Journal of Co-operative and Business Studies (JCBS)
Vol.7, No.2; Publication Date: December. 31, 2023
ISSN: (Online) 2714-2043, (Print) 0856-9037
The current issue and full-text archive of this journal is available at: journals.mocu.ac.tz

Cite this article as: Mkilia, E. L., Kaleshu, J. & Sife, A. S. (2023). Cyber Security Dynamics and Usage of Mobile Banking Services Among Commercial Bank Customers in Tanzania. *Journal of Co-operative and Business Studies,* 7(2), 28-43.

Cyber Security Dynamics and Usage of Mobile Banking Services Among Commercial Bank Customers in Tanzania

Emmanuel L. Mkilia[1], Jones Kaleshu[2] and Alfred S. Sife[3]
[1] *Email: shamklia575@gmail.com*
[1, 2] *Department of Microfinance and Banking, Moshi Co-operative University, Tanzania.*
[2] *Email: jkaleshu@gmail.com*
[3] *Department of Knowledge Management, Moshi Co-operative University, Tanzania.*
Email: Alfred.sife@mocu.ac.tz

Abstract

Recent developments in the banking sector have greatly improved bank customers' access to and use of banking services. However, such development in the industry is subjected to various risks, causing mistrust of the banking infrastructures among its users. Using the Extended Parallel Process Model (EPPM) and Trust Theory, this paper aims to examine cyber security dynamics that affect commercial customers' decisions to use mobile banking services in Tanzania. By adopting a cross-sectional research design and Partial least squares structural equation modelling (PLS-SEM), this study found that customers' self-assessment, customers' decision to take risks and customers' confidence in Automated Teller Machines (ATM) applications have a positive and significant effect on mobile banking services usage. Moreover, the findings indicate that access to passwords has a negative significant relationship with mobile banking services usage. The influence of customers' trust in mobile phone applications was conformed insignificant towards mobile banking services usage. Based on these findings, a positive evaluation of the potential cyber risks and security measures enhances customers' trust and confidence when adopting and utilising mobile banking services. Thus, customers should be aware and carefully consider possible risks associated with mobile banking and adopt a sensible approach to cybersecurity while taking proactive measures to help protect their financial information.

Keywords: Cyber Security, Perceived Risks, Mobile Banking, PLS-SEM

1.0 Introduction

Recent developments in the banking sector have provided great convenience to bank customers in accessing and using banking services. Customers can now complete their banking at a time and place of their choice. Banking activities such as fund transfers, investments, payments, and regular account information check-ups are possible through mobile banking applications (Merhi *et al*., 2019). Such development is influenced by technological advancement, innovation, and invention that necessitate changing banking methods, ways of transacting, and revamping banking operations (Baabdullah *et al*., 2019). One of the witnessed changes in the banking sector is the introduction of mobile banking to easy, fast and effective banking transactions (Moşteanu *et al*., 2020). Mobile banking allows customers to conduct financial transactions remotely using mobile devices such as smartphones, tablets, and credit cards. However, such development in the industry is subjected to various risks, causing mistrust in the banking infrastructures among its users (Wazid *et al*., 2019). Mobile banking users are exposed to a range of cyber security risks, including identity theft, financial fraud, and malware attacks, among others (Thomas, 2018). Such exposure has increased concern among banks, regulators, and customers, calling for immediate interventions to increase trust and effective usage of mobile banking services.

Banking and other financial institutions across the globe have responded to that concern by implementing various cybersecurity systems to protect financial transactions and customer data. For example, banks have put in place systems and measures that allow for Two-Factor Authentication (2FA), End-to-End Encryption, Biometric Authentication, Mobile Device Management (MDM), Fraud Detection and Prevention and Secure Socket Layer (SSL) aiming at increasing the protection of the financial transaction and data of customers (Ghelani *et al*., 2022; Moşteanu, 2020; Srinivas *et al*., 2019). Such systems and measures have been managed to add a layer of security to prevent unauthorised access, ensure that data is not intercepted and read by unauthorised parties, verify customers' identities before granting access to their accounts, perform remote data wiping, enforce password policies, limit access to particular apps, and detect unusual activity or location-based anomalies (Tirfe & Anand, 2022). These safety measures are in place to guarantee a high level of security and operational dependability in banks, and they are powerful enough to foresee the likelihood of upcoming cyber events and take automatic safety precautions before a cyber breach relating to mobile banking (Uddin *et al*., 2020). This has aided in boosting the stability of banking transactions and fostering client confidence in mobile banking services (Ghelani *et al*., 2022).

Despite the presence of banks' cybersecurity systems, customers who use mobile banking are still concerned about the risks associated with mobile banking. Mobile banking customers in African countries are at higher risk of cybersecurity breaches and substantial financial losses than other continents (Mwangi *et al*., 2022; Mbanaso *et al*., 2019). The cost of financial cybercrime incidences in 2017 in five selected African countries (Ghana, Kenya, Nigeria, Tanzania and Uganda) was estimated to be USD 3.5 billion (Lebogang *et al*., 2022). In Tanzania, only in 2020, more than 3,141 cybercrime incidences were reported, which involved a total of TZS 5,045,985,155 in financial loss. This is a concern that threatens individuals' welfare and the economy of the country at large. Demirkan *et al*. (2020) and Dupont (2019) argue that although banks and other financial institutions have implemented cyber security systems to lessen cybercrime threats for mobile banking, these systems are still insufficient from customers' perspectives. The effectiveness of these systems also depends on the defensive factors and behaviours of the consumers of mobile banking services (Maalem *et al*., 2020). The defensive behaviours and factors involve strategies and actions customers develop to protect themselves and their financial information when using mobile banking services (McIlwraith, 2021). Customers satisfying themselves with these factors consent to their ultimate decision to use mobile banking services in the prevailing cybersecurity systems of banks (Ali *et al*., 2023).

The Extended Parallel Process Model (EPPM) claim that when people perceive a threat, they take two steps (Witte, 1992). First, they evaluate the threat's seriousness (perceived risks), and second, they assess their effectiveness and the efficacy of suggested actions (self-assessment) on a threat (Chen *et al*., 2020). Further, based on the Trust Theory (TT), customers' confidence in the security, reliability, and privacy of the mobile banking application and the institution that provides it inclines their likelihood to use mobile banking applications (Alshboul & Hamouri, 2023; Asnakew, 2020). Previous studies (e.g., Ali *et al*., 2023; Dash & Ansari, 2022; Sharma & Sharma, 2019; Gunduz & Das, 2020; Jünger & Mietzner, 2020; Singh & Srivastava, 2020) highlight factors such as customers' self-assessment, perceived risk, trusts in mobile applications, custody of credit cards and access to password as major defensive factors and behaviours observed in customers of various financial applications when responding to cybersecurity issues. These factors determine customers' dynamic use of financial services offered through mobile phones. However, what is not yet clear is the extent to which such factors are associated with the usage of mobile banking services among customers. Given the banks ' existing cybersecurity systems, it is necessary to understand how customers position themselves to use mobile banking services. Against this backdrop, this paper aims to examine cyber security factors affecting customers' decisions to use mobile banking services. Attaining this objective will shed knowledge and suggest ways to improve cybersecurity systems in mobile banking, thereby protecting customers from cyber-attacks and enhancing trust in these services.

2.0 Theoretical Review and Modelling

The Trust Theory (TT) and the Extended Parallel Process Model (EPPM) guided the study in exploring customers' defensive factors in cyber security systems and their usage of mobile banking services. The Trust Theory (TT) posits that trust is a psychological state rooted in the willingness to be vulnerable to another person based on their perceived trustworthiness. It is based on the belief that one party has in another party's reliability, honesty, and competence. On the other hand, the Extended Parallel Process Model (EPPM) is a theoretical framework that sheds light on how individuals process fear-based messages and make decisions in response to threats. It suggests that effective fear appeals should strike a balance by eliciting a strong sense of threat without overwhelming individuals' perceived efficacy. By integrating these theories, the study aims to conceptualise customers' defensive factors in cyber security systems and their adoption of mobile banking services.

2.1 Trust Theory

In 1978, Psychologist Jack Gibb introduced the Trust theory, emphasising the significance of trust in relationships. Within the realm of cyber security and mobile banking, trust serves as the foundation for the relationship between customers and service providers (Krishna *et al.*, 2022; Alshboul & Hamouri, 2023). By considering the three components of trust - perceived security, competence, and benevolence - service providers can enhance customers' trust, leading to increased usage of mobile banking services. To explore customers' defensive factors in cyber security systems and their adoption of mobile banking services, this study incorporated the Trust theory, specifically examining customers' trust in the security of mobile banking applications, passwords, and credit card applications (ATMs). However, the Trust theory does not adequately explain how customers evaluate self-assessment or make decisions regarding related cyber security risks. The Extended Parallel Process Model (EPPM) was incorporated as a supplementary framework to address this gap

2.2 Extended Parallel Process Model

The Extended Parallel Process Model (EPPM) was developed by communications scholar Kim Witte in 1992 as a fear appeal theory, specifically examining individuals' reactions to fear-inducing messages. This model holds significant relevance when studying customers' defensive factors in cyber security systems and their usage of mobile banking services. According to the EPPM, effective fear appeals strike a delicate balance by generating a strong sense of threat without overwhelming individuals' perceived efficacy. These appeals should provide clear and actionable recommendations, enhance self-efficacy, and emphasise the effectiveness of recommended behaviours to encourage adaptive responses.

By incorporating the EPPM, researchers gain insights into how individuals process fear-based messages, perceive threats, and make decisions regarding protective behaviours. This model has proven valuable in understanding and promoting behaviour change in various contexts, including cybersecurity and risk perception (Phuksuksakul *et al.*, 2021). The EPPM helps examine customers' defensive factors in cybersecurity systems and mobile banking services. It aids in identifying the factors that influence customers' responses to threats and how they can be motivated to take action, particularly in self-assessment and perceived risk

2.3 Hypothesis Development

2.3.1 Customers Self-Assessment

Customer self-assessment in mobile banking involves individuals evaluating mobile banking applications' security measures and protective elements. Customers play a vital role in assessing the cybersecurity systems implemented by financial institutions, considering factors like effectiveness, reliability, and trustworthiness (Vučinić, 2020). The objective is to ensure the safety of sensitive data during mobile banking activities (Sharma *et al.*, 2022). Key aspects to guarantee the self-assessment process include authentication mechanisms, data encryption, secure communication channels, system updates and patches, security awareness and education (Telo, 2023). This assessment lets customers make informed decisions about trusting a mobile banking service and take necessary steps to safeguard their financial information.

Mobile banking customers face concerns regarding cybersecurity scams, including theft through social engineering via various channels such as text messages, phone calls, and emails. The lack of awareness about social engineering poses a significant risk regarding human cyber security (Aldawood & Skinner, 2019). Threat detection and mitigation proficiency is influenced by factors such as the social, political, constitutional, organisational, economic, and personal aspects of the business environment. Customers often respond to cybersecurity risks by choosing to avoid or minimise their use of technology. Instead, they opt for traditional methods such as visiting physical bank premises, utilising mobile banking agencies, or relying on ATMs for their financial transactions. Customers with extensive cybersecurity awareness are more likely to use mobile banking services than those with limited awareness (Daengsi *et al*., 2021).

In Tanzania, many mobile banking customers have fallen victim to well-organised scammers through mobile banking platforms. Kessy's (2021) study revealed that despite customers having a good knowledge of mobile banking technologies, their awareness of the risks associated with cybersecurity systems is often limited. Based on these observations, the study hypothesises that:

H1: Customers' self-assessment of security measures associated with cybercrime on mobile banking services positively influences their use.

2.3.2 The decision to take a risk

Customers' decision-making regarding risk-taking is influenced by their perceptions of the risks associated with the cybersecurity systems in place. Concerns arise regarding data breaches and the compromise of personal and financial information (Zou *et al*., 2019). Research suggests that individuals develop risk evaluations and security awareness when exposed to information about security risks, such as data breaches (Chua *et al*., 2021). When considering mobile banking services, customers consider the service provider's track record regarding data breaches and the security measures implemented to prevent such incidents. The risk of identity theft is also a significant concern as customers assess the likelihood of personal information being stolen or misused, which could lead to fraudulent activities and financial losses (Jibril *et al*., 2020). The effectiveness of identity verification methods, data encryption, and secure authentication mechanisms employed by mobile banking service providers significantly influence customers' decision-making to use mobile banking services (Maček *et al*., 2019). It is important to note that customers' perceptions of risks can vary based on individual experiences, knowledge, and comfort levels with technology. Ultimately, customers' decision to use or not use mobile banking services is based on their assessment of the risks associated with the cybersecurity systems in place (Yan *et al*., 2021). Based on these observations, this study hypothesises that:

H2: The decision to take risks of using mobile banking is positively influenced by the prevailing mobile banking cybersecurity systems.

2.3.3 Trust of Mobile phone Applications for Mobile Banking

The customers' trust in mobile phone applications **used for mobile banking** significantly impacts their usage of mobile banking services. Trust is crucial in customers' decision to adopt and use mobile banking services. When customers trust the mobile phone application **used for mobile banking** and perceive it as secure and reliable, they are more likely to start using the offered mobile banking services. Additionally, customers develop defensive behaviours to enhance their security while using mobile banking applications.

These defensive factors are influenced by the cybersecurity systems implemented by mobile banking applications and customers' trust in secure usage practices (Hamid *et al*., 2022). While customers understand the importance of strong and unique passwords for their mobile banking applications, there is still a sense of distrust due to the increasing prevalence of cybersecurity compromises, cyber-attacks, and data breaches (Shankar *et al*., 2022). As a result, customers actively take proactive steps to enhance the security of their mobile banking applications and protect their sensitive data. Considering these factors, this study formulates the hypothesis that:

H3. Customers' trust in applications for mobile banking positively influences their use of mobile banking services.

2.3.4 Confidence in Credit Card Applications

Customers' confidence in credit cards can positively influence their willingness to use mobile banking services. Several factors, including trust in secure payment systems, familiarity with electronic transactions, perceived convenience, and financial control, play significant roles in shaping customers' attitudes towards mobile banking. When customers utilise credit card apps in mobile banking services, they demonstrate defensive behaviours to protect themselves against potential cybersecurity risks. However, despite the availability of payment options through point-of-sale (POS) terminals in various establishments, some customers still prefer cash payments over mobile banking services due to concerns about cybercrime risks (Marafon *et al*., 2018).

Customers' interest in credit cards goes beyond their benefits, as they prioritise the associated cybersecurity risks. Specifically, customers express concerns about data breaches and credit card fraud when using credit cards at POS terminals (Zou and Schaub, 2019). Despite security measures implemented by banks and payment processors, specific customers maintain a lack of trust in the security of credit card transactions. This lack of confidence can be influenced by factors such as data breaches, phishing scams, and a perceived lack of transparency in the payment process (Jamra *et al*., 2020; Mittal & Tyagi, 2020; Park *et al*., 2019). Considering these observations, this study formulates the following hypothesis:

H4: Customers' confidence in credit card applications for mobile banking positively impacts the usage of mobile banking services.

2.3.5 Access to password

A third-party access to customers' passwords can significantly impact their attitude toward mobile banking usage. Several factors, including convenience, security concerns, trust in password protection, perception of control, password management practices, and past experiences with password-related incidents, play a crucial role in shaping customers' overall attitude and willingness to engage with mobile banking services. Customers exhibit defensive behaviour regarding cybersecurity systems involved in third-party access to passwords within mobile banking services. This behaviour stems from concerns about potential unauthorised access to their accounts, financial fraud, and identity theft (Dzidzah *et al*., 2020; Kocabas *et al*., 2021; Li *et al*., 2019). If customers perceive the cybersecurity systems as weak or inadequate, they may hesitate to enter their passwords because they fear compromising their sensitive information (Ogonji *et al*., 2020). Furthermore, a lack of trust in the overall security infrastructure and implemented cybersecurity measures can contribute to customers' defensive behaviour in mobile banking usage (Zwilling *et al*., 2022). Based on these observations, this study puts forth the following hypothesis:

H5. Customers' confidence in passwords involved in mobile banking applications positively influences their decision to use mobile banking services.

2.4 Conceptual Framework

Fig 1 presents the Conceptual Framework that describes the relationship between dependent and independent variables. The dependent variable, mobile banking usage, depends on self-assessment, decision to take risks, mobile phone application and access to passwords based on the trust of mobile banking cyber security system while using mobile banking services.

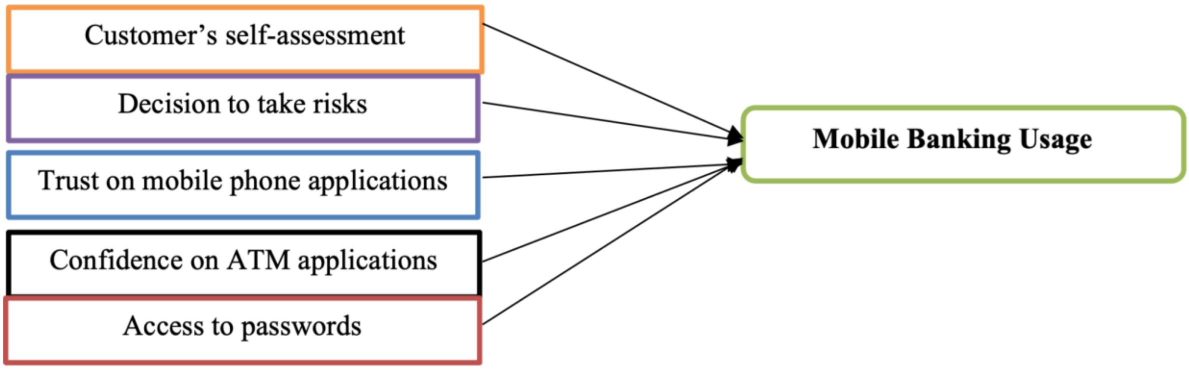
Customer's self-assessment
Decision to take risks
Trust on mobile phone applications
Confidence on ATM applications
Access to passwords
Mobile Banking Usage

Figure 1: Conceptual framework of the study

3.0 Methodology

3.1 Research design, sample size and sampling procedure

This study used a cross-sectional research design in which quantitative data were collected. Data was collected at a particular point in time. A quantitative method examined the relationships between the variables under investigation. A survey strategy was also employed, which is typically connected with the deductive approach and allows for collecting huge amounts of data from a large population in a cost-effective manner (Saunders *et al*., 2012). Data was mainly obtained by using a questionnaire.

The study was conducted in Dar es Salaam because it is the capital business city with the highest number of commercial banks and their headquarters. Dar es Salaam has the highest number of commercial bank branches compared to other regions in Tanzania (BOT, 2020). The city is also categorised as having a high percentage of people formally financially included, with a score of 73%, and 40% of its population have or use bank services (Fin Scope, 2017). Cochran's (1977) formula for the unknown population was used to calculate the sample size at a confidence level of 95%, and a 5% sampling error was considered.

$$n_0 = \frac{Z^2pq}{e^2} = \frac{(1.96)^2x0.5x0.5}{0.05^2} = 384\ respondents$$

Where n is the sample size, Z is the selected critical value of the desired confidence level, p is the estimated proportion of an attribute that is present in the population, q=1- p, and e is the desired level of precision; p = 0.5 and hence q=1-0.5 = 0.5; e= 0.05; z =1.96

Purposive sampling was employed to select ten commercial banks in the study, as the aim was to involve well-informed institutions in mobile banking services. Convenience sampling was used to obtain 478 commercial mobile bank customers as respondents. However, contrary to the calculated sample, 478 mobile customers of commercial banks took part in this research for two reasons. First, Hair *et al.* (2019) suggest that the sample size range between 200 and 500 is appropriate when analysing data using the Structural Equation Model (SEM). This is why the sample size was larger than the calculated 384. Second, having more data is better since it reduces parameter estimate error and enhances decision accuracy (Kelly & Lai, 2011).

The commercial bank customers who participated in this study were from NMB, CRDB, KCB, NBC, DTB, Azania Bank, FNB, TPB (now Tanzania Commercial Bank TCB), Stanbic and Equity Bank. The establishment in terms of the number of branches countrywide, their level of information technology development, the number of customers they serve, and their experience in operations were all factors in choosing these banks and their customers to be respondents.

Partial least squares structural equation modelling (PLS-SEM) was used to gauge bank clients' defensive factors on cybersecurity system usage of mobile banking services. PLS-SEM is a statistical technique that allows researchers to simultaneously test and estimate predicted associations in a conceptual model, allowing them to determine probable correlations between dependent and independent variables. The dimensionality of mobile banking usage was investigated using confirmatory factor analysis (CFA), which assessed the overall validity of the measures to see if the constructs (self-assessment, decision to take risk, mobile phone apps, access to password) fit the data set. PLS-SEM was deemed appropriate because the research goal was to predict and explain the variance of dependent variables as explained by distinct, independent factors.

3.2 Validity and Reliability

CFA was used to check whether the proposed model was fit, and all of the item variables had loadings larger than 0.7. Convergent validity, Reliability, and Discriminant validity were used to assess the measurement model's validity. Convergent validity refers to the degree to which theoretically linked scale items should strongly correlate. The three most popular metrics for convergent validity of measures are Composite Reliability (CR) above 0.6, Cronbach Alpha (CBA) above 0.7, and Average Variance Extracted (AVE) above 0.5. (Hair *et al*., 2019). Prior to verifying data analysis by convergent validity and discriminant validity, confirmatory factor analysis (CFA) was used to validate the instrument. The instrument-based one-factor loading test is proposed to attain a significant level (p< 0.05) by CFA via the model's convergent validity verification, which is acceptable (Nyongesa *et al*., 2020). The results demonstrate that all of the items were significant. According to the results, all factors passed the test (see Table 1).

Table 1: Items Reliability, Constructs Reliability and Convergent Validity Tests

Aspects	Items	Loadings	VIF	CR	AVE
Mobile Usage	MBU1	0.914	2.001	0.864	0.682
	MBU2	0.859	1.875		
	MBU3	0.788	1.329		
Self-Assessment	SAS1	0.887	1.244	0.790	0.561
	SAS2	0.734	1.225		
	SAS3	0.704	1.326		
The decision to Take Risk	DTR1	0.781	1.639	0.834	0.502
	DTR2	0.761	1.405		
	DTR3	0.701	1.394		
	DTR4	0.683	1.321		
	DTR5	0.711	1.457		
Mobile Phone App	MP_App1	0.739	1.361	0.809	0.514
	MP_App2	0.731	1.264		
	MP_App3	0.746	1.249		
	MP_App4	0.705	1.347		
ATM Card App	AC_App1	0.719	1.252	0.804	0.577
	AC_App2	0.788	1.300		
	AC_App3	0.771	1.210		
Access to Password	AC_Pass1	0.757	1.203	0.840	0.637
	AC_Pass2	0.809	1.723		
	AC_Pass3	0.826	1.706		

3.2.1 Discriminant Validity test

The Fornell-Lacker criterion is used to determine whether or not there are any relationships between constructs that are not supposed to be related.

Table 2: Discriminants Validity (Fornell-Larcker Criterion)

	MBU	SAS	DTR	MP_App	AC_App	AC_Pass
MBU	**0.826**					
SAS	0.867	**0.749**				
DTR	0.523	0.707	**0.709**			
MP_App	0.540	0.606	0.557	**0.717**		
ATM_App	0.543	0.584	0.588	0.629	**0.760**	
AC_Pass	0.475	0.635	0.793	0.457	0.550	**0.798**

NOTE: Diagonals represent SQUARE ROOT OF Average Variance Extracted (AVE)

The degree to which a construct is empirically distinct from other constructs in the structural model is known as discriminant validity. The standard metric was proposed by Fornell and Larcker (1981), who advised that each construct's AVE be compared to the squared inter-construct correlation (as a measure of shared variance) of that construct and all other reflectively assessed constructs in the structural model. All model constructs' shared variance should not be greater than their AVEs. Because the squared correlation of all components is greater than the squared correlation of other constructs, the result demonstrates discriminant validity (Hair *et al*., 2019).

4.0 Findings

The study analysed the significance of the effect of customers' Self-Assessment (H1), the decision to take risks (H2), trust in mobile phone applications (H3), confidence in ATM Card applications (H4) and access to passwords (H5) on mobile banking usage. All modelled main hypotheses were tested simultaneously, and their results are shown in Table 4. The study findings confirm the acceptance of four out of five hypotheses. First, the analysis confirmed the positive and significant impact of customers' self-assessment (β = 0.958, p < 0.01) on mobile banking usage, supporting H1. This suggests that the customers' self-assessment of the cybersecurity systems plays an important role as one of the defensive factors in their decision to use mobile banking services offered by banks. Second, the study findings indicate that the effect of customers' decision to take risks on mobile banking usage is positive and significant (β = 0.187, p < 0.01). These findings confirm H2. This shows that mobile banking customers' desires towards risks involved in mobile banking services signify their decision to use mobile banking.

Table 3: Hypotheses testing results

		R2 = 0.778			
Hypotheses	Path	Coefficient	T Statistics	P Values	Remark
H1	SAS -> MBU	0.958	18.354	0.000	Significant
H2	DTR -> MBU	0.187	3.608	0.000	Significant
H3	MP_App -> MBU	0.019	0.359	0.719	Not Significant
H4	ATM_App -> MBU	0.113	2.262	0.024	Significant
H5	AC_Pass -> MBU	-0.056	4.074	0.000	Significant

Third, findings reveal that customers' confidence in ATM applications has a positive significant effect (β = 0.113, p < 0.01) on mobile banking services usage, confirming H4. Lastly, H5 was accepted as the findings indicate that access to passwords (β = -0.056, p < 0.01) negatively correlates with mobile banking services usage. This connotes that customers exhibit defensive behaviour when they feel unsafe with cybersecurity systems that may allow third parties to access passwords involved in mobile banking services. However, the influence of customers' Trust on mobile phone applications (H3) was confirmed insignificant (β=0.019, P< 0.719) towards mobile banking services usage. Hence, H3 was not supported.

While customers' defensive factors on cybersecurity systems as to mobile banking usage are led by self-assessment, followed by a decision to take risk, confidence in ATM applications and access to password, from these findings, generally, the customers' defensive factors determine more 77% (R2 = 0.778) of their likelihood to use mobile banking services based on the prevailing banks' cybersecurity systems.

4.1 Discussions of the Findings

4.1.1 Customers Self-Assessment

The study's findings revealed that customers' self-assessment as a defensive factor in the state and implications of the banks' cybersecurity systems positively influence their likelihood of using mobile banking services. Customers' self-assurance and acceptance of the effectiveness, reliability, and trustworthiness of cybersecurity measures in banks that relate to mobile banking services give rise to their effective decision to use them. Such assurance and acceptance rely on aspects such as authentication mechanisms, data encryption, secure communication channels, system updates, and patches. The indication is that whenever customers assess themselves and come up with a positive perception of banks' cybersecurity systems, it instils their confidence that sensitive data will be protected and their financial transactions will be secure. This, in turn, encourages them to engage in mobile banking activities and rely on mobile banking services for their financial needs. As reflected in previous studies (e.g., Telo, 2023; Sharma *et al*., 2022; Vučinić, 2020; Aldawood & Skinner, 2019), customers' self-assessment of cybersecurity systems allows them to make informed decisions about the level of trust that they can place in a mobile banking service depending on the banks' cybersecurity systems. Based on these findings, customers' self-assessment enables them to evaluate the security measures in place, gauge the level of risk associated with using the service and take necessary steps to protect their financial information regarding mobile banking services.

4.1.2 Customers' Decisions to take risk

This study found that customers' decision to take risks associated with cybersecurity systems on mobile banking positively and significantly signifies their decision to use mobile banking services. These findings concur with the studies by Hanif and Lallie (2021), Khatun *et al*. (2021), Shankar and Rishi (2020), and Alraja *et al*. (2019), who reported a positive association between customers' decision to take risks on cybersecurity systems and mobile banking usage. The fact that there are no entirely risk-free systems customers' willingness to accept these risks for the benefits and convenience of the services offered stimulate customers' decision to use mobile banking. Customers' appetite towards mobile banking potential cybersecurity risks such as data breaches, identity theft, and financial fraud are in a better position to access and enjoy fast, convenient, and timely financial transactions using their mobile devices. Likewise, this study's findings imply that customers who embrace risk-taking may perceive mobile banking services as an opportunity for financial growth and efficiency. They recognise the potential benefits of quick and convenient access to their accounts, faster transactions, and enhanced financial management tools. These findings imply that perceived benefits outweigh the potential risks associated with cybersecurity and increase customers' likelihood of using mobile banking services. Additionally, this study's findings suggest that customers willing to take risks may take a proactive approach to cybersecurity. They actively educate themselves about best practices, employ security measures like strong passwords and two-factor authentication, and regularly update their mobile banking apps to mitigate potential risks. This responsible behaviour further reinforces their trust in the system and encourages continued usage of mobile banking services.

4.1.3 Trust of Mobile phone Applications for Mobile Banking

As for customers' confidence in ATM applications regarding cybersecurity systems in banks, this study's findings indicated a positive significant effect on mobile banking services usage. In line with previous studies (e.g., Jamra *et al*., 2020; Mittal & Tyagi, 2020; Park *et al*., 2019; Zou and Schaub, 2019), confidence in using ATM applications that incorporate robust cybersecurity systems can indeed have a positive influence on mobile banking usage. The implication is that ATM applications offer customers the convenience of conducting banking transactions anytime and anywhere using their mobile devices. With secure cybersecurity systems, customers can confidently access their accounts, check balances, transfer funds, and perform various banking activities efficiently using ATM applications. This convenient accessibility can lead to increased usage of mobile banking services. Customers who feel that their ATM personal and financial information is well-protected are more likely to engage in mobile banking services. Based on this study's findings, when customers lose confidence in ATM applications due to cybersecurity risks, they will defend themselves by refraining from using mobile banking services.

4.1.4 Access to Password

This study's findings also revealed a significant negative relationship between the possibility of a third party accessing the password due to poor bank cybersecurity systems and mobile banking services usage. This suggests that customers may be reluctant to enter their passwords and, hence, use mobile banking services if they believe the cybersecurity systems are weak or insufficient to the extent of compromising their personal information. Zwilling *et al*. (2022), Kocabas *et al*. (2021), Dzidzah *et al*. (2020), Ogonji *et al*. (2020), and Li *et al*. (2019) also reported that customers may hesitate to enter their passwords and use mobile banking services due to the fear of compromising their sensitive information when they perceive the banks' cybersecurity systems to be weak or inadequate. Such behavioural conduct is driven by worries about possible identity theft, financial fraud, and unauthorised access to their accounts. The implication is that a lack of trust in the overall security infrastructure and implemented cybersecurity systems of banks offering mobile banking services can contribute to customers' defensive behaviour of not using mobile banking services.

5.0 Conclusion and Recommendations

This study examined the customer's defensive factors regarding cybersecurity systems and the usage of mobile banking services. From the study, it can be concluded that customers' self-assessment of cybersecurity systems is vital in influencing their usage of mobile banking services. A positive evaluation of security measures enhances customers' trust and confidence in the service, leading to increased adoption and utilisation of mobile banking applications. By considering the potential risks and taking proactive measures, customers can protect their financial information and engage in secure mobile banking activities. Furthermore, it is essential to note that taking risks can positively influence mobile banking usage; a sensible and informed approach to cybersecurity should accompany it. Finally, it is critical to note that the positive influence on mobile banking usage is contingent on implementing effective cybersecurity systems. If customers perceive the ATM application to have weak security measures or if there have been security breaches, it could negatively impact their usage. Continuous monitoring, updates, and improvements to the cybersecurity systems are crucial to maintaining customers' trust and promoting ongoing usage of ATM applications in mobile banking. Moreover, customers are more likely to resist using mobile banking services if they feel unsafe about the authorised parties accessing their password involved in mobile banking services.

It is recommended that customers should be aware and carefully consider potential risks associated with mobile banking and adopt a sensible approach to cybersecurity while taking proactive measures to help protect their financial information. Similarly, it is recommended that banks ensure robust security measures to enhance customer confidence by updating and improving security protocols to help maintain trust and prevent security breaches. Moreover, banks must advise customers to use strong, unique passwords and avoid sharing them with others. Regularly changing passwords and using additional authentication methods, such as two-factor authentication, can enhance security.

References

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, 14*(7), 1523-1536.

Alam, S. S., Omar, N. A., Ariffin, A. M., & Hashim, N. M. H. N. (2018). Integrating TPB, TAM and DOI theories: An empirical evidence for the adoption of mobile banking among customers in Klang Valley, Malaysia. *International Journal of Business and Management Science, 8*(2), 385-403.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73.

Aldiabat, K., Al-Gasaymeh, A., & Rashid, A. S. K. (2019). The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry. *iJIM, 13*(2), 37.

Ali, A., Hameed, A., Moin, M. F., & Khan, N. A. (2023). Exploring factors affecting mobile-banking app adoption: a perspective from adaptive structuration theory. *Aslib Journal of Information Management*, *75*(4), 773-795.

Almarashdeh, I., Aldhmour, K., Aljamaeen, R., Alsmadi, M., & Jaradat, G. (2019, December). The effect of perceived trust in technology, trust in the bank and perceived risk on customer adoption of mobile banking. In *2019 international conference on internet of things, embedded systems and communications (IINTEC)* (pp. 118-123). IEEE.

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.

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: the mediation role of risk perception. *Ieee Access*, *7*, 111341-111354.

Alshboul, Y., & Al. Hamouri, N. (2023). Cybersecurity antecedents of trust: toward OPS adoption in Jordan. *International Journal of Information and Decision Sciences, 15*(1), 73-93.

Ananda, S., Devesh, S., & Al Lawati, A. M. (2020). What factors drive the adoption of digital banking? An empirical study from the perspective of Omani retail banking. *Journal of Financial Services Marketing, 25*(1-2), 14-24.

Asnakew, Z. S. (2020). Customers' continuance intention to use mobile banking: Development and testing of an integrated model. *The Review of Socionetwork Strategies, 14*(1), 123-146.

Ataya, M. A. M., & Ali, M. A. (2019, August). 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.

Baabdullah, A. M., Alalwan, A. A., Rana, N. P., Kizgin, H., & Patil, P. (2019). Consumer use of mobile banking (M-Banking) in Saudi Arabia: Towards an integrated model. *International journal of information management*, *44*, 38-52.

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.

Bani-Hani, I., & Shepherd, E. (2021, July). Self-Reinforcement Mechanisms of Sustainability and Continuous System Use: A Self-Service Analytics Environment Perspective. In *Informatics* (Vol. 8, No. 3, p. 45). MDPI.

Changchit, C., Klaus, T., Lonkani, R., & Sampet, J. (2020). A cultural comparative study of mobile banking adoption factors. *Journal of Computer Information Systems, 60*(5), 484-494.

Chaouali, W., Souiden, N., & Ladhari, R. (2017). Explaining adoption of mobile banking with the theory of trying, general self-confidence, and cynicism. *Journal of Retailing and Consumer Services, 35*, 57-67.

Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., ... & Xu, L. (2020, June). An empirical assessment of security risks of global android banking apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 1310-1322).

Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., & Hammer, J. (2020, July). Hacked time: Design and evaluation of a self-efficacy based cybersecurity game. In *Proceedings of the 2020 acm designing interactive systems conference* (pp. 1737-1749).

Chopdar, P. K., Korfiatis, N., Sivakumar, V. J., & Lytras, M. D. (2018). Mobile shopping apps adoption and perceived risks: A cross-country perspective utilising the Unified Theory of Acceptance and Use of Technology. *Computers in Human Behavior, 86*, 109-128.

Chua, H. N., Teh, J. S., & Herbland, A. (2021). Identifying the effect of data breach publicity on information security awareness using hierarchical regression. *IEEE Access*, *9*, 121759-121770.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies,* 1-24.

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *Int. Res. J. Eng. Technol.* (IRJET), 9.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics, 7*(2), 189- 208.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity, 5*(1), tyz013.

Dzidzah, E., Owusu Kwateng, K., & Asante, B. K. (2020). Security behaviour of mobile financial service users. *Information & Computer Security, 28*(5), 719-741.

Farah, M. F., Hasni, M. J. S., & Abbas, A. K. (2018). Mobile-banking adoption: empirical evidence from the banking sector in Pakistan. *International Journal of Bank Marketing*, *36*(7), 1386-1413.

Febrian, D., Simanjuntak, M., & Hasanah, N. (2021). The effect of benefits offered and customer experience on re-use intention of mobile banking through customer satisfaction and trust. *Jurnal Keuangan dan Perbankan, 25*(3), 551-569.

Geebren, A., Jabbar, A., & Luo, M. (2021). Examining the role of consumer satisfaction within mobile eco-systems: Evidence from mobile banking services. *Computers in Human Behavior*, 114, 106584.

Ghauri, F. A. (2021). Why Financial Sectors Must Strengthen Cybersecurity. *International Journal of Computer Science and Information Security (IJCSIS),* 19(7).

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*, 1-9

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks, 169*, 107094.

Hamid, K., Iqbal, M. W., Muhammad, H. A. B., Fuzail, Z., Ghafoor, Z. T., & Ahmad, S. (2022). Usability evaluation of mobile banking applications in digital business as emerging economy. *Int. J. Comput. Sci. Netw. Secur, 22*, 250-260.

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.

Ho, J. C., Wu, C. G., Lee, C. S., & Pham, T. T. T. (2020). Factors affecting the behavioral intention to adopt mobile banking: An international comparison. *Technology in Society, 63*, 101360.

Jamra, R. K., Anggorojati, B., Sensuse, D. I., & Suryono, R. R. (2020). Systematic Review of Issues and Solutions for Security in E-commerce. In *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)* (pp. 1-5). IEEE.

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management, 7*(1), 1832825.

Jünger, M., & Mietzner, M. (2020). Banking goes digital: The adoption of FinTech services by German households. *Finance Research Letters, 34*, 101260.

Kangapi, T. M., & Chindenga, E. (2022, May). Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa. In *2022 IST-Africa Conference (IST-Africa)* (pp. 1-8). IEEE.

Karjaluoto, H., Shaikh, A. A., Saarijärvi, H., & Saraniemi, S. (2019). How perceived value drives the use of mobile financial services apps. *International Journal of Information Management, 47*, 252-261.

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.

Khatun, M. N., Mitra, S., & Sarker, M. N. I. (2021). Mobile banking during COVID-19 pandemic in Bangladesh: A novel mechanism to change and accelerate people's financial access. *Green Finance, 3*(3), 253-267.

Kocabas, H., Nandy, S., Tamanna, T., & Al-Ameen, M. N. (2021). Understanding User's behavior and protection strategy upon losing, or identifying unauthorised access to online account. In *HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings* (pp. 310-325). Cham: Springer International Publishing.

Krishna, B., Krishnan, S., & Sebastian, M. P. (2022). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, 1-29.

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating cybersecurity strategies in africa. In *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 1-19). IGI Global.

Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimisation perspective. *Decision Support Systems, 121*, 13-24.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1), 1-18.

Maček, N., Adamović, S., Milosavljević, M., Jovanović, M., Gnjatović, M., & Trenkić, B. (2019). Mobile banking authentication based on cryptographically secured iris biometrics. *Acta Polytechnica Hungarica*, 16(1).

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *The African Journal of Information and Communication,* 23,1-26.

McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

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.

Mittal, S., & Tyagi, S. (2020). Computational techniques for real-time credit card fraud detection. Handbook of Computer Networks and Cyber Security: *Principles and Paradigms,* 653-681.

Moşteanu, D. N. R., Faccia, D. A., Cavaliere, L. P. L., & Bhatia, S. (2020). Digital technologies' implementation within financial and banking system during socio distancing restrictions–back to the future. *International Journal of Advanced Research in Engineering and Technology*, *11*(6).

Moşteanu, N. R. (2020). Challenges for organisational structure and design as a result of digitalisation and cybersecurity. *The Business & Management Review, 11*(1), 278-286.

Mwangi, T., Asava, T., & Akerele, I. (2022). Cybersecurity Threats in Africa. In *The Palgrave Handbook of Sustainable Peace and Security in Africa* (pp. 159-180). Cham: Springer International Publishing.

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review, 38*, 100312.

Ong, H. B., Jaffar, N., Yap, V. C., & Norhashim, M. (2023). Empirical analysis of internet and mobile banking in Malaysia. *Asian Economic and Financial Review, 13*(2), 138- 147.

Owusu Kwateng, K., Osei Atiemo, K.A. and Appiah, C. (2019), "Acceptance and use of mobile banking: an application of UTAUT2", *Journal of Enterprise Information Management, 32* (1), 118-151.

Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries, 29*(1), 31-43.

Phuksuksakul, N., Kanitpong, K., & Chantranuwathana, S. (2021). Factors affecting behavior of mobile phone use while driving and effect of mobile phone use on driving performance. *Accident Analysis & Prevention, 151*, 105945.

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.

Salam, M. A., Saha, T., Rahman, M. H., & Mutsuddi, P. (2021). Challenges to Mobile Banking Adaptation in COVID-19 Pandemic.'. *Journal of Business and Management Sciences, 9*(3), 101-113.

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

Shankar, A., Tiwari, A.K. and 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.

Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms. *IJARCCE, 11*(7), 153-160.

Sharma, S. K. (2019). Integrating cognitive antecedents into TAM to explain mobile banking behavioral intention: A SEM-neural network modeling. *Information Systems Frontiers, 21*(4), 815-827.

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. and Srivastava, R.K. (2018), "Predicting the intention to use mobile banking in India", *International Journal of Bank Marketing*, *36*(2), 357-378.

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), 86-96.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems, 92*, 178-188.

Telo, J. (2023). Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis. *Sage Science Review of Educational Technology, 6*(1), 26-38.

Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management, 12*(3), 1-23.

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.

Tian, Y., Chan, T. J., Mohd Suki, N., & Kasim, M. A. (2023). Moderating Role of Perceived Trust and Perceived Service Quality on Consumers' Use Behavior of Alipay e-wallet System: The Perspectives of Technology Acceptance Model and Theory of Planned Behavior. *Human Behavior and Emerging Technologies*, *2023*(527640).

Tirfe, D., & Anand, V. K. (2022). A survey on trends of two-factor authentication. In *Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020* (pp. 285-296). Springer Singapore.

Trinh, H. N., Tran, H. H., & Vuong, D. H. Q. (2020). Determinants of consumers' intention to use credit card: a perspective of multifaceted perceived risk. *Asian Journal of Economics and Banking, 4*(3), 105-120.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management, 22*(4), 239-309.

Van, H. N., Pham, L., Williamson, S., Huong, V. T., Hoa, P. X., & Trang, P. L. H. (2020). Impact of perceived risk on mobile banking usage intentions: trust as a mediator and a moderator. *International Journal of Business and Emerging Markets, 12*(1), 94-118.

Vučinić, M. (2020). Fintech and financial stability potential influence of FinTech on financial stability, risks and benefits. *Journal of Central Banking Theory and Practice, 9*(2), 43- 66.

Wang, W. (2019), "The influence of perceived technological congruence of smartphone application and air travel experience on consumers' attitudes toward price change and adoption", *Journal of Hospitality and Tourism Technology, 10*(2), 122-135.

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.

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.

Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking, 10*(6), 15-56.

Wu, D., Moody, G. D., Zhang, J., & Lowry, P. B. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Information & Management, 57*(5), 103235.

Yan, C., Siddik, A. B., Akter, N., & Dong, Q. (2021). Factors influencing the adoption intention of using mobile financial service during the COVID-19 pandemic: The role of FinTech. *Environmental Science and Pollution Research*, 1-19.

Yildirim, N., & Varol, A. (2019,). A research on security vulnerabilities in online and mobile banking systems. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

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, 10*(3), 279-295.

Zou, Y., & Schaub, F. (2019). Beyond mandatory: Making data breach notifications useful for consumers. *IEEE Security & Privacy, 17*(2), 67-72.

Zou, Y., Danino, S., Sun, K., & Schaub, F. (2019). You Might'Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.