as well as regulatory compliance measures and the understanding of the population, which is critical to building a safe and trustful banking environment (Oyolola et al., 2023). The success of these efforts is also directly associated with the ability of banks to predict the coming risks and change their security approach, which guarantees that customer trust in an all-digital environment will not diminish (Onatuyeh et al., 2025).

The secure digital environment is not just an aspect that keeps one within the regulatory requirements, but a component of customer loyalty and business existence. It has been found that effective security practices can lead to increased customer trust and operation sustainability, which may be compromised by the lack of compliance and awareness (Nwankwo and Kanyangale, 2023). With the sector going on, continued investments in technology and customer-centric security strategies will be essential to ensure that the Nigerian banks can combat the dynamism of cyber threats and foster long-term relationships with customers (Ayinaddis et al., 2023; Oyolola et al., 2023).

Although biometric verification could be aimed at improving security, unwittingly, the same principle may have the effect of creating customer loyalty obstacles in the banking industry. Additional types of customer frustration might be caused by technical malfunctions (fingerprint or facial recognition error), which could be a barrier to using their accounts and affect the banking process (Elumaro and Obamuyi, 2018). Furthermore, the implementation of biometric data could lead more people to distrust the company because of risks of misuse and privacy invasions, especially when customers believe that their personal data could be exploited or shared without their knowledge (Fatoki, 2023).

Multi-factor authentication (MFA) is positively advertised because of its security capabilities, but the complexity may negatively impact customer loyalty. Being forced to memorize various passwords, using tokens, or one-time codes may seem inconvenient, particularly to customers less skilled in technology or experiencing poor mobile connectivity (Fatoki, 2023). This added complexity to the banking experience can lead to poor customer satisfaction, since people appreciate convenience and the speed with which they can get services (Ayinaddis et al., 2023). Provided that MFA is perceived as excessive, it might decrease the perceived quality of service

and encourage customers to go to other banks whose authentication processes are simpler (Uwabor & Ugwuonah, 2020).

Security awareness programs, though crucial in reducing frauds, have unintended customer loyalty effects. Unnecessarily lengthy or anxious communication can increase anxieties on the topic of digital banking safety, thus causing customers to lose trust in the abilities of the bank in securing their holdings (Mustapha & Sinha, 2024). Moreover, when the needs of the audience are not taken into consideration or the customer feels patronized by the campaigns, customers might be overwhelmed or disinterested (Fatoki, 2023). Such degradation of trust and felt inconvenience may contribute to a decrease in the emotional bond between a customer and the bank (Ayinaddis et al., 2023).

The specific objectives of the study include: to determine the effect of biometric verification on customer loyalty; to investigate the influence of multi-factor authentication on customer loyalty; and to examine the influence of security awareness campaigns on customer loyalty.

2. Conceptual Review

2.1 Concept of Cyber-Security Measures

Financial sector cyber-security is meant to secure the digital assets, sensitive information, and critical infrastructure against an ever-changing environment of cyberattacks. All these measures comprise various components that would involve advanced encryption, threat detection using artificial intelligence, and regulatory compliance frameworks, which would serve to protect financial operations and keep them active (Mahadevan, 2025; Dorosh, 2023). Machine learning and big data analytics have also contributed to improving the capability of institutions to identify anomalies and act on threats in real-time, contributing to improving the overall security posture of the sector (Asmar and Tuqan, 2024).

The success of cyber-security is not only today determined by the use of technology, but also by the further enhancement of risk management and the development of the security-conscious culture within organizations (Boorugupalli et al., 2025). Financial institutions are also advised to cooperate across sectors and exchange information to enhance early identification and prevention of cyber threats and adhere to legal and regulatory changes (Dorosh, 2023). The dynamism of cyber threats also requires continuous introduction of innovation and funding of security infrastructure so that financial systems can be robust and able to mitigate existing and arising risks (Mahadevan, 2025).

2.2 Customer Loyalty

Customer loyalty in the banking industry is a complex concept, which shows the level of commitment by a customer towards a long-term relationship and interaction with their financial service provider. It is also formed due to an interdependent set of interconnected factors, among them trust, satisfaction, perceived value, and the overall quality of the customer experience (Buhler et al., 2023; Milan et al., 2018). The loyalty is dynamic, as it changes when the customer interacts with digital platforms, receives service innovations, and when the bank meets customer financial demands (Kim et al., 2024).

The workplace proves that tangible and intangible determinants affect the loyalty of a customer, including the reputation of the service provider, the effectiveness of relationship marketing, or

the perceived reliability of digital services (Yen & Chen, 2025). Besides, loyalty has a close connection with emotional and psychological attachment that customers develop to their banks, which can be reinforced by constant positive impressions of the experience and disclosed ethical conduct in business (Buhler et al., 2023). With the rapid impact of digital change, loyalty driving mechanisms are changing, with more emphasis on digital trust and customer-centric financial planning (Kim et al., 2024).

2.3 The Effect of Cyber-Security Measures on Customer Loyalty

Customer loyalty in the banking industry can be significantly affected by strong implementation of cyber-security measures. As customers find that the financial institution they use cares about the security of their personal and financial information, their trust will strengthen, which will make them more loyal (Asmar & Tuqan, 2024; Mishra, 2023). Nonetheless, it is a balancing game, and excessive control over security measures can unintentionally create tension in the user experience, which can turn to frustration and lack of loyalty if not accompanied by convenience (Kim et al., 2024). The difficulty of banks is to provide effective security without reducing the convenience and availability that consumers would expect in digital services (Boorugupalli et al., 2025).

Studies have shown that cyber-security practices are important in eliciting customer perceptions and loyalty due to transparency and communication of the practice (Adejumo & Ogburie, 2025). Well-informed customers with regard to the security measures implemented will be confident and likely to be loyal, even amid the cyber threats committed to by the industry (Mahadevan, 2025). On the other hand, the absence of observable or understandable security practices will bring down trust and make people turn to other providers, showing the necessity to make security smoothly integrated into the entire customer experience (Kim et al., 2024).

2.4 Effect of Biometric Verification on Customer Loyalty

One of the most notable characteristics of digital banking is biometric verification as a new level of safety and convenience, which can have a positive impact on customer loyalty by creating confidence in services related to electronic banking (Ayinaddis et al., 2023). Customers will have more confidence in the bank as they see biometric systems as reliable and secure, which will result in increased loyalty and decrease their risk of switching to competitors (Shankar & Jebarajakirthy, 2019). Nevertheless, the efficiency of biometric verification in cultivating loyalty is strongly associated with the quality of the whole digital experience, such as flexibility and privacy, which is critical to achieving customer satisfaction and commitment over the long term (Mbama et al., 2018).

H1: Biometric verification has a positive influence on customer loyalty.

2.5 Effect of Multi-Factor Authentication on Customer Loyalty

The concept of multi-factor authentication (MFA) is well known as the ability to substantially enhance digital safety, and its application in the banking context can have a considerable influence on customer retention. MFA offers customers supplementary protection on the safety of their financial activities, which can increase trust and lead to loyalty (Afiyah et al., 2015). However, complicated and perceived inconvenience of MFA procedures can also apply friction, which will result in frustration and poor customer experience unless addressed with a high level of care (Zhou et al., 2021). The banks have to find the balance between strong security and

usability, because customer loyalty is likely to be retained once MFA is implemented in a way that will not affect convenience and accessibility (Mbama et al., 2018).

H2: Multi-factor authentication has a positive influence on customer loyalty.

2.6 Effect of Security Awareness Campaigns on Customer Loyalty

Security awareness campaigns play a critical role in informing customers of online threats and banking safely, and the impact they have on customer loyalty is complex. By proactively informing and empowering customers with quality awareness programs, banks are able to amplify customer satisfaction and trust, which are pillars of loyalty (Johri & Kumar, 2023). Nevertheless, when campaigns are viewed as overpowering, irrelevant, or anxiety-inducing, they can also lead to a loss in trust in the bank to safeguard customer assets, hence reducing loyalty (Iqbal et al., 2021). The success of these campaigns will be based on their relevance, understandability, and the level to which they assure customers of their security (Afiyah et al., 2025).

H3: Security awareness campaigns have a positive influence on customer loyalty.

3. Theoretical Review

3.1 Trust-Commitment Theory

The Trust-Commitment Theory, a statement by Morgan and Hunt (1994), argues that trust and commitment are the focal mediating constructs that achieve the effectiveness of relationship marketing; they lead to cooperation, value sharing, and relational equilibrium (Badrinarayanan and Ramachandran, 2024). The theory assumes that trust derives out of the confidence in the reliability of a partner, whereas commitment implies a readiness to maintain a valued association (Dubey et al., 2019). It is assumed that communication, a shared set of values, and low propensity to opportunism are antecedent conditions that lead to the development of trust and commitment, which consequently result in cooperation, reduction of uncertainty, and loyalty (Wang et al., 2019).

The theory can also be applied in the area of cyber security research to provide a clear understanding of how strong security practices can be used to support customer confidence in a bank and its ability to safeguard assets and information, thereby strengthening commitment and consequently fostering loyalty (Jafri et al., 2023; Panditharathna et al., 2024). Such mechanisms will be especially relevant to the Nigerian banking industry, where accelerated digitalization has intensified the need to depend on cyber security as the means to preserve the confidence of customers (Jafri et al., 2023). The empirical research indicates that trust, cyber security awareness, as well as policy implementation have a strong impact on the uptake of digital banking by customers and their retention (Jafri et al., 2023; Panditharathna et al., 2024).

4. Empirical Review

The study by Febriawan et al. (2024), entitled Assess The Impact Of Cyber Crime Mitigation Strategies on the Islamic Banks in Bandar Lampung City, focuses on the case of Islamic banks in Indonesia. The researchers used structural equation modelling with a partial least square (SEM-PLS) as a method to analyze the data based on primary data gathered using questionnaires from 96 respondents. Their results showed that sufficient strategies to look after the cyber dimension have a strong positive influence on customer loyalty and trust. The study established that strong

cyber security management is a requirement to maintain customer loyalty and increase it by reducing customer loss.

Johri and Kumar (2023), in their article titled Exploring Customer Awareness towards their Cyber Security: a study in the age of bank digital transformation, investigated the connection between customer awareness of cyber security and customer satisfaction in Saudi Arabia. The research involved primary data gathered using a structured questionnaire of 355 banking customers with ANOVA and bivariate regression. The findings showed that knowledge on cyber defending, phishing, and hacking is a significant determinant of customer satisfaction with digital banking services. The authors found that financial institutions need to improve their cyber security practices and offer frequent trainings to increase customer satisfaction and loyalty in the digital age.

Redda (2023) discussed the South African setting, studying the quality of e-banking and its role in customer loyalty with the mediation of customer satisfaction. The study utilized a descriptive research design and primary data collected using an online survey of 310 e-banking customers. Mediation analysis was conducted to determine correlations between quality of e-banking, customer satisfaction, and loyalty. The results affirmed that the quality of e-banking, including e-banking security, plays a direct positive significant influence on customer satisfaction and customer loyalty. The researchers concluded that good quality e-banking services supported by effective security measures play a vital role in customer loyalty.

5. Methodology

The study employed a descriptive design and survey methodology. This is due to the fact that the goal of descriptive research is to accurately depict a person, event, or circumstance. Since it contributes to the explanation of present practices related to the topic issue, descriptive research design is deemed suitable to examine the impacts of cyber-security measures on customer loyalty within Nigeria's banking industry. The study focuses on five major commercial banks in Nigeria — Zenith Bank, Access Bank, First Bank, GTBank, and UBA — selected based on their robust deployment of comprehensive cyber security measures such as biometric verification systems, multi-factor authentication protocols, and proactive security awareness campaigns for customers.

Population of interest are principal branches' active customers of the above five banks in Kwara State, and their estimated customer base is 20,000 in principal branches in Ilorin, Offa, and Omu-Aran. A sample size of 377 respondents was adopted using Taro Yamane's (1967) formula when utilizing known population with less than 5% margin error to provide statistical representation and generalizability of results. The study adhered to established ethical standards including informed consent from all participants, voluntary participation with no coercion, confidentiality and anonymity of respondents' data, and approval from relevant institutional review boards.

Participants were identified using purposive-proportional sampling, where there was equal representation in the chosen banks relative to customer population size and digital service usage. A structured questionnaire was used to gather replies from the respondents, which served as the primary source of data. The questionnaire had four major sections. The first covered three structured items on e-banking registration; the second had three items on service integration; the third covered two structured items on bank notification services; while the fourth covered three

structured items on customer experience. A five-point Likert scale was adopted as the scale of measurement for the questionnaire.

The instrument was validated through face and content validity conducted by lecturers and professors in the field of business administration and management, while the reliability of the study was assessed through Cronbach's alpha and Composite Reliability (CR) using SmartPLS version 3.2.9, with thresholds of 0.7 and above. For analytical purposes, descriptive statistics (mean and standard deviation) and inferential statistics were employed, with the utilization of Partial Least Squares Structural Equation Modeling (PLS-SEM) in the study of the structural relationship between cyber-security measures deployment and customer loyalty.

5.1 Model Specification

In this research report, cyber-security measures is the independent variable and customers' loyalty is the dependent variable. The following model will be utilized since the report will make use of structural equation modeling (SEM):

CL = f (Biometric Verification [BA + BD + BS] + Multi-Factor Authentication [PO + RE + SE] + Security Awareness Campaign [CM + IDB + PA])

Where: CL = Customers' Loyalty; BA = Biometric Authentication; BD = Biometric Data; BS = Biometric Security; PO = Password and OTP; RE = Reassurance; SE = Security Enhancement; CM = Cybersecurity Measures; IDB = Improved Digital Banking; PA = Phishing Attempts.

6. Results

6.1 Response Rate

The data needed for this investigation was gathered using a questionnaire. A total of 321 responses have been captured, which is 85.14% of the expected sample size. Thus, the actual responses make up the data used in this study.

6.2 Descriptive Analysis and Normality Test

Table 1: Descriptive Analysis and Normality Test

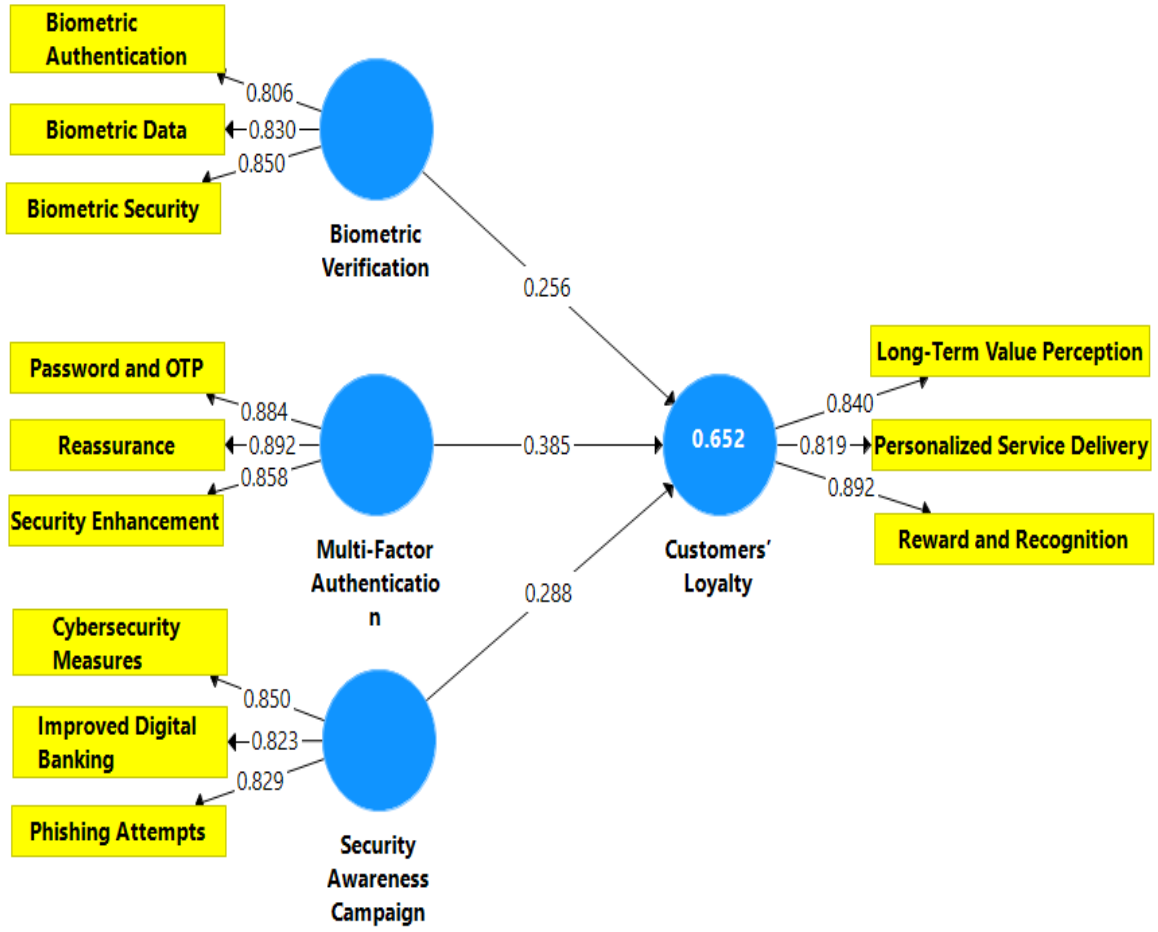
	Mean	Std. Deviation	Excess Kurtosis	Skewness	No. of Obs.
Biometric Authentication	2.863	0.995	-0.284	0.202	321.000
Biometric Data	3.340	0.973	-0.908	0.254	321.000
Biometric Security	3.324	0.876	-0.812	-0.011	321.000
Cybersecurity Measures	3.209	0.891	-0.173	-0.423	321.000
Improved Digital Banking	2.835	1.030	-0.720	-0.215	321.000
Long-Term Value Perception	3.218	1.123	-0.683	-0.239	321.000
Password and OTP	2.433	1.012	-0.783	0.138	321.000
Personalized Service Delivery	3.221	0.923	-0.863	0.216	321.000
Phishing Attempts	2.969	1.132	-0.954	-0.262	321.000
Reassurance	2.769	1.087	-0.765	0.102	321.000
Reward and Recognition	3.047	1.059	-0.802	-0.030	321.000
Security Enhancement	2.835	1.197	-1.010	0.015	321.000

Source: SmartPLS Output, 2025

Table 1 evaluates customer responses concerning cybersecurity measures and their loyalty. The mean values range from 2.433 to 3.340, indicating varying levels of customer agreement. 'Biometric Data' has the highest mean (3.340), signifying that customers view data security positively. In contrast, 'Password and OTP' has the lowest mean (2.433), reflecting dissatisfaction with password-based authentication systems. Standard deviations are mostly below 1.2, indicating moderate variability. Skewness values are near zero, showing symmetrical distributions. Kurtosis values are predominantly negative, indicating flatter distributions and minimal outliers.

6.3 Assessment of Measurement Model

Figure 1: Path Model of Cybersecurity Measures and Customers' Loyalty



Source: SmartPLS Output, 2025

Figure 1 shows the structural model which indicates that cybersecurity measures significantly affect customers' loyalty in the Nigerian banking industry, with an explained variance of 65.2% ($R^2 = 0.652$). Biometric Verification contributes a moderate effect ($\beta = 0.256$), supported by strong loadings on biometric authentication (0.806), biometric data (0.830), and biometric security (0.850). Multi-Factor Authentication is the most influential factor ($\beta = 0.385$), reflecting the importance of password/OTP systems (0.884), customer reassurance (0.892), and overall security enhancement (0.858) in fostering loyalty. Security Awareness Campaigns also play a significant role ($\beta = 0.288$), emphasizing the impact of cybersecurity measures (0.850), improved digital banking security (0.823), and protection from phishing attempts (0.829).

Table 2: Construct Reliability and Validity

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Biometric Verification	0.773	0.868	0.687
Customers' Loyalty	0.811	0.887	0.725
Multi-Factor Authentication	0.852	0.910	0.771
Security Awareness Campaign	0.783	0.873	0.696

Source: SmartPLS Output, 2025

Table 2 confirms the reliability and validity of cybersecurity constructs. Cronbach's Alpha values (0.773 to 0.852) exceed 0.7, confirming internal consistency. Composite reliability values (0.868 to 0.910) are above 0.7, ensuring construct reliability. Average Variance Extracted (AVE) values (0.687 to 0.771) surpass 0.5, verifying convergent validity. These results demonstrate that the constructs are reliable tools for understanding cybersecurity's impact on customer loyalty.

Table 3: Discriminant Validity

	Biometric Verification	Customers' Loyalty	Multi-Factor Authentication	Security Awareness Campaign
Biometric Verification	0.829			
Customers' Loyalty	0.702	0.851		
Multi-Factor Authentication	0.623	0.708	0.878	
Security Awareness Campaign	0.713	0.689	0.564	0.834

Source: SmartPLS Output, 2025

Table 3 assesses the uniqueness of cybersecurity constructs. Diagonal values (square roots of AVE) exceed inter-construct correlations, confirming discriminant validity. For instance, 'Biometric Verification' (0.829) is distinct from 'Customers' Loyalty' (0.702). These findings indicate that each construct uniquely affects customer loyalty, validating the study's focus on diverse cybersecurity aspects.

6.4 Multicollinearity

This assesses the correlation between the independent variables to know if two independent variables are not correlated and producing the same result. The Variance Inflation Factor (VIF) is used to assess likely correlation between the independent variables.

Table 4: Inner VIF Values

	Biometric Verification	Customers' Loyalty	Multi-Factor Authentication	Security Awareness Campaign
Biometric Verification		2.383		
Customers' Loyalty				
Multi-Factor Authentication		1.717		
Security Awareness Campaign		2.137		

Source: SmartPLS Output, 2025

Table 4 evaluates multicollinearity using VIF values. 'Biometric Verification' (2.383), 'Multi-Factor Authentication' (1.717), and 'Security Awareness Campaign' (2.137) all have VIF values below 5, indicating no significant multicollinearity. This confirms that each cybersecurity measure independently impacts customer loyalty without overlap.

6.5 Test of Hypotheses

Table 5: Bootstrapping Results Showing Path Coefficients for Structural Model

	Original Sample (O)	Sample Mean (M)	Std. Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Biometric Verification -> Customers' Loyalty	0.256	0.254	0.059	4.333	0.001
Multi-Factor Authentication -> Customers' Loyalty	0.385	0.382	0.037	10.312	0.001
Security Awareness Campaign -> Customers' Loyalty	0.288	0.294	0.057	5.036	0.001

Source: SmartPLS Output, 2025

Table 5 reveals the significance of cybersecurity measures on customer loyalty. 'Multi-Factor Authentication' (β = 0.385, t = 10.312, p = 0.001) has the strongest positive effect, indicating its critical role in fostering loyalty through robust protection. 'Security Awareness Campaign' (β = 0.288, t = 5.036, p = 0.001) and 'Biometric Verification' (β = 0.256, t = 4.333, p = 0.001) also significantly influence loyalty. The significant p-values confirm that all constructs positively affect customer loyalty, leading to the rejection of the null hypotheses.

Table 6: Coefficient of Determination Score

	R Square	R Square Adjusted
Customers' Loyalty	0.652	0.648

Source: SmartPLS Output, 2025

Table 6 reports an R-Square of 0.652, indicating that 65.2% of the variability in customer loyalty is explained by cybersecurity measures. The Adjusted R-Square (0.648) confirms the model's strong explanatory power, showing the substantial role of cybersecurity measures in fostering customer loyalty.

Table 7: Assessment of the Effect Size (f^2)

	Biometric Verification	Customers' Loyalty	Multi-Factor Authentication	Security Awareness Campaign
Biometric Verification		0.079		
Customers' Loyalty				
Multi-Factor Authentication		0.248		
Security Awareness Campaign		0.112		

Source: SmartPLS Output, 2025

Table 7 assesses the effect size (f^2) of cybersecurity constructs on customer loyalty. 'Multi-Factor Authentication' (0.248) has the largest effect, while 'Security Awareness Campaign' (0.112) and 'Biometric Verification' (0.079) show moderate and small effects respectively. These findings suggest prioritizing multi-factor authentication to maximize customer loyalty.

7. Discussion of Findings

The study results demonstrate that cybersecurity measures significantly affect customer loyalty. 'Multi-Factor Authentication' emerged as the most impactful factor, emphasizing the importance of advanced authentication protocols in fostering trust and loyalty. 'Security Awareness Campaign' significantly contributes to loyalty by educating customers about threats and preventative measures, fostering a secure banking environment. Similarly, 'Biometric Verification' positively impacts loyalty by providing reliable and secure access control. These findings lead to rejecting the null hypotheses and affirm that comprehensive cybersecurity strategies are critical for enhancing customer loyalty.

These results align with Ojo (2024), who identified multi-factor authentication as a key driver of trust in digital banking. Bajwa et al. (2023) emphasized the role of security awareness in improving customer confidence, while Abbas and Sallal (2025) highlighted biometric verification's effectiveness in securing customer data. Together, these findings validate the role of cybersecurity in achieving long-term customer loyalty in the Nigerian banking context.

8. Conclusion

This study concludes that cybersecurity measures play a significant role in enhancing customer loyalty in the five selected banks in Nigeria. Multi-factor authentication emerged as the most impactful measure, providing robust protection and fostering trust. Security awareness campaigns educate customers about threats, enhancing confidence, while biometric verification ensures secure and reliable access. Collectively, these measures show the strategic importance of cybersecurity in achieving customer loyalty.

8.1 Recommendations

To improve customer loyalty, Nigerian banks should prioritize cybersecurity especially by focusing strongly on multi-factor authentication as the cornerstone of their cybersecurity strategy. This should include implementing tokenized access and adaptive authentication systems bank-wide. Security awareness campaigns should be tailored to educate customers regularly through digital and physical channels. Biometric verification systems must be upgraded to ensure seamless and secure user experiences. These measures should be rolled out across all branches and digital platforms immediately, with regular monitoring and customer feedback integration to refine strategies.

Declarations

Conflicts of Interest

The author declares no conflict of interest.

Funding Statement

The author declares that no external funding was received for this research

Data Availability Statement

The author declares that all data supporting the findings of this study are included in the article. No additional data are available

Ethics Approval and Consent to Participate

Informed consent was obtained from all respondents. Participation was voluntary, and respondents were assured of confidentiality and anonymity of their responses.

Consent for Publication

Not applicable. This study did not involve any individual participant data, including personal details, images, or video

Author Contributions

Introduction: O. O. O.; literature review: O. O. O.; gaps in literature: O. O. O.; writing-review and editing: O. O. O.; methodology O. O. O.; results: O. O. O.; conclusion: O. O. O.; references O. O. O.

Acknowledgments

The authors express sincere appreciation to Zenith Bank Plc, Access Bank Plc, First Bank Plc, Guaranty Trust Bank Plc, and United Bank for Africa Plc for granting permission and support during data collection. We are also deeply grateful to the customers of these banks who voluntarily participated in the study and shared their experiences. Their time and responses made this research possible. The authors received no direct funding from any of the institutions mentioned above

Artificial Intelligence (AI) Use Statement

The authors declare that they have not used AI or AI-assisted tools during the preparation of this manuscript.

References

- Abbas, A., & Sallal, Z. (2025). Hybrid biometric authentication for banks security improvements. Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/10.47974/jdmsc-2030.
- Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2025.25.3.0909.
- Afiyah, E., Rizan, M., & Usman, O. (2025). Analysis of Mobile Banking Usage in Increasing Customer Trust and Loyalty. Journal of Economics, Management and Trade. https://doi.org/10.9734/jemt/2025/v31i11268.
- Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. Heliyon, 10. https://doi.org/10.1016/j.heliyon.2024.e37571.
- Ayinaddis, S., Taye, B., & Yirsaw, B. (2023). Examining the effect of electronic banking service quality on customer satisfaction and loyalty: an implication for technological innovation. Journal of Innovation and Entrepreneurship, 12, 1-18. https://doi.org/10.1186/s13731-023-00287-y.
- Badrinarayanan, V., & Ramachandran, I. (2024). Relational exchanges in the sales domain: A review and research agenda through the lens of commitment-trust theory of relationship marketing. Journal of Business Research. https://doi.org/10.1016/j.jbusres.2024.114644.

- Bajwa, I., Ahmad, S., Mahmud, M., & Bajwa, F. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. Inf. Comput. Secur., 31, 635-654. https://doi.org/10.1108/ics-11-2022-0179.
- Boorugupalli, K., Kulkarni, A., Suzana, A., M, D., Ponnusamy, S., & S., K. (2025). Cybersecurity Measures in Financial Institutions Protecting Sensitive Data from Emerging Threats and Vulnerabilities. ITM Web of Conferences. https://doi.org/10.1051/itmconf/20257602002.
- Brown, J., Crosno, J., & Tong, P. (2019). Is the theory of trust and commitment in marketing relationships incomplete? Industrial Marketing Management. https://doi.org/10.1016/j.indmarman.2018.10.005.
- Buhler, R., De Oliveira Santini, F., Ladeira, W., Rasul, T., Perin, M., & Kumar, S. (2023). Customer loyalty in the banking sector: a meta-analytic study. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-08-2023-0484.
- Dorosh, I. (2023). Cyber security and its role in the financial sector: threats and protection measures. Economics. Finances. Law. https://doi.org/10.37634/efp.2023.10.10.
- Dubey, R., Altay, N., & Blome, C. (2019). Swift trust and commitment: The missing links for humanitarian supply chain coordination? Annals of Operations Research, 1-19. https://doi.org/10.1007/s10479-017-2676-z.
- Elumaro, A., & Obamuyi, T. (2018). Card Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. European Scientific Journal, ESJ. https://doi.org/10.19044/esj.2018.v14n16p40.
- Fatoki, J. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2023.9.2.0609.
- Febriawan, M., Lakilaki, E., Ariefandri, D., Saputra, R., Wijaya, P., & Manikam, D. (2024). Assess The Impact Of Cyber Crime Mitigation Strategies On Islamic Banks In Bandar Lampung City. Jurnal Ekuilnomi. https://doi.org/10.36985/0n4h9r29.
- Hassan, A., Ewuga, S., Abdul, A., Abrahams, T., Oladeinde, M., & Dawodu, S. (2024). Cybersecurity in Banking: A Global Perspective With a Focus on Nigerian Practices. Computer Science & IT Research Journal. https://doi.org/10.51594/csitrj.v5i1.701.
- Iqbal, K., Munawar, H., Inam, H., & Qayyum, S. (2021). Promoting Customer Loyalty and Satisfaction in Financial Institutions through Technology Integration: The Roles of Service Quality, Awareness, and Perceptions. Sustainability. https://doi.org/10.3390/su132312951.
- Jafri, J., Amin, S., Rahman, A., & Nor, S. (2023). A systematic literature review of the role of trust and security on Fintech adoption in banking. Heliyon, 10. https://doi.org/10.1016/j.heliyon.2023.e22980.
- Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Human Behavior and Emerging Technologies. https://doi.org/10.1155/2023/2103442.
- Junaid, A. (2024). Theory Review: Factors Affecting the Level of Trust and Commitment in the Supply Chains of High-tech Companies. International Journal of Advanced Engineering and Management Research. https://doi.org/10.51505/ijaemr.2024.9303.
- Kim, L., Jindabot, T., & Yeo, S. (2024). Understanding customer loyalty in banking industry: A systematic review and meta analysis. Heliyon, 10. https://doi.org/10.1016/j.heliyon.2024.e36619.
- Mahadevan, G. (2025). Cybersecurity in Banking and Financial Software Solutions. Economic Sciences. https://doi.org/10.69889/0btn6w55.

- Makudza, F. (2020). Augmenting customer loyalty through customer experience management in the banking industry. Journal of Asian Business and Economic Studies. https://doi.org/10.1108/jabes-01-2020-0007.
- Mbama, C., & Ezepue, P. (2018). Digital banking, customer experience and bank financial performance: UK customers' perceptions. International Journal of Bank Marketing, 36, 230-255. https://doi.org/10.1108/ijbm-11-2016-0181.
- Milan, G., Slongo, L., Eberle, L., De Toni, D., & Bebber, S. (2018). Determinants of customer loyalty: a study with customers of a Brazilian bank. Benchmarking: An International Journal. https://doi.org/10.1108/bij-08-2017-0231.
- Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences. https://doi.org/10.3390/app13105875.
- Morgan, R., & Hunt, S. (1994). The Commitment-Trust Theory of Relationship Marketing. Journal of Marketing, 58, 20-38. https://doi.org/10.1177/002224299405800302.
- Mukherjee, A., & Nath, P. (2007). Role of Electronic Trust in Online Retailing: A Re-examination of the Commitment-Trust Theory. Entrepreneurship & Marketing eJournal. https://doi.org/10.1108/03090560710773390.
- Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian Banking Sector: The Techniques and Preventive Measures. International Journal of Innovative Science and Research Technology (IJISRT). https://doi.org/10.38124/ijisrt/ijisrt24aug395.
- Nwankwo, C., & Kanyangale, M. (2023). Effect of Cyber Security on Business Sustainability of Listed Microfinance Banks in Nigeria. IJEBD (International Journal of Entrepreneurship and Business Development). https://doi.org/10.29138/ijebd.v6i5.2279.
- Ojo, O. (2024). Development of a Three Factor Authentication System for Online Banking. Ajayi Crowther Journal of Pure and Applied Sciences. https://doi.org/10.56534/acjpas.v3i2.114.
- Onatuyeh, E., Oghorodi, D., Okpako, E., Ojei, E., Osakwe, G., Chinedu, N., Okoh, S., Odu, V., Chinedu, P., & Nwankwo, W. (2025). Cybersecurity and Business Survival in Nigeria: Building Customer's Trust. African Journal of Applied Research. https://doi.org/10.26437/ajar.v11i1.882.
- Oyolola, T., Abubakar, A., Bello, U., & Sani, L. (2023). Electronic customer relationship management and customer retention of deposit money banks in Dutsin-Ma, Nigeria. Journal of Management and Science. https://doi.org/10.26524/jms.13.25.
- Panditharathna, R., Liu, Y., De Macedo Bergamo, F., Appiah, D., Trim, P., & Lee, Y. (2024). How Cyber Security Enhances Trust and Commitment to Customer Retention: The Mediating Role of Robotic Service Quality. Big Data Cogn. Comput., 8, 165. https://doi.org/10.3390/bdcc8110165.
- Redda, E. (2023). E-banking quality and customer loyalty: The mediating role of customer satisfaction. Banks and Bank Systems. https://doi.org/10.21511/bbs.18(2).2023.15.
- Reis, O., Oliha, J., Osasona, F., & Obi, O. (2024). Cybersecurity Dynamics in Nigerian Banking: Trends and Strategies Review. Computer Science & IT Research Journal. https://doi.org/10.51594/csitrj.v5i2.761.
- Shankar, A., & Jebarajakirthy, C. (2019). The influence of e-banking service quality on customer loyalty. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-03-2018-0063.
- Uwabor, O., & Ugwuonah, G. (2020). E-Service Quality and Customer Loyalty in Deposit Money Banks in Nigeria. European Journal of Business and Management. https://doi.org/10.7176/ejbm/12-21-04.
- Wang, X., Tajvidi, M., Lin, X., & Hajli, N. (2019). Towards an Ethical and Trustworthy Social Commerce Community for Brand Value Co-creation: A trust-Commitment Perspective. Journal of Business Ethics, 1-16. https://doi.org/10.1007/s10551-019-04182-z.

- Yen, Y., & Chen, S. (2025). The Triple Pathway to Loyalty: Understanding How Banks' Corporate Social Responsibility Influences Customers via Moral Identity, Service Quality, and Relationship Quality. Sustainability. https://doi.org/10.3390/su17073220.
- Zhou, Q., Zhou, Q., Lim, F., Yu, H., Xu, G., Ren, X., Liu, D., Wang, X., Mai, X., & Xu, H. (2021). A study on factors affecting service quality and loyalty intention in mobile banking. Journal of Retailing and Consumer Services. https://doi.org/10.1016/j.jretconser.2020.102424