Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 07 Issue 12 December 2024

Article DOI: 10.47191/jefms/v7-i12-28, Impact Factor: 8.044

Page No: 7215-7224

The Effect of Perceived Security Risks on Mobile Banking Adoption in Fashion Retail Industry. A Case Study of Mwanza Region, Tanzania

Albert Moshi

Tanzania Institute of Accountancy, P.O. Box 9522, Dar es Salaam, Tanzania

ABSTRACT: The adoption of mobile banking among fashion retailers is increasingly recognized as a powerful catalyst for economic empowerment and financial inclusion. It reduces reliance on traditional banking methods, allowing consumers and suppliers to engage in transactions without the constraints of banking hours or physical locations. This flexibility enables online transactions to occur anytime and anywhere, fostering a more dynamic and responsive shopping environment. However, its adoption is very limited in fashion industry. This study was set to explore security issues that affect adoption of mobile banking by fashion retailers in Mwanza municipal councils. The study is grounded on perceived risk theory which explain how individuals assess risk and make decisions under uncertainty. The data for this study were collected using a close-ended questionnaire distributed to a sample of 138 respondents, who were selected through a simple random sampling technique. The study employed a combination of content analysis and binary logistic regression analysis as its analytical approach. The study revealed a negative effect of fraud, phishing attacks, and transaction errors on the adoption of mobile banking, while highlighting the positive influence of security literacy in encouraging this adoption. The study concluded that that mobile banking service providers should implement comprehensive user education programs focused on security best practices, including the importance of strong passwords and awareness of phishing schemes. Additionally, enhancing authentication methods and establishing robust transaction error resolution processes that can mitigate risks and foster greater trust in mobile banking among fashion retailers.

KEY WORDS: mobile banking, perceived security risk, fashion industry, perceived risk theory

INTRODUCTION

Globally, the rise of mobile banking has revolutionized financial transactions, providing convenience and accessibility like never before in fashion retail industry. It offers unprecedented opportunities for economic empowerment and financial inclusion (Aziz *et al.,* 2022). Mobile banking refers to financial transactions conducted through mobile devices, enabling users to make payments, transfer money, and access banking services without the need for physical cash or traditional banking infrastructure (Siano *et al.,* 2020). Mobile banking platforms have emerged as a promising solution, enabling fashion retail industry to engage more effectively in the financial system, conduct transactions, and manage their finances efficiently (Hultberg & Pal, 2021). The widespread availability and affordability of smartphones, along with reliable internet access in urban areas, has created a solid foundation for the growth of mobile banking among fashion retailers (Jibril *et al.,* 2020). Banks, telecommunications companies, and other financial institutions facilitate mobile banking services. Telecommunications providers such as Vodacom, Halotel, Tigo, and Airtel play a crucial role in ensuring reliable internet connectivity with their respective banking networks (Msengi, 2022). Meanwhile, banks such as CRDB, NMB, Standard Chartered, United Bank for Africa (UBA), Exim Bank**,** TPB Bank offer mobile apps that allow users to manage their accounts seamlessly and enable individuals to send and receive funds, make purchases, and access a variety of financial services directly from their mobile devices. This flexibility empowers users to conduct financial transactions anytime and anywhere, significantly reducing reliance on cash and traditional banking systems (Kasowaki & William, 2024). However, study shows that this increased reliance on digital platforms has also attracted hackers and other malicious actors who seek to exploit vulnerabilities within these financial networks (Nish *et al.,* 2022). As mobile banking continues to expand, cybercriminals work tirelessly to identify and infiltrate these financial systems (Ibrahimnur, 2023). Hackers typically centre around stealing money, personal information, or accessing sensitive data using variety of tactics such as phishing attacks, fake mobile bank apps, and social

engineering, to deceive users and bypass security measures (Chanti & Chithralekha, 2022). Study shows that the implications of these security threats endanger individual financial information and weaken consumer trust in mobile banking (Sanni *et al.,* 2023). Literature shows that lack of digital security skills among users significantly heightens the risks associated with mobile banking (Hanif & Lallie, 2021). If users not equipped with the knowledge of best security practices, become more vulnerable to cyber threats. Without a clear understanding of how to identify fraudulent tactics, users may easily fall victim to phishing scams or other deceptive tactics used by cybercriminals (Alkhalil *et al.,* 2021). Additionally, study shows that the inability to effectively recover from transaction errors or report suspicious activities can exacerbate financial losses (Razaq *et al.,* 2021). The study demonstrates that users who possess adequate knowledge of security best practices are less likely to fall victim to hackers (Bitzer *et al.,* 2021). Security literacy enables them to recognize potential threats, such as phishing attempts and fraudulent schemes, and adopt proactive measures to protect their personal information (Bhardwaj *et al.,* 2021).

Recognizing this transformative potential of mobile banks for economic growth and financial inclusion, the Tanzania government has streamlined regulatory frameworks to facilitate the operation of mobile bank platforms (Mapunda, 2022). The Tanzanian government, through the Bank of Tanzania (BoT), has established a comprehensive regulatory framework that fosters mobile banking by prioritizing stability, security, and consumer protection. BoT is responsible for licensing and supervising mobile network operators and financial institutions that wish to offer mobile banking services, ensuring that they meet specific operational standards and regulations. This framework not only promotes a safe and reliable environment for mobile banking but also enhances consumer trust and encourages broader financial inclusion across the country. However, Despite the government efforts and potential benefits offered by mobile banks, its adoption among fashion retail industry in Mwanza remains limited (Macha & Massawe, 2023). Concerns regarding perceived security issues have caused hesitation, leading many to refrain from fully embracing these innovative financial solutions (Ali *et al.,* 2021). while some studies have examined the impact of security risks on mobile banking adoption (Souiden *et al.,* 2021) they frequently lack fashion retail industry specific perspective, failing to consider how factors such as fraud and phishing, customer trust, transaction errors and security literacy affect fashion retailers and their customers in mobile banking adoption. Thus, this study examined security issues specifically focusing on fraud and phishing, security literacy and transaction errors that affect the adoption of mobile banking by fashion retail industry in Mwanza region.

Literature review

Security issues play a pivotal role in the adoption of mobile money payment services, significantly influencing user confidence and willingness to engage with these platforms. Concerns about potential threats, such as fraud, data breaches, and unauthorized transactions, can deter individuals from utilizing mobile bank services (McCray, 2023). The fear of falling victim to scams or losing the hard-earned money can overshadow the convenience and benefits mobile bank offer to fashion retail industry (Banerjee, 2024).

Fraud and Phishing

Fraud and phishing are significant threats that impact mobile banking, creating barriers for its adoption. Fraud refers to deceptive practices aimed at illegally obtaining money or personal information, while phishing involves tricking individuals into revealing sensitive data, such as passwords or financial information, often through fraudulent emails or messages that appear legitimate (Nadeem *et al.,* 2023). These security threats can lead to substantial financial losses for users, fostering a climate of fear and scepticism around mobile bank platforms (Lestari et al., 2024). fashion retailers can be vulnerable to various types of fraud and phishing attacks that threaten their financial security. phishing scams is the common tactic where attackers send fraudulent messages or emails that appear to be from legitimate customer or supplier, urging users to click on links and enter personal information, such as passwords or account numbers (Zhang, 2021).Users may face account takeover risks, where cybercriminals utilize stolen credentials obtained through phishing or data breaches to gain unauthorized access to a victim's bank account, enabling them to withdraw funds or make unauthorized transactions (Rajendran, 2024). Additionally**,** fake mobile bank apps can deceive users into downloading counterfeit mobile bank applications that mimic genuine ones but are designed to steal personal information or funds (Sharma et al., 2021). Fraud and phishing tactics pose significant barriers to the widespread adoption of mobile bank services (Iyelolu *et al.,* 2024).

Transaction errors

Transaction errors refer to mistakes or malfunctions that occur during the processing of financial transactions, which can include incorrect amounts being transferred, failed transactions, or unauthorized payments (Dhobe *et al.,* 2020). These errors can arise from user input mistakes, or connectivity issues, leading to significant frustration and confusion for users (Ebert *et al.,* 2021). When

fashion retailers experience transaction errors without appropriate and timely support, their confidence in mobile banking can be severely weakened. If they are unable to resolve issues quickly, they may fear losing money or having their financial information compromised, which can lead to a reluctance to adopt mobile bank financial services (Dzidzah *et al.,* 2020). The absence of efficient customer support channels exacerbates the situation, as users may feel abandoned or helpless in addressing their concerns (Jain *et al.,* 2023)

Security digital literacy

Security digital literacy refers to the understanding and skills necessary to navigate digital environments safely, particularly regarding the protection of personal information and financial assets (Roszkowska, 2021). It includes knowledge of how to create strong passwords, recognize phishing attempts, use security features effectively, and understand the risks associated with online transactions (Desolda *et al.,* 2021). lack of security digital literacy can significantly hinder the adoption of mobile bank services. Individuals who are not digitally literate increases the risk of unauthorized access to their accounts (Kocabas *et al.,* 2021). Inadequate knowledge of security best practices and familiarity with phishing and fraud may inadvertently expose fashion retailers to cyberattacks (Sandell, 2021). These malicious vulnerabilities create a sense of fear and scepticism about using mobile banking.

Theoretical literature review

This study is grounded on perceived risk theory developed by Bennett in the year1970. This theory posits that that individual assesses the potential risks associated with a particular action or activity, influencing their willingness to engage in that activity. In the context of this study, which examines the effect of perceived security risks on the adoption of mobile banking, if fashion retailers are aware of the prevalence of phishing scams or the possibility of transaction errors leading to financial loss, their apprehension about using mobile banking increases. Security issues such as fraud, phishing, and transaction errors can significantly hinder the adoption of mobile banking services. Perceived risk theory has been widely utilized in various fields such as banking (Karki *et al.,*2024.), e-commerce (Handoyo, 2024), e-learning (Sitar *et al.,*2024.) demonstrating its robustness and reliability in understanding user behaviour in the face of uncertainty.

Conceptual Framework

This conceptual framework serves as a structured representation that outlines how fraud and phishing, transaction error recovery, and security literacy affect mobile bank adoption among fashion retail industry in Mwanza city councils. Fraud and phishing encompass fears related to fraud and phishing attacks, which negatively impact user confidence and hinder the willingness to adopt mobile banking. Transaction error recovery focuses on the effectiveness of resolving transaction issues; difficulties in this area can lead to feelings of insecurity, further deterring adoption. On the positive side, security literacy refers to users' understanding of security best practices. Higher levels of security literacy can significantly enhance confidence in mobile banking, encouraging greater acceptance of these services.

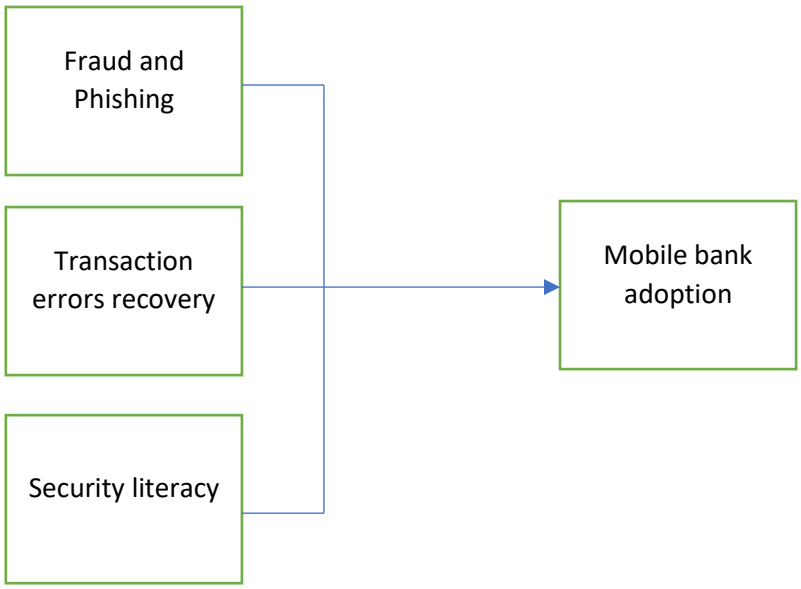

Fig.1 Proposed conceptual framework

METHODOLOGY

Research Approach

This study employed a mixed-methods approach, integrating both quantitative and qualitative research methods to comprehensively examine the determinants influencing the adoption of mobile banking by fashion retailers. The quantitative data were essential for statistical analysis, providing measurable insights into patterns of mobile banking usage. In contrast, the qualitative data offered a deeper understanding on personal experiences and perceptions. By utilizing both approaches, the study leverages the strengths of each method.

Research Design

The study adopted a cross-sectional design, which allows for the collection of data at a single point in time, providing a snapshot of the current attitudes and experiences of the target population. Given the diverse and dynamic nature of mobile banking adoption, this design facilitates the exploration of various security factors affecting its uptake among fashion retailers. Moreover, a cross-sectional approach enhances the efficiency of data collection while enabling researchers to draw meaningful conclusions about the phenomenon under investigation.

Study area

This study was conducted in Mwanza region specifically Mwanza city councils (Nyamagana and Ilemela) due to its strategic significance as a business hub for the Lake Zone countries and its unique position within the fashion retail industry. Many fashion retailers in Mwanza rely on Dar es Salaam as their primary sourcing point for their products, With the distance involved in transporting goods, mobile banking emerges as a vital solution, enabling retailers to make timely payments and manage their finances seamlessly. Additionally, the rapid growth of the online presence of the fashion industry has transformed the way retailers engage with customers and suppliers. As more fashion businesses establish their online platforms, the need for mobile banking becomes increasingly critical.

Population and Sample Size and sampling strategy

The study population comprised all fashion retailers within Mwanza City Councils (Nyamagana and Ilemela), totalling 210 hundred individuals obtained from their association register and database. The sample size was calculated by using statistical formula by Yamane, (1967). Given the study population of 210 fashion retailers, the error margin of 5% and confidence level of 95%; Based on the statistical formula by Yamane, (1967):

$$n=\frac{N}{1+Ne^2}$$

Where: n–Sample size, N–Population size, e- error margin

$$n=\frac{210}{1+210(0.05)^2}$$

Therefore, sample size was 138 fashion retailers

Sampling strategy

The sampling strategy employed a combination of simple random sampling and purposive sampling approaches. For the quantitative component, a simple random sampling technique was utilized to select the sample. A sample frame was obtained from the database of the fashion retailers association, which provided a comprehensive list of fashion retailers along with their mobile numbers, facilitating effective communication with selected participants. This approach was crucial in minimizing selection bias, ensuring that each fashion retailer in the population had an equal opportunity to be included in the sample (Colasante & D'Adamo, 2021). Conversely, purposive sampling was employed to gather insights from key informants that might not be fully captured through quantitative measures alone (Abdul-Sater *et al.,* 2020). This strategy involved intentionally selecting individuals with specific knowledge or experience relevant to mobile banking adoption, including seven leaders from the fashion retail association.

Data collection methods

Data for this study was collected through a combination of structured closed-ended questionnaires and semi-structured interviews. The closed-ended questions were created to provide specific responses in 5-likert scale, enabling participants to select from predefined options. This structured approach facilitated the efficient collection of quantitative data, which is crucial for statistical analysis. Additionally, semi-structured interviews were conducted to gather qualitative insights from key informants. This method allowed for a more flexible dialogue, enabling the interviewer to delve deeper into specific topics while still addressing essential questions related to mobile banking.

Data analysis

The study employed both content analysis and binary logistic regression to comprehensively examine the security issues affecting the adoption of mobile banking among fashion retailers in Mwanza. The rationale for utilizing these two data analysis methods lies in their complementary strengths, which together provide a richer understanding of the security landscape surrounding mobile banking adoption. Content analysis was used to analyze qualitative data gathered from in-depth interviews with fashion retailers. This method allowed for the identification of key themes such as fraud and phishing, transaction error recovery and security literacy. By systematically coding and categorizing responses, content analysis provided nuanced insights into the lived security issues experiences and perceptions of participants, revealing both motivators and barriers to adopting mobile banking. On the other hand, binary logistic regression analysis was employed to examine quantitative data collected through structured surveys. This method enabled the researchers to quantify security factors among respondents, providing a statistical framework for understanding their influence in mobile banking adoption.

$$\log(Odds\ Ratio) = log\left(\frac{Yi=Adopted\ mobile\ banking}{Yi=Not\ adopted\ mobile\ babking}\right) = Xi\beta'$$

Ethical Consideration

The researcher ensured full compliance with all research ethics and practices throughout the study. All participants were thoroughly informed of their rights, which included receiving comprehensive information about the study, providing informed consent before participation, and the assurance of voluntary involvement. Participants were also informed of their right to withdraw from the study at any time, as well as the measures in place to protect their confidentiality and the information they provided.

FINDINGS

Assessment of Assumptions in Binary Logistic Regression

The study assessed the assumptions of multicollinearity, outliers, and the linearity of logits for binary logistic regression as presented in table 1.

Table 1 Assessment of Binary Logistic Regression assumptions

	VIF	Cook's Distance Test	Box-Tidwell Test
Fraud and Phishing	1.025	0.05	0.12
Transaction error recovery failure	2.821	0.02	0.25
Security Literacy	2.232	0.015	0.08

Multicollinearity was evaluated using the Variance Inflation Factor (VIF), with all values falling below 5, indicating no multicollinearity among the independent variables. Outliers were examined through Cook's Distance, revealing all values below 1, which confirms the absence of influential outliers. Additionally, the linearity of logits was tested using the Box-Tidwell test, resulting in a p-value of 0.15, exceeding the 0.05 threshold and satisfying the linearity assumption. These findings collectively support the validity of the binary logistic regression model used in the study, as all assumption criteria have been successfully met.

Construct Reliability

Before conducting the analysis of constructs, we assessed the internal consistency reliability of the measure to determine how closely related the items were to each other as presented in table 2.

Table 2. Construct reliability

Construct	No of items	Cronbach alpha
Fraud and phishing (FP)	4	0.718
Transaction error recovery (TER)	3	0.772
Security literacy (SL)	4	0.753
Adoption of mobile Banking (AMB)	1	0.798

This was evaluated using Cronbach's alpha, which exceeded the threshold of 0.7, indicating satisfactory reliability (Kennedy, 2022). Additionally, we performed a factor loading analysis, accepting items with a loading of 0.5 or above, which suggests a moderate correlation between the items and their respective factors (Schreiber, 2021)

Binary logistic regression analysis

A binary logistic regression analysis was conducted to estimate the logit model concerning mobile banking adoption within the fashion retail industry. Given that the responses for the dependent variable (adoption of mobile banking) were measured by assigning a value of one for fashion retailers had adopted mobile banking and a value of zero (0) for retailers who have not adopted mobile banking (Souiden *et al.,* 2021)

Binary Logistic Regression Goodness of Fit Test

The Binary Logistic Regression Goodness of Fit Test is a statistical assessment used to evaluate how well a logistic regression model fits the observed data (Nattino *et al.,* 2020) as shown in table 3. The test determines whether the model adequately describes the relationship between the predictor variables and the binary outcome.

Table3. Hosmer and Lameshow Goodness of Fit Test

step	Chi-Square	Df	Sig
1	9.92	7	0.289

As shown in Table 3, the Hosmer and Lemeshow test was employed to assess the goodness of fit for the model. The results indicate that the model is a good fit for the data, with a p-value of 0.298, which is greater than the threshold of 0.1 (Zhang *et al.,* 2022).

Omnibus Test of Model Coefficients

The main goal of the Omnibus Test presented in table 4 is to determine if the set of independent variables collectively contributes to the prediction of the outcome variable.

Table 4. Omnibus Test of Model Coefficients

		Chi-Square	Df	Sig
Step 1	Step	58.384	4	0.001
	Block	58.384	4	0.001
	Model	58.384	4	0.001

A significant result from the Omnibus Test (usually a p-value less than 0.05) suggests that the independent variables in the model contribute significantly to predicting the dependent variable, warranting further investigation into the individual coefficients (Han & Dawson, 2021). The results presented on table 4 indicates that the model has a p-value of 0.001 which is below 0.05 this suggests that the model is statistically significant and can further be used for estimations since the overall model is statistically significant; $\chi 2(3) = 58.384$, $p < 0.05$.

Logistic Regression R^2 value

The Nagelkerke R^2 value for the model is presented in table 5 demonstrating how the variance in mobile banking adoption can be explained by the variables included in the model.

Table 5. Logistic regression R^2 value

Step	-2 likehood	Cox & Snell square	Nagelkerke R square
1	41.223	0.478	0.728

The Nagelkerke R^2 value for the model is 72.8%, indicating that 72.8% of the variance in mobile banking adoption can be explained by the variables included in the model. This suggests that the selected predictors provide a strong explanation for the factors influencing mobile banking adoption. Conversely, the remaining 27.2% of the variance is attributed to other factors not captured by this model, highlighting the complexity of mobile banking adoption and the potential influence of additional variables.

Logistic Regression Results

The table 6 presents the coefficients from a logistic regression analysis, offering insights into the relationship between various independent variables and the likelihood of mobile banking adoption.

Table 6. Logistic Regression Results

Variable	β	S.E	Wald	df	Sig	Exp(B)
Presence of fraud and phishing attacks	2.263	0.523	5.67	1	0.001	0.452
Transaction error recovery failure	1.678	0.724	2.232	1	0.008	0.323
Security literacy	4.183	2.33	6.932	1	0.001	4.567

The B value, or coefficient, indicates the change in the log odds of mobile banking adoption for a one-unit increase in each independent variable; a positive B value suggests that as the variable increases, the likelihood of mobile banking adoption also rises. The standard error (S.E.) measures the variability of the coefficient estimate, with smaller values indicating more precise estimates (Andrade, 2020). The Wald statistic tests the significance of each coefficient, where a larger Wald value signifies a stronger relationship with the dependent variable (Wallisch et al., 2021). The degrees of freedom (df) value typically equal 1 for individual predictor variables. The significance (Sig.) column presents the p-value for each variable, where a p-value less than 0.05 indicates statistical significance in predicting mobile banking adoption. Finally, the Exp(B) or odds ratio represents the odds associated with each independent variable; an odds ratio greater than 1 signifies that an increase in that variable is linked to higher odds of adopting mobile banking and odds ratio less than 1 suggests a negative association between the independent variable and the dependent outcome (Jadil *et al.,* 2021)

DISCUSSION OF FINDINGS

The results of the binary logistic regression analysis provide valuable insights into the security factors influencing mobile banking adoption. The presence of fraud and phishing attacks has a coefficient of 2.263, indicating that these security concerns are associated with an increased likelihood of mobile banking adoption. However, the odds ratio of 0.452 suggests that for each unit increase in worries about fraud and phishing attacks, the odds of adopting mobile banking decrease by approximately 54.8%. This significant finding (p = 0.001) highlights the negative impact that security concerns have on user adoption. This finding aligns with the study of Burda et al., (2024) revealed that social engineering stemming from tactics such as phishing and pretexting are the major inhibitor of online financial systems. This is supported by one among of the respondents who affirmed that *"The widespread prevalence of social engineering attacks and their significant impact on financial losses makes us wary of engaging in online banking*" (Respondent 3). This aligns with the conclusion drawn by Bojjagani *et al.,* (2023) who concluded that despite the implementation of strong security protocols, social engineering remains a significant threat to online payment services. Social engineering exploits human psychology rather than technical vulnerabilities, enabling attackers to manipulate individuals into divulging sensitive information or performing actions that compromise their security. This has been revealed in the study as one among of the participant said "*Hackers may employ pretexting, by fabricating scenarios to obtain sensitive information, The emotional impact of these experiences extends beyond financial loss; it also weakens trust in mobile banking* (Respondent 5). Similarly, the analysis reveals that transaction error recovery failure has a coefficient of 1.678, indicating that difficulties in recovering from transaction errors adversely affect mobile banking adoption. The odds ratio of 0.323 implies that for each unit increase in transaction error recovery failure, the odds of adopting mobile banking decrease by about 67.7%, with this result being statistically significant (p = 0.008). This highlights the importance of effective error recovery mechanisms in promoting mobile banking use. This is supported by one among the respondents who said "*When we fail to recover transaction errors, it leaves us feeling insecure in mobile banking and raises concerns about potential financial loss. This uncertainty creates anxiety, as we worry about the safety of our funds, making us hesitant to fully embrace mobile banking"* (Respondent 7).

In contrast, security literacy shows a strong positive relationship with mobile banking adoption, represented by a coefficient of 4.183. The odds ratio of 4.567 indicates that for each unit increase in security literacy, the odds of adopting mobile banking increase by approximately 356.7%. This significant result (p = 0.001) emphasizes the crucial role that security literacy plays in encouraging users to embrace mobile banking services. This align with the study conducted by Shankar *et al.,* (2022) who concluded that education on key best practices is essential for enhancing security in mobile banking. This includes creating strong, unique passwords and enabling two-factor authentication and remain cautious with links and attachments to steer clear of phishing scams. This aligns with one of respondents who said *"If we can effectively identify phishing tactics, such as fake mobile applications and deceptive text messages, our confidence in using mobile banking will significantly increase" (*Respondent 5). In other words, if mobile banking users can recognize the signs of phishing, they can take proactive steps to protect themselves. This includes verifying the authenticity mobile bank apps and carefully examining messages for suspicious links.

CONCLUSION

The adoption of mobile banking by fashion retail in Mwanza City Councils is significantly affected by fraud and phishing, transaction errors recovery failure and security literacy. The study reveals a notable negative impact of fears surrounding fraud and phishing, as indicated by a coefficient of 2.263 and an odds ratio of 0.452. These security issues deter fashion retailers from fully embracing mobile banking. Additionally, the study highlights those difficulties in recovering from transaction errors adversely affect user confidence. With a coefficient of 1.678 and an odds ratio of 0.323, the findings suggest that challenges in resolving transaction issues foster insecurity and anxiety, complicating users' willingness to engage with mobile banking platforms. On a more positive note, the study emphasises the significant role of security literacy in promoting mobile banking adoption. With a coefficient of 4.183 and an odds ratio of 4.567, the data indicates that as users become more educated about security best practices, their confidence in mobile banking increases substantially. This correlation emphasizes the importance of fostering security awareness to enhance the adoption of mobile banking among fashion retailers.

RECOMMENDATION

The banks that provide mobile banking service are recommended to implement comprehensive training programs focused on security best practices. These programs should educate users about identifying phishing tactics, creating strong passwords, and the importance of two-factor authentication. In addition, Mobile bank service provider are recommended to develop and promote efficient transaction error recovery mechanisms. This includes creating user-friendly interfaces for reporting transaction errors and ensuring timely resolutions

REFERENCES

1) Abdul-Sater, Z., Menassa, M., El Achi, N., Abdul-Khalek, R. A., Abu-Sittah, G., & Mukherji, D. (2020). Strengthening capacity for cancer research in conflict settings: key informant insights from the Middle East. ecancermedicalscience, 14.
2) Ali, M., Raza, S. A., Khamis, B., Puah, C. H., & Amin, H. (2021). How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. foresight, 23(4), 403-420.
3) Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.
4) Andrade, C. (2020). Understanding the difference between standard deviation and standard error of the mean, and knowing when to use which. Indian Journal of Psychological Medicine, 42(4), 409-410.
5) Aziz, F., Sheikh, S. M., & Shah, I. H. (2022). Financial inclusion for women empowerment in South Asian countries. Journal of Financial Regulation and Compliance, 30(4), 489-502.
6) Banerjee, R. (2024). Corporate Frauds: Now Bigger, Broader and Bolder. Penguin Random House India Private Limited.
7) Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. Computers & Electrical Engineering, 96, 107546.
8) Bitzer, M., Stahl, B., & Strobel, J. (2021). Empathy for Hackers-an IT Security Risk Assessment Artifact for Targeted Hacker Attacks. ECIS,
9) Bojjagani, S., Sastry, V., Chen, C.-M., Kumari, S., & Khan, M. K. (2023). Systematic survey of mobile payments, protocols, and security infrastructure. Journal of Ambient Intelligence and Humanized Computing, 14(1), 609-654.
10) Burda, P., Allodi, L., & Zannone, N. (2024). Cognition in social engineering empirical research: a systematic literature review. ACM Transactions on Computer-Human Interaction, 31(2), 1-55.
11) Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9(89), 446-476.
12) Colasante, A., & D'Adamo, I. (2021). The circular economy and bioeconomy in the fashion sector: Emergence of a “sustainability bias”. Journal of Cleaner Production, 329, 129774.
13) Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. ACM Computing Surveys (CSUR), 54(8), 1-35.
14) Dhobe, S. D., Tighare, K. K., & Dake, S. S. (2020). A review on prevention of fraud in electronic payment gateway using secret code. Int. J. Res. Eng. Sci. Manag, 3(1), 602-606.
15) Dzidzah, E., Owusu Kwateng, K., & Asante, B. K. (2020). Security behaviour of mobile financial service users. Information & Computer Security, 28(5), 719-741.
16) Ebert, F., Castor, F., Novielli, N., & Serebrenik, A. (2021). An exploratory study on confusion in code reviews. Empirical Software Engineering, 26, 1-48.

17) Han, H., & Dawson, K. J. (2021). Applying elastic-net regression to identify the best models predicting changes in civic purpose during the emerging adulthood. Journal of adolescence, 93, 20-27.
18) Handoyo, S., 2024. Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, *10*(8).
19) Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. Technology in Society, 67, 101693.
20) Hultberg, E., & Pal, R. (2021). Lessons on business model scalability for circular economy in the fashion retail value chain: Towards a conceptual model. Sustainable Production and Consumption, 28, 686-698.
21) Ibrahimnur, A. A. (2023). Impact of Cybercrime on the Finance Sector: a Case of Banks in Nairobi County, Kenya (2008-2022) University of Nairobi].
22) Iyelolu, T. V., Agu, E. E., Idemudia, C., & Ijomah, T. I. (2024). Conceptualizing mobile banking and payment systems: Adoption trends and security considerations in Africa and the US. International Journal of Science and Technology Research Archive, 7(1), 001-009.
23) Jadil, Y., Rana, N. P., & Dwivedi, Y. K. (2021). A meta-analysis of the UTAUT model in the mobile banking literature: The moderating role of sample size and culture. Journal of Business Research, 132, 354-372.
24) Jain, S., Basu, S., Ray, A., & Das, R. (2023). Impact of irritation and negative emotions on the performance of voice assistants: Netting dissatisfied customers' perspectives. International Journal of Information Management, 72, 102662.
25) Jibril, A. B., Kwarteng, M. A., Pilik, M., Botha, E., & Osakwe, C. N. (2020). Towards understanding the initial adoption of online retail stores in a low internet penetration context: An exploratory work in Ghana. Sustainability, 12(3), 854.
26) Karki, D., Bhattarai, G. and Dahal, R.K., 2024. User acceptance determinants in m-banking adoption. *Nurture*, *18*(1), pp.201-213.
27) Kasowaki, L., & William, J. (2024). Digital Dollars: Maximizing the Power of Internet Banking for Seamless E-Commerce Transactions (2516-2314).
28) Kennedy, I. (2022). Sample size determination in test-retest and Cronbach alpha reliability estimates. British Journal of Contemporary Education, 2(1), 17-29.
29) Kocabas, H., Nandy, S., Tamanna, T., & Al-Ameen, M. N. (2021). Understanding user's behavior and protection strategy upon losing, or identifying unauthorized access to online account. International Conference on Human-Computer Interaction,
30) Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4), 444-464.
31) Macha, D. P., & Massawe, N. M. (2023). Financial Technology in Tanzania: Assessment of Growth Drivers.
32) Mapunda, E. F. (2022). Influence of Service Digitalization on the Performance of Commercial Banks in Tanzania: A Case of CRDB Bank Plc Headquarters The Open University of Tanzania].
33) McCray, K. L. (2023). Vulnerabilities and Threats in Mobile Banking that Financial Institutions Must Understand to Reduce Mobile Banking Fraud Marymount University].
34) Msengi, Y. D. (2022). Factors Affecting Customers Loyalty Towards Mobile Telecommunication Service Providers in Dar es salaam The Open University of Tanzania].
35) Nadeem, M., Zahra, S. W., Abbasi, M. N., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing attack, its detections and prevention techniques. International Journal of Wireless Security and Networks, 1(2), 13-25p.
36) Nattino, G., Pennell, M. L., & Lemeshow, S. (2020). Assessing the goodness of fit of logistic regression models in large samples: a modification of the Hosmer-Lemeshow test. Biometrics, 76(2), 549-560.
37) Nish, A., Naumann, S., & Muir, J. (2022). Enduring cyber threats and emerging challenges to the financial sector. Carnegie Endowment for International Peace.
38) Rajendran, R. (2024). Data Breach Fraudulence and Preventive Measures in E-Commerce Platforms. In Advancements in Cybercrime Investigation and Digital Forensics (pp. 161-184). Apple Academic Press.
39) Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., & Mare, S. (2021). " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. Proceedings of the ACM on human-computer interaction, 5(CSCW1), 1-30.

40) Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. Journal of Accounting & Organizational Change, 17(2), 164-196.
41) Sandell, S. (2021). Risk management for universities in the age of cybercrime S. Sandell].
42) Sanni, M. L., Akinyemi, B. O., Akinwuyi, D., Olajubu, E. A., & Aderounmu, G. A. (2023). A Predictive Cyber Threat Model for Mobile Money Services. Annals of Emerging Technologies in Computing (AETiC), 7(1), 40-60.
43) Schreiber, J. B. (2021). Issues and recommendations for exploratory factor analysis and principal component analysis. Research in Social and Administrative Pharmacy, 17(5), 1004-1011.
44) Shankar, A., Tiwari, A. K., & Gupta, M. (2022). Sustainable mobile banking application: a text mining approach to explore critical success factors. Journal of Enterprise Information Management, 35(2), 414-428.
45) Sharma, A., Singh, S. K., Kumar, S., Chhabra, A., & Gupta, S. (2021). Security of android banking mobile apps: Challenges and opportunities. International conference on cyber security, privacy and networking,
46) Siano, A., Raimi, L., Palazzo, M., & Panait, M. C. (2020). Mobile banking: An innovative solution for increasing financial inclusion in Sub-Saharan African Countries: Evidence from Nigeria. Sustainability, 12(23), 10130.
47) Sitar-Tăut, D.A., Mican, D. and Moisescu, O.I., 2024. To be (online) or not to be? The antecedents of online study propensity and e-learning-dependent dropout intention in higher education. *Technological Forecasting and Social Change*, *207*, p.123566.
48) Souiden, N., Ladhari, R., & Chaouali, W. (2021). Mobile banking adoption: a systematic review. International Journal of Bank Marketing, 39(2), 214-241.
49) Wallisch, C., Dunkler, D., Rauch, G., De Bin, R., & Heinze, G. (2021). Selection of variables for multivariable models: Opportunities and limitations in quantifying model stability by resampling. Statistics in Medicine, 40(2), 369-381.
50) Zhang, W., Jin, Y., Liu, N., Xiang, Z., Wang, X., Xu, P., Guo, P., Mao, M., & Feng, S. (2022). Predicting physical activity in Chinese pregnant women using multi-theory model: a cross-sectional study. International Journal of Environmental Research and Public Health, 19(20), 13383.
51) Zhang, Z. (2021). Designing an Autoresponder for Phishing Email Reports PhD thesis, University of Edinburgh].