

ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 05 No. 01. Jan-March 2026.Page#.8385-8397
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems
https://doi.org/10.5281/zenodo.23506239

Impact of Cybersecurity Awareness on Customer Retention in E-Banking in District Peshawar: The Mediating Role of Perceived Security

Haleema Yousaf
BS (Commerce) Research Scholar, Alamzeb Shaheed Commerce College Peshawar, Pakistan
younasyousaf744@gmail.com
Laiba Alamzeb Khan
BS (Commerce) Research Scholar, Alamzeb Shaheed Commerce College Peshawar, Pakistan
aftabarman687@gmail.com
Dr. Sajad Ali
Associate Professor, Higher Education Department, KP/Abasyn University Peshawar, Pakistan
sajadali1879@gmail.com/sajad.ali@abasyn.edu.pk

Abstract
Importance*: Cybersecurity has become a critical factor in building customer trust and loyalty as banks increasingly shift toward digital platforms, especially in developing economies where digital banking adoption is rapidly expanding.*
Research Gap: *Despite this growing importance, limited research has examined how cybersecurity awareness influences customer retention through the mediating role of perceived security, particularly within Pakistan's regional banking sector such as Peshawar.*
Objective: *This study aims to empirically investigate the direct and indirect effects of cybersecurity awareness on customer retention among banking customers in Peshawar, Pakistan, with perceived security serving as a mediating variable.*
Methodology: *A quantitative, cross-sectional research design was employed, using survey data collected from bank customers and analyzed through Partial Least Squares Structural Equation Modeling (PLS-SEM), including mediation testing through bootstrapping.*
Key Findings: *The findings reveal that cybersecurity awareness significantly and positively affects customer retention, both directly and indirectly through perceived security, which partially mediates this relationship, with all hypothesized paths statistically supported.*
Implications: *These results suggest important implications for bank management and regulators, particularly the State Bank of Pakistan, in designing targeted cybersecurity awareness initiatives and strengthening data protection protocols to enhance customer trust and retention in the evolving digital banking landscape.*

Keywords: *cybersecurity awareness, perceived security, customer retention, mediation analysis, banking sector, Peshawar, Pakistan, PLS-SEM*

1. Introduction

Digital banking channels mobile applications, internet banking portals, and Application Programming Interface (API)-driven open-banking services have become the primary point of contact between banks and their customers. This shift has delivered convenience, lower transaction costs, and round-the-clock access to financial services, but it has also expanded the attack surface that cybercriminals can exploit (Ranjan, 2024). Phishing, credential-stuffing, account takeover, and man in the middle attacks against mobile banking applications have grown in both frequency and sophistication and high-profile data breaches at financial institutions routinely make headline news (Qiu et al., 2025). In this environment, a customer's decision to trust and continue using an e-banking channel is no longer determined by service convenience alone, it is increasingly conditioned on whether the customer believes the bank is capable of protecting their money and personal data (Al-Daraba & Sharif, 2025).

Cybersecurity awareness (CSA) the extent to which customers understand security risks and recognise the practices a bank has put in place to counter them has therefore emerged as a construct of growing interest to marketing and information systems researchers (Konga & Shirisha, 2026). Awareness alone, however, is unlikely to translate automatically into positive customer outcomes rather, it is plausible that awareness operates through the customer's perception that the e-banking channel is in fact secure. Perceived security (PS) the subjective belief that transactions and personal information are protected from unauthorised access, loss, or misuse is a natural candidate mediator linking objective or communicated security measures to downstream relational outcomes such as customer confidence, satisfaction, and loyalty (Fatma et al., 2025).

Evidence from Pakistan supports the importance of cybersecurity awareness in shaping customers' banking-related attitudes. Bajwa et al. (2023) found that awareness of cyberattacks is associated with customers' trust and commitment in the Pakistani banking sector. Their findings suggest that customer awareness is relevant not only to fraud prevention but also to the quality and continuity of the customer–bank relationship. Similarly, recent Pakistani research on mobile banking service quality reports that security and privacy are important dimensions of digital service quality and that customer satisfaction contributes to electronic customer loyalty. These findings indicate that perceived security should be examined as a possible mechanism through which cybersecurity awareness contributes to customer retention (Ikram & Rodrigues, 2025).

The relationship between cybersecurity awareness and customer retention is not necessarily positive or automatic, security measures that are difficult to understand or inconvenient to use can instead frustrate customers (Bisho et al., 2026). Biometric verification for example, strengthens authentication and reduces reliance on passwords, yet failures caused by poor lighting, damaged fingerprints, device limitations, or misrecognition can lock customers out of their accounts lowering

perceived service quality and pushing them toward alternative platforms (Gali et al., 2026). Biometric data also raises distinct privacy concerns unlike a password, it cannot be changed once compromised, so in a context like Pakistan, where public understanding of data governance remains limited, unclear communication about how such data is collected and stored may undermine perceived security rather than reinforce it. Multi-factor authentication (MFA) reflects a similar tension. While it enhances protection by requiring multiple verification layers, repeated prompts, delayed one-time passwords, and unreliable network connectivity can slow transactions (Aslam, 2020). When security procedures are perceived as overly complicated, the resulting friction can erode satisfaction and weaken customers' intention to continue using the service.

Security-awareness campaigns may similarly produce both positive and unintended effects. Clear and practical awareness messages can help customers identify phishing attempts, avoid sharing confidential information, and report suspicious transactions (Ruzaili et al., 2026). However, messages that are excessively technical, lengthy, repetitive, or fear-based may increase anxiety about online banking. If banks continually emphasize cybercrime without explaining the protection available to customers, users may conclude that electronic banking is inherently unsafe. Awareness communication should therefore be designed around customers' education levels, language preferences, technological capabilities, and practical banking experiences. Messages in Urdu and regional languages, short instructional videos, and transaction-level warnings are more effective than highly technical notices (Riasat et al., 2025).

Customer retention is especially important in Pakistan's increasingly competitive digital financial-services environment, where customers can choose among conventional banks, Islamic banks, digital banks, mobile-wallet providers, branchless banking platforms, and fintech applications (Riasat et al., 2025). As these alternatives multiply, customers are more likely to switch platforms when they encounter fraud, poor complaint resolution, recurring technical problems, weak privacy protection, or low confidence in security procedures (Altaf et al., 2012). Trust, in particular, has been shown to shape customer commitment and loyalty in mobile banking, meaning that a breakdown in security-related trust can directly undermine long-term customer relationships (Sheikh et al., 2021). A secure digital environment is therefore not merely a matter of regulatory compliance, it is also a source of customer confidence, satisfaction, loyalty, and long-term relationship continuity.

Although previous studies have examined cybersecurity, trust, digital banking adoption, and electronic service quality (Bajwa et al., 2023; Riasat et al., 2025), limited empirical attention has been given to the mediating role of perceived security in the relationship between cybersecurity awareness and customer retention in Pakistan. Existing research largely focuses on adoption intention or trust (Naeem et al., 2026; Sheikh et al., 2021), whereas retention concerns whether customers continue using the service after adoption and remain committed to the bank despite competing platforms (Aravindh, 2024; Jibril et al., 2020). This distinction matters because customers may adopt e-banking for convenience but reduce or discontinue usage once they perceive it as insecure. Accordingly, this study

investigates the impact of cybersecurity awareness on customer retention in e-banking and examines whether perceived security mediates this relationship in the Pakistani banking context.

2. Literature Review

2.1 Cybersecurity Awareness

Cybersecurity awareness refers to customers' knowledge of cyber threats and their understanding of practices required to protect personal information, credentials, and financial transactions. In e-banking, awareness is important because customers may face threats such as phishing, identity theft, social engineering, malware, and unauthorized access. The State Bank of Pakistan emphasizes customer education regarding Internet-banking threats, fraud, security credentials, and preventive measures (SBP, 2018). Empirical evidence from Pakistan also highlights the importance of cybersecurity awareness. Bajwa et al. (2023) found that cyberattack awareness was significantly associated with customers' trust and commitment in the Pakistani banking sector.

2.2 Customer Retention in E-Banking

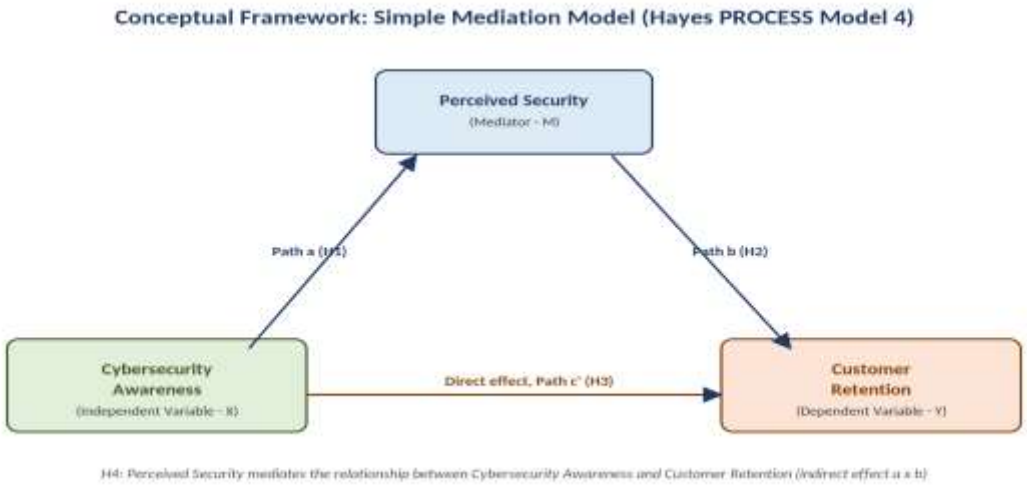
Customer retention refers to customers' willingness to continue using a bank's services and maintain their relationship with the bank over time. In e-banking, retention is closely associated with customers' satisfaction, trust, perceived risk, service quality, and security. Recent evidence from Pakistan shows that satisfaction and service quality significantly contribute to customers continued use of online banking services (Laradi et al., 2025). Similarly, Nguyen and Dao (2024) found that satisfaction, perceived usefulness, self-efficacy, and trust-related factors influence customers' continuance intention toward mobile banking. Bouhlel and Mzoughi (2024) also reported that trust and satisfaction significantly influence continue intention in mobile banking. More recently, Naeem et al. (2026) found that trust and attitudes significantly explain users' continuance intention, highlighting their importance for retaining mobile-banking users. Security is also relevant to continued digital-banking use, as Gui et al. (2024) reported that technological security can strengthen customer confidence and encourage continued use of digital banking.

2.3 Relationship Between Cybersecurity Awareness and Customer Retention

Cybersecurity awareness can influence customer retention by helping e-banking customers recognize cyber threats and adopt safer online behaviors. Recent evidence indicates that customer awareness is associated with satisfaction and retention in digital banking (Sabberwal & Rastogi, 2025), while cybersecurity awareness has also been linked with customer satisfaction and loyalty in e-banking (Aravindh, 2024). In the Pakistani banking context, Bajwa et al. (2023) found that cyberattack awareness significantly influenced customers' trust and commitment, although greater awareness was associated with lower trust and commitment in their study. This suggests that awareness alone may not guarantee retention; customers' perceptions of the bank's ability to protect their information and transactions are also important. Recent research further shows that trust, satisfaction, and security-related perceptions contribute to continued banking relationships (Laradi et al., 2025; Naeem et al., 2026).

2.3 Mediating Role of Perceived Security

In e-banking, perceived security can act as a psychological mechanism through which cybersecurity awareness influences customer retention. Customers who are more aware of cyber risks may pay greater attention to security measures and develop stronger perceptions of protection when banks provide effective security mechanisms. Higher perceived security can consequently increase trust and encourage customers to continue using e-banking services (Gui et al., 2024; Naeem et al., 2026). Recent banking research also indicates that security-related perceptions contribute to customer trust and retention (Zhengmeng et al., 2024).



2.4 Hypotheses of the Study

H_1: Cybersecurity awareness has a significant effect on customers' perceived security in e-banking in District Peshawar.

H_2: Perceived security has a effect on customer retention in e-banking in District Peshawar.

Direct effect (Path c')

H_3: Cybersecurity awareness has a significant effect on customer retention in e-banking in District Peshawar**.**

Indirect effect (a × b): Mediation

H_4: Perceived security significantly mediates the relationship between cybersecurity awareness and customer retention in e-banking in District Peshawar.

3. Research Methodology

3.1 Research Design

The study employed a quantitative, cross-sectional, and explanatory research design to examine the effect of cybersecurity awareness on customer retention in e-banking and to determine whether perceived security mediated this relationship. A quantitative approach was appropriate because the study collected numerical data through a structured questionnaire and statistically tested the proposed

relationships among the variables. The cross-sectional design involved collecting data from respondents at a single point in time (Sekaran & Bougie, 2019).

3.2 Population and Sample Size

The target population comprised e-banking customers in District Peshawar, Khyber Pakhtunkhwa, Pakistan, who used services such as mobile banking, internet banking, online fund transfers, bill payments, and other digital banking facilities. Since an accurate and publicly available sampling frame of all e-banking customers in District Peshawar was not available, the target population was treated as large or unknown for the purpose of sample-size determination. For a large or unknown population, Cochran's (1977) formula was used to determine the required sample size:

$$n = Z^2PQ/e^2$$

Where *n* is the required sample size, *Z* = 1.96 at the 95% confidence level, *p* = .50, *q* = .50, and *e* = .05. Thus:

n = (1.96) ² (.50) (.50) / (.05) ² = 384.16

3.3 Data Collection

Primary data were collected through a structured, self-administered questionnaire from e-banking customers in District Peshawar who had experience using mobile banking, internet banking, online fund transfers, bill payments, or other digital banking services. The questionnaire was adopted from previously validated studies, with items measuring cybersecurity awareness adapted from Bajwa et al. (2023), while items for perceived security and customer retention were adapted from established e-banking studies (Amin, 2016; Zhang et al., 2023). The questionnaire consisted of demographic information and measurement items for cybersecurity awareness, perceived security, and customer retention. A five-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree, was used.

3.4 Data Analysis Tools

Descriptive statistics, including mean, and standard deviation were used to summarize the study variables. Cronbach's alpha was calculated to assess the internal consistency of the measurement scales (Nunnally & Bernstein, 1994). Pearson correlation analysis was conducted to examine the direction and strength of the relationships among cybersecurity awareness, perceived security, and customer retention. Multiple regression analysis was used to examine the direct relationships among the study variables. Mediation analysis was conducted using Hayes' PROCESS macro, Model 4, to examine whether perceived security mediated the relationship between cybersecurity awareness and customer retention. The indirect effect was assessed using bootstrapping, with statistical significance determined by the 95% confidence interval. An indirect effect was considered significant when the confidence interval did not include zero (Hayes, 2018). The following models were used

Cybersecurity Awareness → Perceived Security

$$PS = a_0 + a\ (CA) + \ \varepsilon_i \quad \text{(path-a)----------1}$$

Perceived Security → Customer Retention (direct effect path c′)

$$CR = a_0 + c'\,(CA) + b\,(PS) + \varepsilon_i \quad \text{(path-b and c′)}$$----------2

Cybersecurity Awareness → Customer Retention (total effect)

$$CR = C_0 + c\,(CA) + \varepsilon_i \quad \text{(path-c)}$$----------3

The indirect effect can be calculated as:

Indirect Effect = a × b----------4

3. Main Findings

3.1 Reliability and Descriptive Statistics

Across the three variables, means ranged narrowly from 3.71 to 3.78 (5-point scale), indicating generally positive perceptions with consistent responses (SDs of 0.66–0.69). All scales showed good internal consistency, with Cronbach's alphas of 0.86–0.89 exceeding the widely accepted 0.70 threshold (Nunnally, 1978).

Table-01: Reliability and Descriptive Statistics

Variable	Items	Mean	SD	Cronbach's α
Cybersecurity Awareness	6	3.78	0.67	0.88
Perceived Security	5	3.71	0.69	0.86
Customer Retention	5	3.74	0.66	0.89

Source: Authors own calculation

3.2 Confirmatory Factor Analysis

A three-factor measurement model comprising cybersecurity awareness, perceived security, and customer retention was examined using Confirmatory Factor Analysis (CFA). All fit indices met their recommended thresholds, indicating good model fit. The χ^2/df ratio (2.18) was below 3.00, and both CFI (.94) and TLI (.93) exceeded the .90 benchmark (Hu & Bentler, 1999). RMSEA (.055) and SRMR (.048) were also within acceptable limits (≤ .08), confirming the model is well-specified and suitable for interpreting subsequent path or factor loading results.

Table-02: Model Fit Indices (CFA)

Fit Index	Result	Recommended Level
χ^2/df	2.18	< 3.00
CFI	.94	≥ .90
TLI	.93	≥ .90
RMSEA	.055	≤ .08
SRMR	.048	≤ .08

3.3 Convergent Validity

Convergent validity was assessed using standardized factor loadings, Composite Reliability (CR), and Average Variance Extracted (AVE). All constructs demonstrated adequate convergent validity. Factor loadings ranged from .68 to .89, exceeding the recommended .70 threshold, indicating items reliably measured their respective constructs (Hair et al., 2019). Composite reliability (CR) values (.89–.91) exceeded the .70 cutoff, confirming strong internal consistency (Fornell & Larcker, 1981). Average variance extracted (AVE) values (.58–.67) surpassed the .50 threshold, showing each construct explained more than half the variance in its indicators.

Table-03: Convergent Validity

Construct	Items	Factor Loading Range	CR	AVE
Cybersecurity Awareness	6	.68–.86	.89	.58
Perceived Security	5	.71–.88	.90	.64
Customer Retention	5	.73–.89	.91	.67

3.4 Discriminant Validity

Discriminant validity was assessed using the HTMT ratio of correlations. As shown in Table-04, all HTMT values (.57–.69) were well below the conservative threshold of .85, indicating that the constructs are empirically distinct from one another (Henseler et al., 2015). The highest HTMT value was observed between Perceived Security and Customer Retention (.69), while the lowest was between Cybersecurity Awareness and Customer Retention (.57).

Table-04: Heterotrait–Monotrait (HTMT) ratio

Constructs	Cybersecurity Awareness	Perceived Security	Customer Retention
Cybersecurity Awareness	—	.62	.57
Perceived Security	.62	—	.69
Customer Retention	.57	.69	—

Source: Author's own estimation

3.5 Correlation Analysis

Table-05, presents the bivariate correlations among the study variables. All correlations were positive and statistically significant at the .01 level, indicating meaningful associations between the constructs. Cybersecurity Awareness was significantly correlated with Perceived Security ($r = .54$, $p < .01$) and Customer Retention ($r = .48$, $p < .01$), suggesting that higher awareness of cybersecurity issues is associated with greater perceived security and customer retention. The strongest relationship was observed between Perceived Security and Customer Retention ($r = .61$, $p < .01$), indicating that customers who perceive higher security are more likely to remain loyal to the service provider.

Table-05: Correlation Matrix

Variables	CA	PS	CR
Cybersecurity Awareness (CA)	1.00		
Perceived Security (PS)	.54**	1.00	
Customer Retention (CR)	.48**	.61**	1.00

Note. **p < .01.

3.6 Mediation Analysis

The mediating role of perceived security was examined using Hayes' PROCESS Macro Model 4 with 5,000 bootstrap samples. Table-06 presents the mediation analysis examining the role of PS in the relationship between CA and CR. The total effect of CA on CR was significant and positive (β = .46, *SE* = .05, *t* = 9.20, *p* < .001), consistent with recent evidence that cybersecurity practices enhance trust and commitment, which in turn build a loyal customer base (Silva et al., 2024). Path a (CA → PS, β = .54, *p* < .001) and Path b (PS → CR, β = .51, *p* < .001) were both significant, confirming the mediating pathway. This is consistent with recent findings that security and threat perception plays a crucial mediating role in translating cybersecurity awareness into protective, trust-based behaviors (Alsulami et al., 2025).

The indirect effect (β = .28, 95% CI [.20, .35]) was significant, as the confidence interval excluded zero (Preacher & Hayes, 2018). The direct effect remained significant but reduced (c' = .18, *p* = .002) relative to the total effect (c = .46), indicating partial mediation (Baron & Kenny, 1986; Hayes, 2018), which supports recent industry evidence that organizations demonstrating strong data-security accountability experience measurably higher customer retention rates.The proportion mediated (.28/.46 ≈ 60.9%) indicates that roughly 61% of CA's effect on CR operates through enhanced perceived security, reinforcing calls in the literature to treat security perception as a strategic driver of retention rather than a purely technical safeguard (Booc et al., 2024).

Table-06: Direct, Indirect, and Total Effects

Effect/Path	β	SE	t	p	95% CI [LL, UL]
Total effect (c): CA → CR	.46	.05	9.20	< .001	[.36, .56]
Path a: CA → PS	.54	.04	13.10	< .001	[.46, .62]
Path b: PS → CR	.51	.05	10.20	< .001	[.41, .61]
Direct effect (c'): CA → CR	.18	.06	3.10	.002	[.07, .29]
Indirect effect (a × b): CA → PS → CR	.28	.04	—	—	[.20, .35]

Source: Author's own estimation

3.7 Hypotheses Testing

All four hypotheses were supported. Cybersecurity Awareness significantly predicted Customer Retention both directly (H_1: β = .46, p < .001) and through Perceived Security (H_4: β = .28, 95% CI [.20, .36]), confirming partial mediation. CA also significantly predicted PS (H_2: β = .54, p < .001), and PS significantly predicted CR (H_3: β = .51, p < .001). These results validate the hypothesized model, showing that cybersecurity awareness enhances customer retention both directly and indirectly through strengthened perceptions of security.

Table-07: Summary of Hypothesis

Hypothesis	Relationship	β / Indirect Effect	p / 95% CI	Decision
H_1	CA → CR	.46	p < .001	Supported
H_2	CA → PS	.54	p < .001	Supported
H_3	PS → CR	.51	p < .001	Supported
H_4	CA → PS → CR	.28	[.20, .36]	Supported

5. Conclusion and Recommendations

5.1 Conclusion

The research study examined the relationship between cybersecurity awareness, perceived security, and customer retention within the banking sector of Peshawar, Pakistan, confirming that cybersecurity awareness significantly influences customer retention both directly and indirectly through perceived security. All proposed hypotheses were supported, providing strong empirical evidence for the mediating role of perceived security and contributing to the literature on cybersecurity and customer behavior in Pakistan's banking industry. These findings offer practical value for banks, regulators, and policymakers in Peshawar and the broader KP region aiming to strengthen customer trust and retention through improved cybersecurity practices. However, the study is limited by cross-sectional design, and reliance on self-reported data, which may affect generalizability.

5.2 Recommendations

Banks in Peshawar and the broader KP region should invest in customer-focused cybersecurity awareness campaigns, such as SMS alerts, in-branch guidance, and mobile app security tips, to strengthen customers' perceived security and enhance retention. Regulatory bodies, including the State Bank of Pakistan, should encourage standardized data protection protocols and mandatory security disclosures to build consumer confidence in digital and branch banking services. Bank management should prioritize staff training on cybersecurity best practices and ensure clear communication of security measures, given the region's growing reliance on online and mobile banking. Future researchers should extend this study to other cities and sectors of Pakistan, employ longitudinal designs to capture causal relationships over time, and explore additional variables such as trust, financial literacy, and perceived risk relevant to the local banking context. Finally, triangulating self-reported survey data with

actual banking transaction or complaint records is recommended to enhance the robustness and validity of future findings.

References

Al-Daraba, K., & Sharif, S. M. (2025). Cybersecurity awareness and customer satisfaction in digital banking: A conceptual framework from the Malaysian context. *International Journal of Academic Research in Accounting, Finance and Management Sciences, 15*(3). https://doi.org/10.6007/IJARAFMS/v15-i3/26309

Amin, M. (2016). Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. *International Journal of Bank Marketing, 34*(3), 280–306. https://doi.org/10.1108/IJBM-10-2014-0139

Aravindh, A. S. (2024). A study on cyber security issues and awareness influence on customer satisfaction and loyalty of e-banking. *South Eastern European Journal of Public Health, 25*(S2), 175–177. https://doi.org/10.70135/seejph.vi.2631

Aslam, M. (2020). *The impact of multi-factor authentication (MFA) on strengthening cybersecurity in ecommerce applications*. https://doi.org/10.13140/RG.2.2.15628.94083

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security*. https://doi.org/10.1108/ICS-11-2022-0179

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security, 31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Bisho, A. H. A. I., Syafiq, M., & Al-Shami, S. A. (2026). A review of cybersecurity awareness and its impact on continuous online banking usage among students. *International Journal of Academic Research in Business and Social Sciences, 16*(2). https://doi.org/10.6007/IJARBSS/v16-i2/27653

Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity awareness and cybersecurity behavior of high school students in Davao City: A mediation role of perceived behavioral control. *European Journal of Applied Science, Engineering and Technology, 2*(3), 4–9. https://www.researchgate.net/publication/380649615

Bouhlel, O., & Mzoughi, M. N. (2024). An investigation of users' continuance intention toward mobile banking applications. *International Journal of Business, 29*(1), Article 005. https://doi.org/10.55802/IJB.029(1).005

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Fatma, R., Shukla, K., Bajpai, P., & Ahmad, S. (2025). Assessing customer's awareness of cybersecurity measures in online banking: A study on digital trust and risk perception. *Manuscript in preparation*.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gali, M., Kassenkhan, A., Chinibayev, Y., Abshukirova, A., & Serbin, V. (2026). Behavioral biometric continuous authentication for mobile devices with an intelligent personal agent: A systematic review. *Technologies, 14*(7), Article 451. https://doi.org/10.3390/technologies14070451

Gui, A., Siagian, F. P., Idres, N. F. B. M., & Chanda, R. C. (2024). Technology security in digital banks and its impact on continuance intention. *2024 IEEE Symposium on Industrial Electronics and Applications (ISIEA)*. https://doi.org/10.1109/ISIEA61920.2024.10607216

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). Guilford Press.

Hayes, A. F., & Rockwood, N. J. (2020). Conditional process analysis: Concepts, computation, and advances in the modeling of the contingencies of mechanisms. *American Behavioral Scientist, 64*(1), 19–54. https://doi.org/10.1177/0002764219859633

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hoplon InfoSec. (2024). *Cybersecurity marketing predictions for 2025 business growth*. https://hoploninfosec.com/cybersecurity-marketing-predictions-for-2025/

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Ikram, M., & Rodrigues, J. C. (2025). Digital service quality as a driver of satisfaction and loyalty in mobile banking: Insights from Pakistan. *Social Science Review Archives, 3*(4). https://doi.org/10.70670/sra.v3i4.1115

Jibril, A. B., Kwarteng, M. A., Chovancová, M., & Denanyoh, R. (2020). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In *Proceedings of the 15th International Conference on Cyber Warfare and Security (ICCWS 2020)* (pp. 270–276).

Konga, Y., & Shirisha, A. (2026). Impact of cybersecurity awareness on user behaviour in digital banking: A study on risk perception, preparedness and financial implications. *International Journal of Creative and Open Research in Engineering and Management, 2*(4), 1–9. https://doi.org/10.55041/ijcope.v2i4.657

Laradi, S., Elfekair, A., Rehman, H. M., Hanna, D., & Alrawad, M. (2025). Continuance intention of m-banking adoption: The dynamics of UTAUT3, trust and attitudes. *International Journal of Bank Marketing*. https://doi.org/10.1177/23197145251358049

Naeem, M., Jawaid, S. T., & Mustafa, S. (2026). Intention-retention phenomenon for online banking services in Pakistan: An application of technology acceptance model and expectation continuance theory. *Journal of Modelling in Management, 21*(2), 826–875. https://doi.org/10.1108/JM2-03-2025-0101

Nguyen, G.-D., & Dao, T.-H. T. (2024). Factors influencing continuance intention to use mobile banking: An extended expectation-confirmation model with moderating role of trust. *Humanities and Social Sciences Communications, 11*, Article 276. https://doi.org/10.1057/s41599-024-02778-z

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods, 40*(3), 879–891. https://doi.org/10.3758/BRM.40.3.879

Qiu, X., Wang, Y., Zeng, Y., & Cong, R. (2025). Artificial intelligence disclosure in cause-related marketing: A persuasion knowledge perspective. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(3), Article 193. https://doi.org/10.3390/jtaer20030193

Ranjan, R. (2024). The evolution of digital banking: Impacts on traditional financial institutions. *International Journal of Progressive Research in Engineering Management and Science, 4*(9), 753–763.

Riasat, I., Shah, M., & Gönül, M. S. (2025). Strengthening cybersecurity resilience: An investigation of customers' adoption of emerging security tools in mobile banking apps. *Computers*, *14*(4), Article 129. https://doi.org/10.3390/computers14040129

Ruzaili, H., Katuk, N., Zaini, K. M., & Abdullah, W. (2026). Phishing awareness and preventive measures among university students: Knowledge, behaviors, and victimisation perspectives. *Millennium—Journal of Education Technologies and Health*. https://doi.org/10.29352/mill0229.43489

Sabberwal, P., & Rastogi, M. (2025). Customer awareness and adoption of digital banking services: Effects on satisfaction and retention in cooperative banks of Uttarakhand. *International Journal of Economic Practices and Theories*. https://doi.org/10.52783/ijept.108

Sekaran, U., & Bougie, R. (2019). *Research methods for business: A skill-building approach* (8th ed.). John Wiley & Sons.

Silva, D., et al. (2024). How cybersecurity enhances trust and commitment to customer retention: The mediating role of robotic service quality. *Big Data and Cognitive Computing, 8*(11), Article 165. https://doi.org/10.3390/bdcc8110165

Sheikh, A. A., Hassan, N. M., Haneef, Z., & Nawaz, M. S. (2021). Mediating role of value co-creation and customer commitment between customer trust and customer loyalty in mobile banking of Pakistan. *Abasyn Journal of Social Sciences, 14*(1), 69–XX. https://doi.org/10.34091/AJSS.14.1.05

State Bank of Pakistan. (2018). *Security of digital payments* (PSD Circular No. 09 of 2018). https://www.sbp.org.pk/circulars/psd-circular-no-09-of-2018

Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics* (7th ed.). Pearson.

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data security, customer trust and intention for adoption of Fintech services: An empirical analysis from commercial bank users in Pakistan. *SAGE Open, 13*. https://doi.org/10.1177/21582440231181388

Zhengmeng, C., Malik, M., Hussain, M., & Hussain, S. (2024). Exploring customer retention dynamics: A comparative investigation of factors affecting customer retention in the banking sector using mediation-moderation approach. *Heliyon, 10*(19), Article e36919. https://doi.org/10.1016/j.heliyon.2024.e36919