The Impact of Cyber security Awareness on Customers' Trust and Adoption of Internet Banking in Palakkad District, Kerala

Gopalan P[1], Dr. Sathya Devi[2]
[1]*Research scholar, Dept. of Commerce, SNGC College, KG Chavadi, Coimbatore.*
[2]*Associate Professor & HOD, Dept. of Commerce, SNGC College, KG Chavadi, Coimbatore*

***Abstract*—The present study investigates the impact of cybersecurity awareness on customers' trust and adoption of internet banking in Palakkad District, Kerala. The research aims to understand how customers' knowledge and perception of cybersecurity risks influence their willingness to use digital banking services. The study employs a quantitative approach, collecting data through a structured questionnaire from a sample of bank customers in the district. The findings reveal that increased cybersecurity awareness positively impacts customers' trust in internet banking, which in turn enhances their adoption of these services. The results also highlight the importance of financial institutions proactively educating customers about cybersecurity best practices to foster a secure and reliable digital banking ecosystem. The study contributes to the existing literature on the intersection of cybersecurity, customer trust, and the adoption of innovative banking technologies, with practical implications for banks to strengthen their cybersecurity measures and communication strategies.**

I. INTRODUCTION

The rapid digitization of financial services in India has transformed how individuals manage their finances, driven by technological advancements and increased internet penetration (Singh & Srivastava, 2018). The banking sector has expanded significantly due to a growing middle class and government initiatives like the Pradhan Mantri Jan Dhan Yojana (Kaur et al., 2020). Digital banking solutions have enhanced customer experience, with the sector projected to grow from USD 111 billion to USD 421 billion by 2029 (IBEF). This growth presents opportunities for efficiency but also necessitates a focus on customer satisfaction, which is crucial for fostering loyalty and long-term adoption of digital services (Arora & Banerji, 2024).

Financial institutions are at the forefront of digital innovation, adopting technologies to improve operations and customer engagement (Osei et al., 2023). However, digitization has also introduced cybersecurity challenges. The COVID-19 pandemic accelerated digital banking adoption, but it also heightened vulnerabilities, with Indian banks facing an average of 2,525 cyberattacks in six months—far exceeding the global average (Tripathi, 2025). High-profile incidents, such as ransomware attacks disrupting payment systems for hundreds of banks, have underscored the need for robust security measures. The Reserve Bank of India has urged institutions to strengthen monitoring of critical systems like UPI, RTGS, and NEFT to counter these threats. Over the past two decades, financial sector cyberattacks have caused losses of $20 billion, with 69% targeting commercial banks (Haruna et al., 2022; Priyadarshani & Rengarajan, 2024).

Despite technological progress, India remains underbanked, highlighting the need for broader financial inclusion through digital banking (Jukariya & Singh, 2018). Internet banking has revolutionized financial operations by enabling remote transactions and real-time account monitoring. However, security concerns and lack of trust hinder widespread adoption (Hakkak et al., 2013). While digital banking offers speed and cost benefits, many customers remain wary due to risks like phishing and ransomware (Khan, 2014). Trust is critical—customers who doubt the security of their transactions may prefer traditional banking despite digital convenience (Al-Qawasmi, 2020).

The core challenge lies in balancing convenience with security. Banks must address cyber security risks to build customer confidence and encourage digital adoption (Mahmadi et al., 2016). Enhancing cyber security awareness among users is essential to mitigate threats and foster trust. Without this, the potential of digital banking in India may remain unrealized. Therefore, understanding the role of cyber security awareness in shaping customer trust and adoption is vital for the sustainable growth of internet banking in India.

Aim and Objectives of the study

1. To examine the level of cybersecurity awareness among customers using internet banking.
2. To analyze the impact of cybersecurity awareness on customer trust in internet banking services.
3. To assess how cybersecurity awareness influences the adoption of internet banking.
4. To identify key cybersecurity risks that affect customer confidence in internet banking.

II. REVIEW OF LITERATURE

The rise of digital banks, which offer a variety of financial services via digital platforms, has completely changed the banking sector thanks to the technology's rapid development (Asmar & Tuqan, 2024). But this change also carries significant cybersecurity risks. The safeguarding of financial data is paramount in this digital era, thereby making robust cybersecurity measures indispensable for sustaining trust and confidence in digital banking platforms (Asmar & Tuqan, 2024) (Asmar & Tuqan, 2024). Numerous studies have explored the intricate relationship between digital banking services and customer satisfaction, highlighting the importance of convenience, security, and personalization (Chu & Zhan, 2024). These studies have revealed that customers generally perceive digital banking services positively in terms of reliability and responsiveness, with significant associations found between these factors and overall customer satisfaction (Mwababa & Chrine, 2024).

Moreover, the interconnectedness of financial institutions and the increasing sophistication of cyberattacks have elevated the potential for systemic risk within the banking sector (Uddin et al., 2020). Cybersecurity incidents can trigger a cascade of consequences, ranging from financial losses and goodwill damage to regulatory penalties and loss of customer trust. As a result, regulators worldwide have intensified their scrutiny of cybersecurity practices within the financial industry, implementing stricter requirements and guidelines to enhance resilience against cyber threats.

The crucial Role of Cybersecurity Awareness

The banking industry has become a prime target for cyberattacks, which are growing in frequency, severity, and sophistication (Eskandarany, 2024). Cybersecurity awareness is now more crucial than ever to protect people and organizations from the growing threat landscape. Cybersecurity awareness entails understanding cybersecurity risks, recognizing potential threats, and adhering to best practices to protect oneself from cyberattacks. This includes knowing how to spot phishing scams, create strong passwords, securely manage online accounts, and protect sensitive data on both personal and business devices.

By raising awareness and promoting cybersecurity best practices, organizations can cultivate a culture of security that permeates all levels of operation (Umoga et al., 2024). Moreover, cybersecurity awareness extends beyond individual users to encompass organizations and communities. Organizations must prioritize cybersecurity awareness training for their employees to ensure that they are equipped to identify and respond to cyber threats effectively (Shillair et al., 2022). Cybersecurity awareness is especially crucial for internet banking customers, as they frequently handle sensitive financial data online. Cybersecurity awareness has become an essential element of the digital age, equipping individuals and organizations with the knowledge and tools they need to protect themselves against the ever-evolving threat landscape. Enterprises have become more aware of the significance of cybersecurity and information security management, viewing these issues as crucial for competitiveness and survival in global markets (Antunes et al., 2021). By investing in cybersecurity awareness initiatives, businesses can minimize the risk of cyberattacks, protect their assets, and preserve their reputation in an increasingly interconnected world (Alzahrani, 2022). A multi-faceted strategy is needed to address the dynamic character of cyber threats and provide ongoing cybersecurity education (Taherdoost, 2024).

H0 1: There is no significant relationship between cybersecurity awareness and the adoption of Internet banking.

Cyber security awareness on Customer's Trust

Trust serves as the bedrock of the customer-bank relationship, shaping customer perceptions, loyalty, and willingness to engage with banking services. The importance of trust cannot be emphasized enough, especially in the context of internet banking, where customers entrust financial institutions with their sensitive information and assets. (Kasemsan & Hunngam, 2011; Manzano et al., 2009)

The importance of trust in internet banking is underscored by the inherent risks associated with online transactions, including phishing, identity theft, and account hacking. Cybersecurity awareness plays a pivotal role in fostering customer trust in internet banking services. By educating customers about cybersecurity risks and best practices, banks can instill confidence in the security and reliability of their online platforms. When customers perceive that banks are proactive in protecting their interests, they are more likely to trust the institution and adopt internet banking services wholeheartedly. (Kaur & Arora, 2020; Tangmanee & Sritadawut, 2021)

Moreover, cybersecurity awareness initiatives should underscore the collaborative nature of online security, highlighting that both financial institutions and customers must actively participate in safeguarding transactions and data (Milosavljević & Njagojević, 2019). A synergistic relationship is paramount, where financial institutions not only deploy robust security infrastructures but also empower customers with the knowledge and tools necessary to fortify their own defenses in the digital domain (Dzomira, 2017). Cybersecurity awareness also helps to dismiss misconceptions and allay fears surrounding online banking. Cyberattacks on financial institutions can erode customer trust, leading to a decline in adoption rates and damage to the bank's reputation (Haruna et al., 2022).

H0 2: There is no moderating effect of digital literacy on the relationship between cybersecurity awareness and the adoption of Internet banking.

Impact on Adoption of Internet Banking

The adoption of internet banking has revolutionized the banking sector, offering customers unparalleled convenience, accessibility, and efficiency in managing their finances (Islam, 2020). Cybersecurity awareness significantly impacts the adoption of internet banking services by influencing customer perceptions of risk, trust, and usability. (Mahmadi et al., 2016) When customers are well-informed about cybersecurity risks and the measures, they can take to protect themselves, they are more likely to perceive internet banking as a safe and secure channel for conducting financial transactions. (Stephen et al., 2015) Banks that proactively address these security apprehensions and equip their clients with the requisite knowledge and resources for secure online navigation are poised to cultivate heightened trust and assurance in internet banking platforms, which will translate to greater adoption rates and heightened customer satisfaction.(Kasemsan & Hunngam, 2011) Cybersecurity awareness empowers customers to make informed decisions about their online banking activities, reducing their susceptibility to fraud and enhancing their overall experience (Singh, 2006). Furthermore, cybersecurity awareness can promote the adoption of internet banking by highlighting its benefits in terms of convenience, speed, and cost savings.

H0 3: There is no moderating effect of digital literacy on the relationship between cybersecurity awareness and the adoption of Internet banking.

III. DATA AND METHODOLOGY

A survey was conducted to collect quantitative data, which has been analyzed using statistical methods. The study involved a sample of 114 internet banking customers in Palakkad district, Kerala, India, assessing their cybersecurity awareness levels, trust in internet banking, and adoption rates. The research model proposes that cybersecurity awareness positively influences trust in internet banking, which in turn positively influences the adoption of internet banking (Nor & Pearson, 2008). The study employed a convenience sampling method to collect data, with 200 questionnaires sent to different professionals, of which 120 were returned, and 114 were found suitable for analysis. Before dispatching the questionnaires, a pilot study was conducted to test the validity of the questionnaire, and necessary amendments were made. The collected data has been analyzed using statistical software such as SPSS and R to test the hypotheses and draw meaningful conclusions. The findings of this study offer valuable insights for banks and

policymakers in India to enhance cybersecurity awareness among customers and promote the safe and widespread adoption of internet banking, thereby bolstering the country's digital economy (Kesharwani & Bisht, 2012). By emphasizing the ease of use and accessibility of internet banking platforms, banks can attract new customers and retain existing ones, driving further growth in the digital banking sector.

IV. RESULT AND DISCUSSION

Summary of Demographic Variables-

The demographic analysis reveals interesting insights. The majority of respondents fall within the 26-34 and 35-43 age groups, indicating that middle-aged adults are the primary users of online banking. The gender distribution is nearly balanced, with a slightly higher number of male participants. Most respondents have been using online banking for 5 to 13 years, suggesting a significant level of experience among users. The largest group of respondents works in the manufacturing sector, followed by insurance and other occupations. These findings suggest that internet banking services have gained widespread adoption, particularly among middle-aged and experienced users across various industrie**s.**

Correlational Analysis

	Adequate Knowledge of Cybersecurity Risks	*Awaress of security measures for online banking*	*Understad Security Measures taken by my banks*	*Awareness of Safe Online Banking Practices*	*Customer Trust in Online banking*	*Confidence in the Bank's Security Measures*	*Perception of Risk in Internet Banking*	*Adoption of Internet Banking*	*Frequency of Online Banking Transacti*
Adequate Knowledge of Cybersecurity Risks	1								
Awaress of security measures for online banking	0.019372	1							
Understad Security Measures taken by my	-0.08365	-0.00397	1						
Awareness of Safe Online Banking Practices	0.003175	0.005965	-0.0909	1					
Customer Trust in Online banking	-0.07783	-0.06594	0.019123	0.069944	1				
Confidence in the Bank's Security Measures	-0.06646	0.043446	-0.08599	0.003495	0.070159	1			
Perception of Risk in Internet Banking	-0.02465	-0.11538	0.028473	-0.12991	0.072174	-0.01814	1		
Adoption of Internet Banking	0.063205	-0.18049	0.025888	-0.01443	0.032377	0.072528	0.025874	1	
Frequency of Online Banking Transactions	-0.08365	-0.00397	1	-0.0909	0.019123	-0.08599	0.028473	0.025888	1

Source: Author's Caluclation

The correlation analysis reveals no strong linear relationships between the variables. The observed correlations are relatively weak, ranging from 0.070 to -0.180, suggesting modest associations. The positive correlations of 0.070 and 0.073 indicate a slight tendency for customers who trust their bank to have higher confidence in its security measures, and that higher confidence in security measures may marginally encourage adoption of internet banking. The correlation of 0.072 implies that perceived risk in internet banking might have a minor influence on trust levels. The negative correlation of -0.130 suggests a weak relationship where greater awareness of safe practices may slightly reduce perceived risks. The negative correlation of -0.180 indicates that individuals with higher awareness of security measures might be slightly less inclined to adopt internet banking. The negative correlation of -0.086 implies a weak relationship where greater understanding of bank security measures may be associated with slightly lower frequency of online banking transactions. Overall, the small correlations suggest limited linear relationships between the variables, warranting further investigation into potential nonlinear or complex associations.

Cyber security Awareness and Adoption of Internet Bankin

Regression Statistics	
Multiple R	0.100294
R Square	0.010059
Adjusted R Square	0.00122
Standard Error	0.616069
Observations	114

ANOVA					
	df	*SS*	*MS*	*F*	*Sig F*
Regression	1	0.431931	0.431931	1.138034	0.288362
Residual	112	42.50862	0.379541		
Total	113	42.94055			

Source: Calculated by the author.

The regression analysis revealed that the correlation between customer trust and the adoption of internet banking is very weak, with a multiple R of 0.0426. Additionally, the R-squared value of 0.0018 indicates that less than 1% of the variance in internet banking adoption is explained by customer trust. The negative adjusted R-squared value of -0.0071 further suggests that including customer trust as a predictor actually

worsens the model's ability to explain the variance. Furthermore, the significance F of 0.6527 indicates that the overall model is not statistically significant, implying that customer trust does not have a meaningful impact on the adoption of internet banking. Consequently, we accept the null hypothesis that there is no significant relationship between cybersecurity awareness and the adoption of internet banking.

Customer Trust and Adoption of Internet Banking

Regression Statistics	
Multiple R	0.042603
R Square	0.001815
Adjusted R Square	-0.0071
Standard Error	0.622262
Observations	114

ANOVA					
	df	*SS*	*MS*	*F*	*Signi F*
Regression	1	0.078857	0.078857	0.203655	0.652659
Residual	112	43.36754	0.38721		
Total	113	43.44639			

Source: Calculated by the author.

The regression analysis revealed a very weak positive correlation between customer trust and the adoption of internet banking, with a multiple R of 0.0426. Furthermore, the R-squared value of 0.0018 indicates that less than 1% of the variance in internet banking adoption is explained by customer trust. The negative adjusted R-squared value of -0.0071 further suggests that including customer trust as a predictor actually worsens the model's ability to explain the variance. Additionally, the significance F of 0.6527 indicates that the overall model is not statistically significant, implying that customer trust does not have a meaningful impact on the adoption of internet banking. Therefore, we accept the null hypothesis that there is no moderating effect of digital literacy on the relationship between cybersecurity awareness and the adoption of internet banking.

Cyber security and Adoption of Internet banking: -

Regression Statistics	
Multiple R	0.621041
R Square	0.385692
Adjusted R Square	0.368939
Standard Error	0.492576
Observations	114

ANOVA					
	df	*SS*	*MS*	*F*	*Sign F*
Regression	3	16.75695	5.585649	23.02114	1.22E-11
Residual	110	26.68945	0.242631		
Total	113	43.44639			

Source: Calculated by the author.

The multiple regression analysis, based on 114 observations and three cybersecurity awareness variables, demonstrated moderate explanatory power, with an R-squared of 0.386 and an adjusted R-squared of 0.369. The overall model was statistically significant, suggesting that the cybersecurity awareness factors had a meaningful relationship with the outcome variable.

The strongest predictor was "Understand Security Measures taken by my banks," with a highly significant positive coefficient of 0.352. This implies that educational efforts to help individuals better comprehend their bank's security measures could have the most substantial impact on the adoption of internet banking.However, the variable "Awareness of security measures for online banking" exhibited a statistically significant negative relationship with the dependent variable, indicating that merely being aware of security measures, without a deeper understanding, can create a false sense of security.

In contrast, the variable "Adequate Knowledge of Cybersecurity Risks" did not demonstrate a statistically significant relationship, suggesting that general risk awareness alone may not be sufficient to influence the outcome. The model explained approximately 38.6% of the variance in the dependent variable, leaving 61.4% unexplained, implying that other significant factors not captured in this analysis likely influence the adoption of internet banking.

Therefore, we reject the Null Hypothesis, which stated that there is no moderating effect of digital literacy on the relationship between cybersecurity awareness and the adoption of Internet banking.

V. CONCLUSION

This comprehensive study sheds light on the critical relationship between cybersecurity awareness and the adoption of internet banking services in India. The findings suggest that a deep, holistic understanding of the security measures implemented by banks plays a pivotal role in driving the widespread adoption of these digital banking solutions.

Interestingly, the research also revealed that mere awareness of security risks, without a comprehensive understanding, can actually hinder adoption by creating a false sense of security among customers. This aligns with previous studies, which have highlighted the importance of fostering robust cybersecurity literacy among digital banking users (Alalwan et al., 2016; Martins et al., 2014). The results of this analysis underscore the vital importance of educational initiatives that empower customers to better comprehend the security practices of their banks. By nurturing this understanding, financial institutions can potentially strengthen customer trust and encourage more widespread adoption of convenient digital banking services - a finding corroborated by research demonstrating the link between trust, satisfaction, and digital banking adoption (Ul Haq, 2020; Kesharwani & Bisht, 2012).

However, it's important to note that while this study explained a significant portion of the variance in internet banking adoption, other crucial factors, such as user experience, perceived utility, and demographic characteristics, likely influence this outcome. Further research is needed to uncover the full range of determinants shaping customer decisions to utilize internet banking, as suggested by studies exploring the multifaceted nature of digital banking adoption (Martins et al., 2014; Alalwan et al., 2016). Conversely, some studies have suggested that mere awareness of cybersecurity risks, without a deep understanding, can actually motivate users to adopt internet banking services, as they seek to mitigate perceived threats (Alharbi, 2020; Tam & Oliveira, 2017). This highlights the complex and potentially non-linear relationships between cybersecurity awareness, trust, and digital banking adoption.

Overall, this comprehensive analysis provides valuable insights for banks and policymakers seeking to promote the secure and widespread adoption of digital financial services in India. By empowering customers with knowledge and building trust in cybersecurity measures, the industry can continue to drive innovation and financial inclusion in the digital age.

VI. LIMITATION AND FUTURE RESEARCH

The study has some limitations that need to be acknowledged. First, the sample was limited to customers in India, which may not be representative of customers in other countries. Second, the study only considered a limited number of factors that may influence the adoption of internet banking (Joshi et al., 2019).

Future research could address these limitations by including a more diverse sample of customers and considering a wider range of factors. Future studies could also explore the impact of cybersecurity awareness on other types of digital banking services, such as mobile banking and online payments.

REFERENCES

[1] Al-Qawasmi, K. (2020). Proposed E-payment Process Model to Enhance Quality of Service through Maintaining the Trust of Availability. International Journal of Emerging Trends in Engineering Research, 8(6), 2296. https://doi.org/10.30534/ijeter/2020/16862020

[2] Alzahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. International Journal of Advanced Computer Science and Applications, 13(1). https://doi.org/10.14569/ijacsa.2022.01301102

[3] Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. F. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219. https://doi.org/10.3390/jcp1020012

[4] Arora, P., & Banerji, R. (2024). The impact of digital banking service quality on customer loyalty: An interplay between customer

experience and customer satisfaction. Asian Economic and Financial Review, 14(9), 712. https://doi.org/10.55493/5002.v14i9.5199

[5] Asmar, M., & Tuqan, A. (2024a). Integrating Machine Learning for Sustaining Cybersecurity in Digital Banks. https://doi.org/10.2139/ssrn.4686248

[6] Asmar, M., & Tuqan, A. (2024b). Integrating Machine Learning for Sustaining Cybersecurity in Digital Banks. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e37571

[7] Axis Bank. (2024). Cyber Security in Banking: Importance, Challenges & Tips. https://www.axisbank.com/progress-with-us-articles/digital-banking/cyber-security-in-banking

[8] Bueno, L. A., Sigahi, T. F. A. C., Rampasso, I. S., Filho, W. L., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. International Journal of Information Management Data Insights, 4(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230

[9] Chinni, Mr. N., Mohini, Dr. P. V., & Mr.S.Srinadh. (2021). IMPACT OF DIGITALIZATION OF BANKS. EPRA International Journal of Multidisciplinary Research (IJMR), 187. https://doi.org/10.36713/epra6556

[10] Chu, H., & Zhan, X. (2024). The Impact of Digital Banking Services on Customer Satisfaction. Frontiers in Business Economics and Management, 15(3), 356. https://doi.org/10.54097/5qaf7d23

[11] Dzomira, S. (2017). Internet banking fraud alertness in the banking sector: South Africa. Banks and Bank Systems, 12(1), 143. https://doi.org/10.21511/bbs.12(1-1).2017.07

[12] Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: a qualitative survey of board of directors. Frontiers in Artificial Intelligence, 7. https://doi.org/10.3389/frai.2024.1440051

[13] Galazova, S. S., & Магомаева, Л. Р. (2019). The Transformation of Traditional Banking Activity in Digital. International Journal of Economics and Business Administration, 41. https://doi.org/10.35808/ijeba/369

[14] Hakkak, M., Vahdati, H. A., & Biranvand, V. P. (2013). An extended technology acceptance model for detecting influencing factors: An empirical investigation. Management Science Letters, 2795. https://doi.org/10.5267/j.msl.2013.09.030

[15] Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022a). Defending against cybersecurity threats to the payments and banking system. arXiv (Cornell University). https://doi.org/10.48550/arXiv.2212.

[16] Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022b). Defending against cybersecurity threats to the payments and banking system. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2212.12307

[17] Islam, S. (2020). Enhanced Information System Security in Internet Banking and Manufacturing. International Journal of Engineering Materials and Manufacture, 5(2), 62. https://doi.org/10.26776/ijemm.05.02.2020.05

[18] Jukariya, T., & Singh, S. (2018). Topic: Assessment of Female Customers' Level of Satisfaction from E-Banking. International Journal of Current Microbiology and Applied Sciences, 7(4), 3408. https://doi.org/10.20546/ijcmas.2018.704.385

[19] Kasemsan, M. L. K., & Hunngam, N. (2011). Internet Banking Security Guideline Model for Banking in Thailand. Communications of the IBIMA, 1. https://doi.org/10.5171/2011.787725

[20] Kaur, J., Kaur, S., Syan, A. S., & Sharma, R. R. (2020). Factors Influencing the Adoption of Payment Banks in India Using an Extended TAM. Asia-Pacific Journal of Management Research and Innovation, 16(4), 309. https://doi.org/10.1177/2319510x211013598

[21] Kesharwani, A., & Bisht, S. S. (2012). The impact of trust and perceived risk on internet banking adoption in India. International Journal of Bank Marketing, 30(4), 303. https://doi.org/10.1108/02652321211236923

[22] Khan, H. U. (2014). E-banking: Online Transactions and Security Measures. Research Journal of Applied Sciences Engineering and Technology, 7(19), 4056. https://doi.org/10.19026/rjaset.7.766

[23] Kumar, J., & Gupta, S. S. (2023). Impact of Artificial Intelligence towards customer

relationship in Indian banking industry. Gyan Management Journal, 17(1), 105. https://doi.org/10.48165/gmj.2022.17.1.12

[24] Mahmadi, F., Zaaba, Z. F., & Osman, A. M. (2016). Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security. IOP Conference Series Materials Science and Engineering, 160, 12107. https://doi.org/10.1088/1757-899x/160/1/012107

[25] Milosavljević, N., & Njagojević, S. (2019). Customers' perception of information security in internet banking. https://doi.org/10.2991/senet-19.2019.45

[26] Mwababa, Y. C., & Chrine, C. H. (2024). Assessing The Effect of Digital Banking Services on Retail Banking Customers' Satisfaction Levels in Lusaka's Central Business District. Journal of Economics Finance and Management Studies, 7(7). https://doi.org/10.47191/jefms/v7-i7-74

[27] Nor, K. M., & Pearson, J. (2008). An Exploratory Study into the Adoption of Internet Banking in a Developing Country: Malaysia. Journal of Internet Commerce, 7(1), 29. https://doi.org/10.1080/15332860802004162

[28] Osei, L. K., Cherkasova, Y., & Oware, K. M. (2023). Unlocking the full potential of digital transformation in banking: a bibliometric review and emerging trend [Review of Unlocking the full potential of digital transformation in banking: a bibliometric review and emerging trend]. Future Business Journal, 9(1). Springer Science+Business Media. https://doi.org/10.1186/s43093-023-00207-2

[29] Priyadarshani, K. M. C., & Rengarajan, A. (2024). Cybersecurity in the Financial Sector. International Journal of Research Publication and Reviews, 5(3), 751. https://doi.org/10.55248/gengpi.5.0324.0709

[30] Purbey, U. K. (2020). Customer Satisfaction in Indian Banking Services: Problems and Solutions. International Journal of Advanced Academic Studies, 2(4), 134. https://doi.org/10.33545/27068919.2020.v2.i4c.342

[31] Ramachentrayar, P., & Ram, P. S. (2022). A Study on Customers' Satisfaction with E-Banking Services with Special Reference to the Madurai District Central Cooperative Bank LTD. Shanlax International Journal of Arts Science and Humanities, 9, 129. https://doi.org/10.34293/sijash.v9is1-may.5949

[32] Saha, M. (2023). Can Your Bank Avoid Cyber Attacks? https://www.rediff.com/business/report/can-your-bank-avoid-cyber-attacks/20231201.htm

[33] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Solms, B. von. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

[34] Singh, S. (2006). The Social Dimensions of the Security of Internet Banking. Journal of Theoretical and Applied Electronic Commerce Research, 1(2), 72. https://doi.org/10.3390/jtaer1020014

[35] Singh, S., & Srivastava, R. K. (2018). Predicting the intention to use mobile banking in India. International Journal of Bank Marketing, 36(2), 357. https://doi.org/10.1108/ijbm-12-2016-0186

[36] Stephen, W., Hsu, M. K., Pelton, L. E., & Liu, A. H. (2015). Risky Business? Consumers' Propensity to Engage in Online Banking Services. In Developments in marketing science: proceedings of the Academy of Marketing Science (p. 337). Springer International Publishing. https://doi.org/10.1007/978-3-319-24184-5_88

[37] Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information, 15(9), 512. https://doi.org/10.3390/info15090512

[38] Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239. https://doi.org/10.1057/s41283-020-00063-2

[39] Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies [Review of A critical review of emerging cybersecurity threats in financial technologies]. International Journal of Science and Research Archive, 11(1), 1810. https://doi.org/10.30574/ijsra.2024.11.1.0284

[40] Vats, L., & Maheshwari, A. (2019). Role of Customer's Trust on the Adoption of Internet

Banking in Gwalior City. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3308030