INTERNATIONAL JOURNAL OF BANKING AND FINANCE
https://e-journal.uum.edu.my/index.php/ijbf

How to cite this article:
Mkilia, E. L., Kaleshu, J., & Sife, A. S. (2025). Customers' perceptions on banks' cybersecurity and their use of mobile banking services in Tanzania. *International Journal of Banking and Finance*, *20*(2), 43-59. https://doi.org/10.32890/ijbf2025.20.2.3

CUSTOMERS' PERCEPTIONS ON BANKS' CYBERSECURITY AND THEIR USE OF MOBILE BANKING SERVICES IN TANZANIA

[1]Emmanuel L Mkilia, [2]Jones Kaleshu & [3]Alfred S. Sife
[1&2]Department of Banking Accounting and Finance
Moshi Co-operative University (MoCU), Tanzania
[3]Department of Knowledge Management
Moshi Co-operative University (MoCU), Tanzania

[1]Corresponding author: shamkilia575@gmail.com

Received: 10/2/2024 Revised: 1/10/2024 Accepted: 6/10/2024 Published: 31/7/2025

ABSTRACT

In this contemporary era, mobile banking services enable customers to organise and accomplish cashless financial transactions using mobile devices. However, the general state of banks' cybersecurity systems significantly impacts the usage of banking services offered through mobile networks among customers. The analysis was performed to assess how customers perceive the cybersecurity systems of banks and their association with mobile banking usage. By adopting a cross-sectional research design under the guidance of the Unified Theory of Acceptance and Use of Technology (UTAUT), the Partial least squares structural equation modelling (PLS-SEM) analysis reveals that banks' cybersecurity systems' performance expectancy had a significant positive impact on the use of mobile banking services. Further, banks' cybersecurity systems' effort expectancy, significant others' comments and facilitating conditions significantly and positively influence bank customers to use mobile banking. Aligning with these findings, banks and financial institutions should prioritise and strengthen cybersecurity systems and simplify mobile banking processes for enhanced mobile banking adoption and usage among bank customers.

Keywords: Cybersecurity systems, UTAUT, mobile banking, PLS-SEM.

INTRODUCTION

Banks and other financial institutions increasingly invent and adopt new technologies that add value to their businesses and create greater customer value. Such technologies include mobile banking, which enables customers to organise and accomplish financial transactions using mobile gadgets such as phones (Dissanayake et al., 2023). The proliferation and use of mobile banking services increasingly dominate worldwide discussions on financial matters (Pattnaik et al., 2024). This is primarily due to mobile banking's potential to address challenges in financial inclusion, particularly in access to and usage of financial services. Consequently, advancements in financial technology have resulted in a greater number of users using mobile banking apps.

Since mobile banking services, in most cases, do not involve human contact, they create uncertainty and anonymity in transactions involved, hence security threats to the user (Wizid et al., 2019; Mettouris et al., 2015). The security threats in mobile banking, among others, include cyberattacks and hacking. This calls for cybersecurity systems to protect mobile banking users from cybersecurity risks. Kumar and Yukita (2021) and Thusi and Maduku (2020) opine that security is the priority for mobile banking customers since they disclose their banking details and other personal information when using mobile banking services. Any exposure to cyberattacks resulting in loopholes in banks' cybersecurity systems is more likely to affect customers' decisions to use and recommend others for mobile banking services (Apau & Lallie, 2022; Nilashi et al., 2022).

Studies (Apau & Lallie, 2022; Sinha & Singh, 2022) have established that the general state of banks' cybersecurity systems may significantly impact customers' usage of mobile banking services. Amro and Tiantian (2017) recommend that mobile banking services require dependable cybersecurity systems as they have correspondingly increased the appetite of cybercriminals to target consumers. Correspondingly, the perception of mobile banking users on banks' ability to deal with cyber criminals has emerged as a key aspect in determining the usage of mobile banking services (Kumar & Yukita, 2021; Merhi et al., 2021; Obaid, 2021). Customers need to have confidence and incline positive perception of the banks' ability to deal with cyber-risks (Albort-Morant et al., 2022; Jiang et al., 2022; Hong et al., 2020) for them to adopt and then use mobile banking services. Nevertheless, Ramli et al. (2021) argue that customers should be guaranteed and satisfied with all dimensions of banks' cybersecurity systems to use mobile banking facilities confidently.

Given the recent nature of mobile banking, previous research in most developing countries, including Tanzania, has primarily focused on customer intention to adopt and use (Mujahed et al., 2022; Rabaa'i & AlMaati, 2021), ability to use (Al-Dmour et al., 2020), as well as bank readiness and ability to offer the services (Kitsios et al., 2021). In Tanzania, available literature (e.g., Akinbowale et al., 2020; Mori & Mlambiti, 2020; Mbogoro & Masele, 2020) is mainly on the development and acceptance of mobile banking across various populations in the country. The primary focus is on how mobile banking catalyses financial inclusion. Much is unknown about customers' exposure to cybercrime and how it affects mobile banking usage. There is scarce evidence of customers' perceptions and responses to banks' cybersecurity systems and how they affect their decision to use mobile banking in Tanzania.

The theoretical lens for this study is rooted in the Unified Theory of Acceptance and Use of Technology (UTAUT), which explains technology adoption and usage as determined by the outcomes of performance expectancy, effort expectancy, social attributes and facilitating conditions of such technology. Further, proponents of the UTAUT claim that customers' perceptions of the performance expectancy, effort expectancy, social attributes and facilitating conditions of the cybersecurity systems

of banks form the basis for the decision to practice mobile banking services (Marikyan et al., 2023; Venkatesh et al., 2016). However, it is unclear whether the abovementioned factors suggest the state of mobile banking usage among mobile banking customers in Tanzania. Thus, this is an opaque to fill. By bridging this gap, this study is significant as it contributes to advancing knowledge, adding to existing information, and expanding the collective understanding of cybersecurity issues and their impact on mobile banking usage in Tanzania. This is important for developing countries, particularly Tanzania, as it provides insight into the banking sector's existing initiatives, innovations and improvements to align with global trends. This study, therefore, analysed the customers' perceptions of banks' cybersecurity systems and their association with mobile banking usage.

Theoretical Underpinning, Hypotheses and Conceptual Framework of the Study

Previous studies on the emergence and advancement of mobile banking have concentrated mainly on customer intentions to adopt and use the technology, the ability to use, and the readiness and capability of banks to offer the service (Mujahed et al., 2022; Kitsios et al., 2021; Rabaa'i & AlMaati, 2021; Al-Dmour et al., 2020). In Tanzania, existing literature centers on the development and adoption of mobile banking in promoting financial inclusion. Customers' exposure to cybercrime and its impact on mobile banking is yet to be studied. Relying on the dimensions of the UTAUT, this study focuses on analysing bank customers' use of mobile banking based on their perceptions of the existing banks' cybersecurity measures.

Theoretical Underpinning

Various theories and models that explain technology acceptance and use have been introduced, originating from different roots and disciplines, which limit their applications and predictive power to contexts. The UTAUT is best suited for explaining technology adoption and usage among individuals in different contexts. UTAUT incorporates social psychology, information systems management and behavioural psychology perspectives in predicting behavioural intention and the use of technology (Venkatesh et al., 2003; Marikyan et al., 2023). The theoretical argument of the UTAUT is that the actual use of technology is determined by behavioural intention. Such intention to use technology is triggered by four dimensions: performance expectancy, effort expectancy, social influence, and facilitating conditions (Venkatesh et al., 2003).

The first dimension, performance expectancy, predicts use intention (Zhou *et al*., 2010). It involves the degree to which individuals consider using technology to help attain and gain efficiency during a particular task (Venkatesh et al., 2016; Venkatesh et al., 2003). Another dimension of the theory is effort expectancy, which is about individuals' perceptions of the ease of using a specific technology (Chauhan & Jaiswal, 2016; Venkatesh et al., 2003). Social influence is related to the degree to which an individual recognises the significant others' beliefs on using innovative technology (Venkatesh et al., 2003). The last dimension, facilitating conditions, confines itself to the level that an individual considers organisations and technical setups available to aid usage of the new technology (Venkatesh et al., 2003). These dimensions suggest a more substantial predictive power than other theories and models explaining technology acceptance (Lee & Heo, 2020; Venkatesh et al., 2016). UTAUT has been validated by various studies (e.g., Mütterlein et al., 2019; Raza et al., 2019; Baptista & Oliveira, 2015; Zhou et al., 2010) to be significant in explaining the acceptance and use of various technologies in the banking industry. Thus, UTAUT was adopted to guide an analysis of the impact of customer perceptions of cybersecurity systems in banks on their use of banking services offered through mobile in Tanzania.

Hypotheses Development

Cybersecurity Systems' Performance Expectancy and Usage of Mobile Banking Services

According to UTAUT, performance expectancy suggests that adopting and using a particular technology is conditioned by favourable beliefs about a range of such technology's potential outcomes (Venkatesh et al., 2016). For this study, mobile banking usage among customers is likely to increase if they believe the cybersecurity systems associated with it are relatively stable and can protect them. The implication is that mobile banking customers' perceptions of being protected and secure should be inclined using mobile banking app technologies (Mütterlein et al., 2019; Park et al., 2007). Such perceptions may persuade customers to use mobile banking services and benefit from the promptness of transactions, suitability, ubiquity, immediacy and, foremost, security backed in all these aspects (Baptista & Oliveira, 2015). To account for this situation in the context of emerging economies, the following hypothesis was postulated:

H1: The perception of mobile banking customers on banks' cybersecurity systems performance expectancy positively influences the usage of mobile banking services.

Effort Expectancy of Cybersecurity Systems and Its Influence on Mobile Banking Service Usage

The probability of accepting and using any technology and its related services increases when little effort is required for its effective use (Alalwan et al., 2017; Akturan & Tezcan, 2012; Venkatesh et al., 2003). For this study, the anticipation is that acceptance and usage of mobile banking technologies among customers will likely occur when it requires less effort to deal with security issues (Singh & Srivastava, 2020; Lim et al., 2019). The argument for this is that banks' cybersecurity systems in place for mobile banking should not induce prolonged security measures for customers to complete mobile banking transactions. Literature (e.g., Raza et al., 2019; Aboelmaged & Gebba, 2013; Venkatesh et al., 2012) claim a positive relationship between effort expectancy in terms of perceived ease of use of mobile banking applications and consumers' decision to accept and use of it. This study assumes that customers' perception of the efforts they put into complying with the banks' cybersecurity systems that are in place for mobile banking apps facilitates decisions on using mobile banking facilities. Therefore, the following hypothesis was made:

H2: Mobile banking customers' perception of the effort expectancy of cybersecurity systems in banks positively impacts usage of banking services.

Social Influence on Cybersecurity Systems and its Impact on Mobile Banking Service Usage

Recommendations and beliefs of other people play a pivotal role in influencing and shaping individuals' decisions, particularly on the use of technology. Also, based on the UTAUT, social influence, as reflected in other people's belief in the new technology, shapes individuals' acceptance and usage of that technology (Venkatesh et al., 2003). Individuals accept and adopt mobile banking applications due to social influences from friends, family, coworkers, and social media (Apaua & Lallie, 2022). For this study, it was postulated and expected that mobile banking customers will be influenced to use mobile banking services given that their significant others (friends, family, and social media) have recommended the effectiveness of the security and safety of the mobile banking services (Lim et al., 2019). Hence, in this study, it was hypothesised that:

H3: Mobile banking customers' perception of peers' beliefs regarding banks' cybersecurity systems in banks impacts positively usage of banking services.

Cybersecurity Systems' Facilitating Conditions and Usage of Mobile B Banking Services

The presence of supportive organisations and technical infrastructure to help use technology has the potential for its acceptance and continued usage (Venkatesh et al., 2003). Mobile banking clients are more likely to use mobile banking services if they consider the present mobile banking services to be backed with organisational and technical infrastructure to support any challenge related to cybersecurity systems (Singh and Srivastava, 2020; Stewart and Jürjens, 2018). Customers with access to enabling environments from the organisation and technical infrastructure on mobile banking services are likelier to opt to use the services (Apaua and Lallie, 2022; Baptista and Oliveira, 2015). Facilitating conditions of mobile banking services cybersecurity in such aspects as manuals, demos, and video tutorials can play part towards the adoption and usage of mobile banking services, hence the hypothesis:

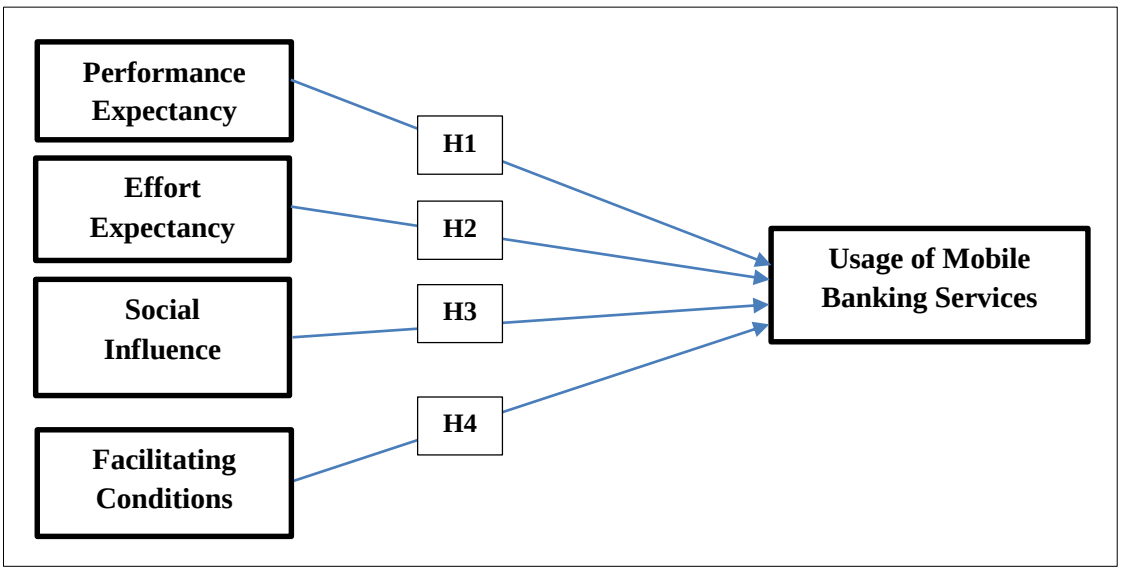
H4: The perception of mobile banking customers on facilitating conditions of the banks' cybersecurity systems positively influences the usage of mobile banking services.

Conceptual framework of the study

Based on the UTAUT and the hypotheses of this study, it is conceptualised that customers' perception of the banks' cybersecurity systems on such aspects as performance expectancy, effort expectancy, social influence and facilitating conditions influences usage of mobile banking services as presented in Figure 1.

Figure 1

Theoretical Framework



METHODS

Data Collection

A cross-sectional research design was used in this study. Data were collected through a survey strategy typically associated with the deductive approach, which permits data collection from a wider population using fewer resources (Proudfoot, 2023). Survey questionnaire was used to obtain data for this study. A Likert scale varying from "1 strongly disagree" to "5 strongly agree" was employed to assess the perception of mobile banking customers of the banks' cybersecurity systems on mobile banking services.

Dar es Salaam City was the area for this study as it has the relative maximum number of commercial banks in Tanzania (BOT, 2020). Compared to other areas, Dar es Salaam City was also chosen because it has a high financial inclusion score of 73%, out of which 40% of its population is accessing banking services (Fin Scope, 2017).

Ten commercial banks were purposively preferred for the study - Tanzania Commercial Bank (TCB), CRDB Bank PLC, KCB Bank Tanzania LTD, Stanbic Bank, National Bank of Commerce (NBC), Diamond Trust Bank (DTB), Azania Bank, First National Bank of Tanzania (FNB), NMB Bank PLC, and Equity Bank. These banks were selected based on their nationwide branch network, level of technological advancement, customer base size, and extensive experience in banking operations (BOT, 2020).

The study sample was obtained using Cochran's (1977) formula. The formula is applicable when the total population for the study is unknown. A 95% confidence level and a 5% sampling error were chosen using the formula. The formula is expressed as

$$\mathrm{N} = \frac{Z^2 PQ}{e^2}$$

Here, N represents the calculated sample size, Z is the desired confidence level, p denotes the estimated proportion of characteristics in the population, Q =1− P and e is the chosen margin of error. Given the value of P = 0.5, Q =1-0.5 = 0.5, e = 0.05, and Z =1.96

From the formula:

$$\mathrm{N} = \frac{(1.96)^2 x 0.5 x 0.5}{0.05^2} = 384$$

Nevertheless, 478 commercial banks' mobile customers were involved as respondents for this study. The sample size used in this study exceeded the computed value of 384 because, firstly, Hair et al. (2017) recommends a sample size range of 200 to 500 as suitable when applying the Structural Equation Model (SEM) for data analysis. Secondly, incorporating additional data is essential and ensures greater accuracy in minimising parameter approximation errors (Kelly & Lai, 2011). Third, the respondents were obtained through a convenience sampling technique, which allows data collection from respondents who are easy to contact (Jager et al., 2017).

Data Analysis

Partial least squares structural equation modelling (PLS-SEM) was used to analyse mobile banking customers' perceptions of banks' cybersecurity systems and their impact on their decision to use mobile banking services. PLS-SEM allows testing and predicting associations in a conceptual model for dependent and independent variables (Hair et al., 2019). Considering that the goal of this study was to test the predictive relations and clarify the changes in the dependent variables as justified by controlled variables, PLS-SEM was regarded as suitable for data analysis.

Validity and Reliability

The validity of the measurement model was assessed by inspecting convergent validity, reliability, and discriminant validity. Convergent validity was tested by analysing the extent to which hypothetically associated scale items correlate by looking at Composite Reliability (CR) (which should be above 0.6), Cronbach Alpha (CBA) (which should be above 0.7), and Average Variance Extracted (AVE) that also must be above 0.5 (Hair et al., 2019). As shown in Table 1, all the items in this study met the thresholds for convergent validity.

Table 1

Validity and Reliability Tests

Aspects	Indicator	Loadings	VIF	CBA	CR	AVE
Performance Expectancy	PE1	0.862	1.541	0.868	0.819	0.826
	PE2	0.897	1.715			
	PE3	0.846	1.109			
Effort Expectancy	EE1	0.872	1.474	0.893	0.729	0.797
	EE2	0.759	1.315			
	EE3	0.876	1.716			
	EE4	0.736	1.128			
Social Influence	SI1	0.918	1.419	0.913	0.931	0.886
	SI2	0.874	1.621			
	SI3	0.915	1.539			
Facilitating Conditions	FC1	0.737	1.146	0.792	0.859	0.821
	FC2	0.801	1.523			
	FC3	0.759	1.531			
Mobile banking Usage	MBU1	0.914	1.164	0.812	0.761	0.782
	MBU2	0.859	1.965			
	MBU3	0.788	1.429			

Discriminant validity, indicating how much a construct varies empirically from other constructs in the structural model, was confirmed using the Fornell-Lacker criterion. The standard measure of Discriminants Validity was put forth by Fornell and Larcker (1981), who suggested relating the AVE of each construct to the squared inter-construct correlation of that construct and all other reflectively assessed constructs in the structural model as a gauge of shared variance. The shared variance of every model construct should not be higher than its AVEs. This is done to determine if any connection exists among constructs that should not be associated.

Table 2

Discriminants Validity

	Mean	SD	PE	EE	SI	FC	MBU
PE	3.95	1.05	**0.746**				
EE	3.86	1.14	0.667	**0.715**			
SI	3.83	1.17	0.523	0.707	**0.842**		
FC	3.81	1.19	0.540	0.606	0.557	**0.813**	
MBU	3.77	1.23	0.543	0.584	0.588	0.629	**0.716**

The result (Table 2) demonstrates discriminant validity as the squared correlation of each component exceeds the squared correlation of other constructs (Hair et al., 2019).

FINDINGS AND DISCUSSION

Demographic Characteristics

The findings show that most (59.6%) respondents were male, and the majority (77%) were aged between 15 and 44 years. Less than half (45.6%) of the respondents had a bachelor's degree or above. All respondents had at least secondary education. About half (49.8%) of the respondents used mobile banking multiple times a week, and two-thirds (65.7%) had used mobile banking for over two years. Many (60.8%) respondents were employed in the government and private sectors (Table 3).

Table 3

Demographic Characteristics of the Respondents

Characteristics	Value	Frequency	Percentage
Sex	Male	285	59.6
	Female	193	40.4
Age	15-25	106	22.2
	26-44	265	55.4
	45-64	97	20.3
	65+	10	2.1
Education level	Secondary	107	22.4
	Certificate	60	12.5
	Diploma	93	19.5
	Degree	197	41.2
	Masters and above	21	4.4
Occupation	Government employee	102	21.3
	Private sector employee	189	39.5
	Self-employed	84	17.6
	Student	79	16.5
	Unemployed	24	5.1
Mobile banking usage	Once a week	196	41.0
	Multiple times a week	238	49.8

(continued)

Characteristics	Value	Frequency	Percentage
Experience in using Mobile Banking	Once a month	37	7.7
	Once a year	7	1.5
	Less than a year	59	12.3
	1-2 years	105	22
	More than 2 years	314	65.7

Banks' Cybersecurity and Usage of Mobile Banking

The structural model was evaluated to analyse the path coefficients and total effects of performance expectancy, effort expectancy, social influence, and facilitating conditions as independent variables on the dependent variable of mobile banking usage. The findings are indicated in Table 4.

Table 4

Structural Model Relationship on Banks Cybersecurity and Usage of Mobile Banking

Relationship	Hypothesis	β	T-Statistic	ρ-value	Significance at ρ<0.05?
PE → MBU	H1	0.296	3.897	0.000	Yes
EE → MBU	H2	0.319	2.983	0.001	Yes
SI → MBU	H3	0.381	5.513	0.000	Yes
FC → MBU	H4	0.171	2.899	0.004	Yes

Findings show that the performance expectancy of banks' cybersecurity systems has a significant and positive impact on the use of mobile banking ($\beta = 0.296$, $t = 3.897$, $p = 0.000$), supporting H1. This means the degree to which individuals believe that using a technology, in this case, mobile banking, will help them perform tasks more effectively or improve their overall performance positively influences decisions for adopting and using mobile banking services. These findings align with those of Merhi et al. (2019), Mütterlein et al. (2019), Baptista and Oliveira (2015) and Park et al. *(*2007). As stipulated by the UTAUT, performance expectancy on the cybersecurity systems of banks suggests the acceptance and usage of mobile banking services among commercial bank customers.

The implication is that mobile banking customers need banks' cybersecurity systems to provide and guarantee protection when using mobile banking services. This vents the notion that banks should improve mobile banking products and services backed by strong cybersecurity to meet mobile banking service users' performance expectations. Moreover, banks need to run marketing and awareness campaigns to enhance users' knowledge about the effectiveness of the banks' cybersecurity systems on mobile banking services. Publicising the efficiency of the banks' cybersecurity systems creates confidence among customers about the mobile banking services offered. This will stimulate customers' positive perceptions towards banks' cybersecurity systems, enhancing the likelihood of adopting and using mobile banking services among commercial bank customers. Positive perceptions about the expected cybersecurity performance of banks on mobile banking services reduce users' anxiety about security breaches and give them confidence that the services are reliable, secure, real-time, speedy, convenient, and ubiquitous. Such perceptions persuade and increase customers' attitudes to use mobile banking services and benefit from them.

The influence of effort expectancy of the banks' cybersecurity systems on mobile banking usage among mobile banking customers was also positive and significant ($\beta = 0.319$, $t = 2.983$, $\rho = 0.001$), supporting H2. Complying with the prepositions of the UTAUT (Venkatesh et al., 2003 & Venkatesh et al., 2012), this study also found that effort expectancy of the banks' cybersecurity systems plays a crucial role in shaping mobile banking user behaviour. These findings imply that if bank customers perceive that the prevailing banks' cybersecurity systems allow mobile banking apps to be user-friendly, intuitive and require minimal effort to navigate, they are more likely to have a positive attitude toward using them. These findings align with the previous studies such as (Singh & Srivastava, 2020; Lim et al., 2019; Raza et al., 2019; Alalwan et al., 2017; Aboelmaged, & Gebba, 2013; Venkatesh et al., 2012) that found effort expectancy on the mobile banking technology or systems to influence its adoption and usage among individuals.

Based on the findings, if bank customers evaluate the effort required for specific tasks within mobile banking, such as checking balances, moving funds, or settling bills, straightforward and require minimal cognitive or physical effort, given the current banks' cybersecurity, users are more likely to engage with the mobile banking app regularly. Generally, bank customers' perception and belief that using mobile banking apps can streamline their financial tasks and make their lives easier, they are more likely to overcome any perceived effort associated with its adoption and usage. Mobile banking customers' perceptions of effort expectancy of the bank's cybersecurity systems and their decision to use mobile banking services also relate to the available alternatives. If mobile banking is perceived as more convenient and requires less effort than the available alternatives, customers will likely to choose it to complete various banking activities. Conversely, these findings imply that if the banks' cybersecurity system makes mobile banking tasks and services seen as complex or time-consuming, bank customers may be less inclined to use the technology.

Similarly, H3 was supported as the impact of social influence (significant others' comments) on the banks' cybersecurity systems had a positive significant impact ($\beta = 0.381$, $t = 5.513$, $\rho = 0.000$) on mobile banking usage. This study's findings synchronise the argument by Apaua and Lallie (2022), Jiang et al. (2022) and Lim et al. (2019), who articulated that social and peer influence relate to and significantly influence one's decision to use and continue using mobile banking services.

The implication is that when bank customers perceive that their friends, family, or colleagues are using mobile banking and view it as positively related to its cybersecurity status, they are more likely to feel the social pressure and are encouraged to adopt, use or try it. The findings further reveal that social influence on the trust of peers, friends, and family in financial institutions and mobile banking systems' security also significantly influences mobile bank usage among bank customers. Whenever bank customers trust the opinion of a friend or family member who speaks positively about the convenience, security, and benefits, they are more likely to be influenced to use it. Moreover, this study's findings suggest that bank customers will likely use mobile banking when they observe others using it successfully and effortlessly in making payments or checking balances through mobile banking apps, perceiving the act as an acceptable and practical way to manage their finances.

The facilitating conditions of banks' cybersecurity systems also revealed a significant positive influence ($\beta = 0.171$, $t = 2.899$, $\rho = 0.004$) on mobile banking usage among mobile banking customers; hence, H4 was also supported. This means the extent to which bank customers believe that necessary cybersecurity resources and support are available to support mobile banking services, the more they will use them. This study's findings reflect what was reported by Apaua and Lallie (2022), Singh and

Srivastava (2020) and Stewart and Jürjens (2018) that customers' access to a set of enabling environments from the organisation and technical infrastructure on mobile banking services serve as a catalyst for the use of the services.

These findings imply that customers are more likely to adopt mobile banking and continue to use it if they believe they can get assistance when facing technical and security issues. When mobile banking customers' needs to secure access to smartphones or mobile devices with internet connectivity are easily met with assured availability of technical support and assistance, they are more likely to use mobile banking services. The findings further imply that perceptions of security and trustworthiness in the banks' cybersecurity relating to mobile banking are critical. Given the prevailing banks ' cybersecurity systems, suppose bank customers perceive mobile banking as secure and trustworthy. In that case, it enhances facilitating conditions, as they feel confident using the technology without concerns about unauthorised access or fraud. The findings also reveal that usage of mobile banking services among bank customers is more likely to rise if the current banks' cybersecurity systems allow mobile banking to be easily integrated with other existing banking infrastructure. If bank customers perceive mobile banking as secure and trustworthy, given the prevailing banks' cybersecurity systems, it enhances facilitating conditions, as they feel confident in using the technology without concerns about unauthorised access or fraud.

THEORETICAL IMPLICATIONS, CONCLUSION AND RECOMMENDATIONS

This study assessed customers' perceptions of banks' cybersecurity systems and their association with mobile banking usage. Based on these findings, customers' perceptions reveal that the performance expectancy, effort expectancy, social influence, and facilitating conditions of a bank's cybersecurity systems positively affect mobile banking usage. Among these variables, social influence has the most significant impact on mobile banking usage, followed by effort expectancy, performance expectancy and facilitating conditions. Supporting the UTAUT, social influence encompassing the influence of peers, family, and social norms shapes bank customers' attitudes and intentions toward using mobile banking facilities, given the prevailing banks' cybersecurity structures. Moreover, when customers believe that banks' cybersecurity systems' performance expectancy on mobile banking will improve their financial transactions and tasks' efficiency, convenience, and accuracy, they are more likely to adopt and use it regularly. Also, customers' perceptions of the banks' cybersecurity effort expectancy in such aspects as usability, task complexity, perceived usefulness, support resources, and even comparative evaluation positively facilitate customers' mobile banking usage. Facilitating conditions in the context of customers' perceived availability of resources, support, and favourable conditions is an important element influencing the usage of mobile banking.

From this study's findings, first, it is recommended that understanding and harnessing social influences should be essential for financial institutions and mobile banking providers to encourage widespread adoption and usage of their services. Second, banks and financial institutions should emphasise performance-related benefits and ensure that their mobile apps deliver as per customers' expectations to promote mobile banking usage. Third, providers should focus on improving the ease of use of their apps, providing user-friendly interfaces, offering adequate training and support, and highlighting the convenience and benefits of mobile banking to users for effective adoption and usage of mobile banking services. Lastly, banks and financial institutions should prioritise security and simplify the setup processes of mobile banking services for enhanced adoption and use.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for profit sectors.

REFERENCES

Aboelmaged, M., & Gebba, T. R. (2013). Mobile banking adoption: An examination of technology acceptance model and theory of planned behavior. *International Journal of Business Research and Development*, *2*(1).

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*, *27*(3), 945-958.

Akturan, U., & Tezcan, N. (2012). Mobile banking adoption of the youth market: Perceptions and intentions, Market. *Marketing Intelligence & Planning*, *30*(4), 444–459.

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, *37*(3), 99–110.

Albort-Morant, G., Sanchís-Pedregosa, C., & Paredes Paredes, J. R. (2022). Online banking adoption in Spanish cities and towns. Finding differences through TAM application. *Economic Research-Ekonomska istraživanja*, *35*(1), 854-872.

Al-Dmour, R., Dawood, E. A. H., Al-Dmour, H., & Masa'deh, R. E. (2020). The effect of customer lifestyle patterns on the use of mobile banking applications in Jordan. *International Journal of Electronic Marketing and Retailing*, *11*(3), 239-258.

Alonso-Dos-Santos, M., Soto-Fuentes, Y., & Valderrama-Palma, V. A. (2020). Determinants of mobile banking users' loyalty. *Journal of Promotion Management*, *26*(5), 615-633.

Amro, A. & Tiantian, D. (2017) Examining young users' security perceptions of mobile banking: A qualitative study on users' insights about mobile banking. Umea University. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1156302&dswid=4465

Apaua, R., & Lallie, H. S. (2022). Measuring user perceived security of mobile banking applications. *arXiv preprint arXiv:2201.03052*.

Ataya, M. A. M., & Ali, M. A. (2019). Acceptance of website security on e-banking. A-review. In *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)* (pp. 201-206). IEEE.

Avdić, A. (2019). Use of biometrics in mobile banking security: Case study of Croatian banks. *IJCSNS Int J Comput Sci Network Security*, *19*, 83-89.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063.

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of cceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, *50*, 418-430.

Chauhan, S., & Jaiswal, M. (2016). Determinants of acceptance of ERP software training in business schools: Empirical investigation using UTAUT model. *The International Journal of Management Education*, *14*(3), 248-262.

Dissanayake, H., Popescu, C., & Iddagoda, A. (2023). A Bibliometric analysis of financial technology: Unveiling the research landscape. *FinTech*, *2*(3), 527-542.

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.

Hong, L. M., Nawi, N. B. C., Hamsani, N. H., Zulkiffli, W. F. W. (2020). Online store image effect on perceived risks towards online purchasing behaviour. *Int. J. Bus. Inf. Syst. 35*, 27–44.

Jager, J., Putnick, D. L., & Bornstein, M. H. (2017). II. More than just convenient: The scientific merits of homogeneous convenience samples. *Monographs of the Society for Research in Child Development*, *82*(2), 13-30.

Jiang, M., Rifon, N. J., Cotten, S. R., Alhabash, S., Tsai, H. Y. S., Shillair, R., & LaRose, R. (2022). Bringing older consumers onboard to online banking: A generational cohort comparison. *Educational Gerontology*, *48*(3), 114-131.

Kelley, K., & Lai, K. (2011). Accuracy in parameter estimation for the root mean square error of approximation: Sample size planning for narrow confidence intervals. *Multivariate Behavioral Research, 46*(1), 1-32.

Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(3), 1-15.

Kumar, S., & Yukita, A. L. K. (2021, May). Millennials Behavioral Intention in Using Mobile Banking: Integrating Perceived Risk and Trust into TAM (A Survey in Jawa Barat). In *International Conference on Business and Engineering Management (ICONBEM 2021)* (pp. 210-217). Atlantis Press.

Lee, J. D., & Heo, C. M. (2020). The effect of technology acceptance factors on behavioral intention for agricultural drone service by mediating effect of perceived benefits. *Journal of Digital Convergence*, *18*(8), 151-167.

Lim, F. W., Ahmad, F., & Talib, A. N. B. A. (2019). Behavioural intention towards using electronic wallet: a conceptual framework in the light of the unified theory of acceptance and use of technology (UTAUT). *Imperial Journal of Interdisciplinary Research*, *5*(1), 79-86.

Marikyan, D., Papagiannidis, S., & Stewart, G. (2023). Technology acceptance research: Meta-analysis. *Journal of Information Science*, 01655515231191177.

Mbogoro, F., & Masele, J. J. (2020). Adoption of cash deposits through Automated Teller Machines (ATMs) by banks in Tanzania: A case of selected commercial banks in Dar es Salaam. *Business Management Revi*ew, *24*(1), 71-86.

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, *59*, 101151.

Mettouris, C., Maratou, V., Vuckovic, D., Papadopoulos, G. A., & Xenos, M. (2015) 'Information Security Awareness through a Virtual World: An end-user requirements analysis'. In *Proc. 5th International Conference on Information Society and Technology* – ICIST, pp. 273–278.

Mori, N., & Mlambiti, R. (2020). Determinants of customers' adoption of mobile banking in Tanzania: Further evidence from a diffusion of innovation theory. *Journal of Entrepreneurship, Management and Innovation*, *16*(2), 203–230.

Mujahed, H. M. H., Musa Ahmed, E., & Samikon, S. A. (2022). Factors influencing Palestinian small and medium enterprises intention to adopt mobile banking. *Journal of Science and Technology Policy Management*, *13*(3), 561-584.

Mütterlein, J., Kunz, R. E., & Baier, D. (2019). Effects of lead-usership on the acceptance of media innovations: A mobile augmented reality case. *Technological Forecasting and Social Change*, *145*, 113-124.

Nilashi, M., Abumalloh, R. A., Alrizq, M., Alghamdi, A., Samad, S., Almulihi, A., ... & Mohd, S. (2022). What is the impact of eWOM in social network sites on travel decision-making during the COVID-19 outbreak? A two-stage methodology. *Telematics and Informatics*, *69*, 101795.

Obaid, T. (2021). Predicting mobile banking adoption: An integration of TAM and TPB with trust and perceived risk. *Available at SSRN 3761669*.

Park, J., Yang, S., & Lehto, X. (2007). Adoption of mobile technologies for Chinese consumers. *Journal of Electronic Commerce Research*, *8*(3).

Pattnaik, D., Ray, S., & Raman, R. (2024). Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. *Heliyon*, *10*, e23492.

Proudfoot, K. (2023). Inductive/Deductive Hybrid Thematic Analysis in mixed methods research. *Journal of Mixed Methods Research*, *17*(3), 308-326.

Rabaa'i, A. A., & AlMaati, S. (2021). Exploring the determinants of users' continuance intention to use mobile banking services in Kuwait: Extending the expectation-confirmation model. *Asia Pacific Journal of Information Systems*, *31*(2), 141-184.

Ramli, Y., Harwani, Y., Soelton, M., Hariani, S., Usman, F., & Rohman, F. (2021). The implication of trust that influences customers' intention to use mobile banking. *The Journal of Asian Finance, Economics and Business*, *8*(1), 353-361.

Raza, S. A., Shah, N., & Ali, M. (2019). Acceptance of mobile banking in Islamic banks: Evidence from modified UTAUT model. *Journal of Islamic Marketing*, *10*(1), 357-376.

Rouse, M., & Verhoef, G. (2016). Mobile banking in Africa: The current state of play. *The Book of Payments: Historical and Contemporary Views on the Cashless Society*, 233-257.

Sadiku, M. N., Tembely, M., Musa, S. M., & Momoh, O. D. (2017). Mobile banking. *International Journals of Advanced Research in Computer Science and Software Engineering*, *7(*6), 75-76.

Shankar, A., & Rishi, B. (2020). Convenience matter in mobile banking adoption intention? *Australasian Marketing Journal (AMJ)*, *28*(4), 273-285.

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management*, *44*, 65-75.

Singh, S., & Srivastava, R. K. (2020). Understanding the intention to use mobile banking by existing online banking customers: An empirical study. *Journal of Financial Services Marketing*, *25*(3-4), 86-96.

Sinha, N., & Singh, N. (2023). Moderating and mediating effect of perceived experience on merchant's behavioral intention to use mobile payments services. *Journal of Financial Services Marketing*, *28*(3), 448-465.

Stewart, H. & Jürjens, J. (2018). 'Data security and consumer trust in FinTech innovation in Germany', *Information and Computer Security*, *26*(1), 109–128.

Thusi, P., & Maduku, D. K. (2020). South African millennials' acceptance and use of retail mobile banking apps: An integrated perspective. *Computers in Human Behavior*, *111*, 106405.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, *36*(1), 157–178.

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, *17*(5), 328-376.

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: Evolution and threats: Malware threats and security solutions. *IEEE Consumer Electronics Magazine, 8*(2), 56-60.

Zhang, T., Lu, C., & Kizildag, M. (2018). Banking "on-the-go": Examining consumers' adoption of mobile banking services. *International Journal of Quality and Service Sciences*.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, *26*(4), 760-767.

Appendix 1

Survey Tool for Analysing Customers' Perceptions fo Banks' Cybersecurity and Usage of Mobile Banking Services

	PERFORMANCE EXPECTANCY	**AGREEMENT LEVEL**				
PE	I believe the cybersecurity measures in place are effective at preventing fraud in mobile banking.	1	2	3	4	5
PE	My confidence in the cybersecurity of mobile banking influences how often I use it.	1	2	3	4	5
PE	The performance of cybersecurity systems assures me that my financial transactions are secure.	1	2	3	4	5
PE	I would use mobile banking more if the cybersecurity systems were more robust.	1	2	3	4	5
PE	I trust that cybersecurity updates in mobile banking keep my account safe from hackers.	1	2	3	4	5
PE	Effective cybersecurity in mobile banking reduces my anxiety about digital financial transactions.	1	2	3	4	5
PE	I consider the strength of cybersecurity before performing significant transactions through mobile banking.	1	2	3	4	5
PE	I am likely to suggest mobile banking to others based on the effectiveness of its cybersecurity systems.	1	2	3	4	5
PE	The reliability of cybersecurity measures influences my decision to deposit or withdraw funds using mobile banking.	1	2	3	4	5
PE	I am satisfied with how the cybersecurity systems handle potential security breaches in mobile banking.	1	2	3	4	5
	EFFORT EXPECTANCY	**AGREEMENT LEVEL**				
EE	I find it easy to understand and use the cybersecurity features available in my mobile banking app.	1	2	3	4	5
EE	The user-friendliness of cybersecurity measures in mobile banking encourages me to use it more often.	1	2	3	4	5
EE	I feel that the cybersecurity systems in mobile banking require too much effort to manage effectively.	1	2	3	4	5
EE	The simplicity of setting up security features in mobile banking makes me feel confident in its use.	1	2	3	4	5
EE	I am more likely to use mobile banking if the cybersecurity processes do not interfere with my experience.	1	2	3	4	5
EE	Complex cybersecurity procedures discourage me from using mobile banking regularly.	1	2	3	4	5
EE	I appreciate mobile banking services that provide clear instructions for their cybersecurity features.	1	2	3	4	5
EE	I am deterred from using mobile banking if the security features are too cumbersome to set up.	1	2	3	4	5
EE	The ease of updating security settings in my mobile banking app influences my usage frequency.	1	2	3	4	5
EE	I prefer mobile banking platforms that make it straightforward to monitor and manage security settings.	1	2	3	4	5
	SOCIAL INFLUENCE	**AGREEMENT LEVEL**				
SI	My family and friends' positive experiences with mobile banking security influence my own usage.	1	2	3	4	5
SI	I am more likely to use mobile banking if people I trust recommend its cybersecurity measures.	1	2	3	4	5

SI	The opinions of others about the security of mobile banking significantly affect my trust in it.	1	2	3	4	5
SI	I feel reassured using mobile banking when I see many others doing so without security issues.	1	2	3	4	5
SI	Endorsements from reputable figures about mobile banking security encourage me to use these services.	1	2	3	4	5
SI	I rely on community feedback about mobile banking security before deciding to use or continue using these services.	1	2	3	4	5
SI	My decision to use mobile banking is influenced by the security experiences shared in my social networks.	1	2	3	4	5
SI	I am more cautious about using mobile banking if I hear about security breaches from my social circle.	1	2	3	4	5
SI	Social media discussions about mobile banking security impact my usage of these services.	1	2	3	4	5
SI	I am influenced by professional advice on the effectiveness of cybersecurity measures in mobile banking.	1	2	3	4	5
	FACILITATING CONDITIONS	**AGREEMENT LEVEL**				
FC	The availability of customer support for cybersecurity issues encourages me to use mobile banking more frequently.	1	2	3	4	5
FC	I feel confident using mobile banking when I know there are effective tools for reporting security concerns.	1	2	3	4	5
FC	The presence of clear and accessible information on cybersecurity practices affects my usage of mobile banking.	1	2	3	4	5
FC	My bank provides sufficient resources for me to understand and use its cybersecurity systems effectively.	1	2	3	4	5
FC	I am more likely to engage with mobile banking when I know there are regular updates to the cybersecurity systems.	1	2	3	4	5
FC	Technical support availability for cybersecurity issues in mobile banking makes me feel more secure.	1	2	3	4	5
FC	The ease of accessing cybersecurity features in mobile banking influences my decision to use it.	1	2	3	4	5
FC	I am more willing to use mobile banking if the bank provides proactive communications about cybersecurity.	1	2	3	4	5
FC	The adequacy of cybersecurity training provided by my bank impacts my comfort level with mobile banking.	1	2	3	4	5
	I trust the mobile banking services more when there are visible and effective cybersecurity alerts and updates.	1	2	3	4	5
	MOBILE BANKING USAGE	**AGREEMENT LEVEL**				
MBU	I am concerned about the possibility of cybercrime when using mobile banking.	1	2	3	4	5
MBU	I have experienced or know someone who has experienced cybercrime related to mobile banking.	1	2	3	4	5
MBU	The risk of cybercrime affects my decision to use mobile banking.	1	2	3	4	5
MBU	I believe that cybercrime incidents are increasing among mobile banking users.	1	2	3	4	5
MBU	I take additional security measures (e.g., using two-factor authentication) to protect myself from cybercrime when using mobile banking.	1	2	3	4	5