Local Administration Journal 16(3) • July – September • 329 - 354
Received: April 15, 2023 • Revised: May 22, 2023 • Accepted: June 6, 2023
RESEARCH ARTICLE

Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania

Emmanuel Lameck Mkilia
Department of Banking Accounting and Finance - Moshi Co-operative University (MoCU)

Jones T. Kaleshu
Department of Banking Accounting and Finance - Moshi Co-operative University (MoCU)

Alfred S. Sife
Professor, Department of Knowledge Management – Moshi Co-operative University (MoCU)

Abstract
Cybersecurity threats rise as more people use mobile applications to access their bank accounts. This study examined customer's protection motivation on cybersecurity risks and usage of mobile banking services in Tanzania. A survey of 478 commercial bank customers was conducted using questionnaire and key informant interviews. The relationship between mobile banking customers' protection motivation of cybersecurity and how it affects their use of mobile banking services was analyzed using partial least squares structural equation modeling (PLS-SEM). The results indicate that perceived threat, perceived severity, data confidentiality, self-efficacy, and cybersecurity awareness have significant influences on mobile banking customers on use of mobile banking services. The results of the study are in line with Protection Motivation Theory (PMT) because of the fact that five out of seven constructs derived from risk appraisal and coping appraisal were found to influence use of mobile banking services. The study concludes that protective behavior on usage of mobile banking services by customers depends on cybersecurity threat appraisal and coping appraisal. However, perceived susceptibility and perceived integrity had no effect. It is recommended that banks should make an investment in educating users about the mobile banking service by providing guidance and information, which will lessen the impact of cybersecurity concerns.

Keywords:
Cybersecurity, Mobile Banking, Protective Behavior

CORRESPONDING AUTHOR
Emmanuel Lameck Mkilia, Department of Banking Accounting and Finance, Moshi Co-operative University, P.O Box 474. Sokoine Road, Tanzania. E-Mail: shamklia575@gmail.com

1. Introduction

Mobile banking is a service offered by banks and other financial institutions to allow users access financial services via a mobile device such as mobile phones or laptops. Checking balances, paying bills, and transfer of money from one bank account to another or from a bank account to mobile money services are examples of such services. Mobile banking services provide several advantages including low service delivery costs, low transaction costs, manageability, real-time data upgrades, quick transaction verification, worldwide connectivity, and online banking services (Rahi *et al.,* 2020; Wazid *et al*., 2019). From the perspective of the banks, mobile banking is projected to result in lower costs to financial services providers and increased competitiveness (Farah *et al*., 2018). Banks see mobile banking as a way to gain a competitive advantage. However, practices indicate that prices for bank clients who use mobile services are marginally higher than those who utilize services at bank counters. Despite the costs associated with mobile banking, customers tend to use it because of other costs such as transport to the bank and time spent while waiting for services.

Despite the tremendous developments in the adoption and use of mobile banking, there are concerns about cybersecurity risks. The term cybersecurity risks refer to possibility of occurrence that has the potential to harm information system by illegal access, destruction, disclosure, alteration of data, and/or denial of service (Tariq, 2018; Mugari *et al.,* 2016). The major goal of cybersecurity in digital banking is to safeguard the assets of customers because as more individuals go cashless, more activities and transactions are taking place online. Malicious attacks that seek to unlawfully access confidential financial data, disrupt digital operations, damage information, theft of funds from mobile banking, weak security infrastructure, phishing, cyber pyramid frauds, and system hacking are among the top cybersecurity issues that financial institutions face (He *et al.,* 2015).

Credential and identity theft are the most common cybersecurity risks to mobile banking clients (Wyre *et al.,* (2020). Account takeover is a particularly hazardous type of cybersecurity attack in which a criminal gains access to a customer's account and then alters information on it, preventing the real owner from accessing it or receiving account updates. They could potentially use the information acquired to commit identity theft. Presence of cybersecurity risks and privacy issues to mobile banking customers has therefore become prevalent considering the magnitude of digital related transactions particularly on mobile banks platforms. The news and experiences about the safety of mobile banking have made bank clients feel uncomfortable (Marafon *et al*., 2018).

The presence of cybersecurity risks and violation of privacy has been considered as one of the factors that influence bank customers' protective behavior toward decision to use mobile banking services (Jibril *et al.,* 2020; Singh and Srivastava, 2018). The major challenges posed by these cybersecurity risks is due to complications caused by the variety of mobile devices and platforms from which customers are required to use. For instance, as part of an effort to enhance income and tax collection, the government of Tanzania developed a payment gateway to make it simpler for individuals to pay for government services using a created control number, putting them at risk for cybercrime. As online services develop and proliferate, people are therefore forced to use mobile banking services, which exposes them to a variety of cybersecurity issues as a result of cyber-attacks.

A study by Mbanaso *et al*. (2019), shows that African countries as being at risk concerning cybersecurity breaches and experienced substantial financial losses through cyber-attacks. Serianu (2017) reported that estimated cost of financial cybercrime incidences in businesses in 2017 was USD 3.5 billion in five selected African countries (Ghana, Kenya, Nigeria, Tanzania and Uganda). Amongst the top cybersecurity weaknesses faced by financial institutions in Africa are cybersecurity skills gap, insufficient guidelines on detection, protection and response to cybercrime incidences and partial formal frameworks for measuring actual cybersecurity resilience (Semboja *et al.,* 2017).

In Tanzania, it is estimated that half the population own mobile phones but only one in four use mobile banking. There were about 29.4 million active registered accounts for mobile money by the end of December 2020 (BOT, 2020). However, many customers tend to sign up for mobile banking applications but some become reluctant to use it due to a defensive motivation brought on by cybersecurity risks when connected to internet. The use of mobile banking services is influenced by many factors including pursuance, transaction speed, communication, personal desire, personal knowledge, habit, resistance to innovation, and experience. The use or repetition of mobile banking services by mobile banking customers is not guaranteed by their approval of using those services.

Merhi *et al*. (2021) argue that one of the key issues affecting many online applications such as e-commerce, mobile banking, and online shopping is user behavior that is protective owing to cybersecurity-related threats. According to Mettouris *et al*. (2015), mobile banking consumers experience cybersecurity anxiety because of its inherent uncertainty, anonymity, and lack of human contact or interpersonal relationships. This encourages them to take precautions when using mobile banking services in a virtual environment. Clients may have handled their

financial services through mobile banking applications instead of visiting the bank counter if bank customers had a good awareness and experience with cybersecurity. In Tanzania, variables impacting the adoption of mobile banking have been examined, however, the nexus between customers' protection motivation on cybersecurity risks and use of mobile banking services is not known (Chawla and Joshi, 2018; Choudrie *et al*., 2018; Tsai *et al* 2016). This study therefore sought to examine customer's protection motivation on cybersecurity risks and usage of mobile banking services in Tanzania. Specifically, this study aimed to:

- Analyze the customer's protective behavior in relation to cybersecurity risks and the driving force behind using mobile banking services.
- Determine the driving forces behind consumers' protective behavior when using mobile banking services.

2. Theoretical Review and Modeling

Protection Motivation Theory (PMT). PMT is a combination of threat and coping appraisals as proposed by Rogers in 1975 and it was revised in 1983. Threat appraisals and coping appraisals, according to PMT, inspire protective behavior (Chang *et al.,* 2018). PMT states that two cognitive processes, threat assessment and coping appraisal influence people's protective motivation (i.e., the desire to perform a recommended action or behavior). Both appraisals can be triggered by a variety of sources of information or antecedents (Rogers, 1983) such as observational learning, personality factors, or prior experience with the danger.

The risk evaluation assesses the severity and seriousness of the problem, whereas the coping appraisal assesses how one handles it. Studies on perception of online dangers (Towbin, 2019, Tsai et al., 2016), information security, and health cybersecurity are among the studies that have used the PMT framework (Menard et al., 2017). When an individual is confronted with a threat, PMT implies that threat assessments and coping appraisals drive the individual's response to the threat (Verkijika, 2018, van Bavel *et al* 2019). PMT posits that threat, susceptibility and severity have positive effects on adaptive behavior and that intrinsic and extrinsic rewards minimize an individual's sensitivity to the threat and have a negative impact on adaptive behavior.

PMT is relevant for this study because the study sought to examine mobile customers protective motivation on cybersecurity risks and usage of mobile banking services (Johnson *et al.,* 2018; Abdullah & Ward, 2016). In this study, PMT is modified whereby risk assessments are determined by perceived threat, perceived severity, susceptibility, data integrity and

confidentiality which is linked to maladaptive behavior, while coping appraisals are based on self-efficacy and cybersecurity awareness is linked with safe or adaptive behaviors. Maladaptive responses are a range of behaviors in which the threat recipient avoids implementing a recommended response. Adaptive behaviors are recommended responses that are designed to safeguard someone from the risk.

Hypothesis Development

Risk Appraisal

Perceived threat

A cybersecurity threat is any harmful attack that attempts to gain unauthorized access to data, disrupt digital activities, or damage data. These threats are also associated with the development of mobile banking technologies that come up with associated risks (Nambiro *et al.,* 2020). The imagined magnitude of uncertainty that an individual can experience when confronted with a certain scenario or stimuli is referred to as a perceived threat (Alexandrou & Chen, 2019). The majority of these threats are anonymous remote assaults that target devices and infrastructure utilized in cyber business processes (Mbelli & Dwolatzky, 2016, Nam, 2019). The more advanced that technology becomes, the greater the risk of cyber-threats (Lee, 2020). Commercial banks and their customers are still vulnerable to threats generated by the usage of mobile banking services despite various efforts made.

Social engineering is one of the most serious challenges to commercial banks and mobile banking clients. Customers are frequently the weakest link in the security chain; they might be duped into divulging important information and credentials. The main reason can be the nature of commercial banks operations on a shared network, providing third-party access to their information and exposing them to greater cybersecurity threats. In mobile banking services, the presence of cybersecurity threat and privacy issues considering the magnitude of digital-related transaction has been a major factor which affects mobile banking customers' decision to use and retain the technology (Jibril *et al.,* 2020, Wazid *et al*., 2019).

Time, psychological, social, and privacy hazards are all examples of perceived dangers (Khedmatgozar & Shahnazi, 2018). The fewer users and potential users use technology, the higher the protective motivation toward the threat level (Jansen & van Schaik, 2018). This study hypothesizes that:

Hypothesis H1: Customers' understanding of cybersecurity threat drives them to use mobile banking services.

Perceived susceptibility

Perceived susceptibility or vulnerability refers to how vulnerable one believes they are to the potential circumstance being presented. It instills fear in the respondent and attempts to convince or influence them by threatening a negative or frightening outcome if they do not take the advised action (Lawson *et al.,* 2016). Adoption of mobile banking services can be regarded as increasing opportunity from the possibility of being a victim of cybersecurity risks. Mobile banking costumer's protective behavior from susceptibility of cybersecurity risks leads to initiating a particular course of preventive behavior. Typically, mobile banking applications cause bank customers to worry about becoming a victim of cybercrime. As a result, many mobile banking customers still prefer to pay in hard cash to avoid becoming a victim of cybercrime incidences.

Supermarkets, gas stations, hotels, restaurants, and bars prefer payment through point of sale, and that allows mobile banking customers to pay bills through mobile applications or credit cards. However, the majority of customers still prefer to pay with cash rather than using mobile banking services, which may be related to a worry about becoming a victim of cybercrime. The lesser the use of mobile banking services, the higher the protective behavior on cybersecurity susceptibility in the form of a high degree of being affected by cyber-attacks (Marafon *et al.,* 2018). This study, therefore, hypothesizes that:

Hypothesis H2: Customers' susceptibility of cybersecurity motivates their usage of mobile banking services

Perceived severity

The degree of physical, psychological, economic, and social pain, as well as hazards to others rather than oneself, and even threats to other species, is referred to as severity. Perceived severity refers to an individual's estimate of the severity of the consequences of threats (Wu, 2020). These consequences may relate to an anticipated event that may occur in the future or such existing cybersecurity threats to a current state. In the context of the internet, perceived severity is also defined as the degree of harm in terms of loss or expense that can occur from security threats or cyber-attacks (Lawson *et al.,* 2016). Perceived severity of cyber threats usually determines the decision of mobile banking customers to use or not use the application. This is

why mobile banking customers can easily walk into a bank to obtain services that might have been obtained through the mobile banking application. In other words, mobile banking users may prefer to obtain bank services at a bank counter rather than via mobile banking.

From the mobile banking perspective, the magnitude of the perceived severity by customers triggers fear toward usage of mobile banking services (Alexandrou & Chen, 2019, Hajian *et al.,* 2015). Therefore, perceived severity can have high effect on the user's plan of actions and can influence their usage of mobile banking technologies (Kamdjoug *et al.,* 2021). The more serious a person takes the consequences of risky action, the more unfavorable his or her attitude toward it becomes (Lin & Bautista, 2016). As a result, this study tested the following hypothesis:

Hypothesis H3: Customers' protective behavior on cybersecurity severity motivates their usage of mobile banking services.

Perceived Data Confidentiality

Data confidentiality is defined as preventing inadvertent, unlawful, or unauthorized access, disclosure, or theft of data. Confidentiality refers to the privacy of data, as well as permissions to view, distribute, and utilize it (Shaju & Panchami, 2016). All contacts between trading parties are restricted to the parties involved in the transaction, according to confidentiality. Because hackers may gain access to sensitive information, confidentiality is extremely crucial in the e-commerce industry. Mobile banking customers are very sensitive to their financial data confidentiality, and their biggest fear is to be contacted by a third party. Their perception on using mobile banking is attached to higher probability of these data to be snatched through hacking while using a mobile banking application. This protective behavior motivates the decision to use or not use mobile banking service.

In mobile banking, customers use digital devices to carry out various services such as account balance enquiry, funds transfer, and bill payment, which raise data confidentiality risks. Data confidentiality is defined as whether data on a system is protected from unintentional or unauthorized access (Akinyede & Esese, 2017). One of the most critical issues banks confront while doing business in cyberspace is the safeguarding of consumer information (Mbelli & Dwolatzky, 2016). Cyber data being stolen or released to unauthorized persons can result in data confidentiality being lost (Bertino & Ferrari, 2018). As a result, desire to use technology is motivated by level of data confidentiality in mobile banking services (Akram *et al*, 2018).

Hypothesis H4: Customer usage of mobile banking services is motivated by data confidentiality.

Perceived data integrity

Perceived data integrity refers to the protection of data from unauthorized modification or manipulation. It means that unauthorized parties are unable to alter data in transit between two or three parties (Jibril *et al.,* 2020, Stewart & Jürjens, 2018). Therefore, information has value only when it is correct. Having this in mind, potential mobile banking users are skeptical of cybersecurity risks associated with mobile banking services, which consequently affects the overall rate of acceptance and adoption as expected in the business environment. Mobile banking consumers are wary of the risk connected with using the service because of the security of their financial data and information. This is why banks use a combination of authentication, encryption, and auditing procedures to ensure that the privacy, confidentiality, and integrity of transactions and information received, disclosed, shared and kept, or used in online banking systems are protected (Normalini *et al.,* 2019).

However, hackers also work around the clock to break into people's systems and access sensitive information that may jeopardize one's position through financial loss or other damages. Despite efforts to develop technical tools like cryptography, there is still a noticeable number of incidences related to compromised data integrity of mobile banking customers, which ultimately affects usage of mobile banking services (Eastin *et al.,* 2016). Customers who use mobile banking require assurance that their information will stay accurate, unaltered, and secure while in transit and stored on applications (Wazid *et al.,* 2019). The confidence in the data integrity of mobile banking customers will create confidence for mobile banking service and hence motivate them towards usage of technology. Thus, this study proposes that:

Hypothesis H5: Data integrity motivates customer's usage of mobile banking services

Coping Appraisal

Perceived Self-efficacy

People's perceptions about their capacities to create specified levels of performance that exert influence over events that affect their lives are defined as perceived self-efficacy (Lin & Bautista, 2016). Consumers' confidence in implementing an invention is also referred to as perceived self-efficacy (Koksal, 2016). It can also be defined as a determination of

one's capacity to employ a specific technology to complete a task (Makanyeza, 2017). Before using a mobile banking application, bank customers usually conduct a self-assessment and skill audit in using the technology efficiently. The level of knowledge and experience on using mobile banking will determine the decision of mobile banking customers to use or not use the services.

This design is important to examine in mobile banking services since it requires a bank customer to undertake and conduct financial transactions without the assistance of a bank employee (Alalwan *et al*., 2015). Studies conducted in Zimbabwe and Jordan found a positive correlation between technology experience and actual mobile banking usage (Cudjoe *et al.,* 2015; Abayomi *et al.,* 2019). Self-efficacy, on the other hand, can affect more than only people's attitudes toward using mobile services. If social pressure to use the service proves to be a significant factor in differentiating themselves from others, customers will use mobile banking services (Singh *et al*., 2018, Salum, 2020). On this note, this study hypothesizes that;

Hypothesis H6: Customer self-efficacy on cybersecurity risks motivate their usage of mobile banking services

Cybersecurity awareness

End-user awareness of cybersecurity threats, risks they introduce, and mitigating security best practices to influence their behavior is referred to as cybersecurity awareness. Cybersecurity awareness advocates for users of technology to be aware of the hazards and consequences of their actions. Mobile banking customers are afraid of cybersecurity scams such as theft through social engineering which comes through various approach including short messages, phone calls, and emails. The bank customers who have wide cybersecurity awareness are more likely to use mobile banking services than the ones with no awareness.

Mobile banking customers become victims of well-organized scammers through mobile banking platforms. A study by Alotaibi *et al.,* (2016) found that, although costumers can have good knowledge of mobile banking technologies, most had limited awareness of cybersecurity risks. The more knowledgeable technology users are about cybersecurity, the more likely they are to want to use mobile banking (Li *et al.,* 2016, Kessy, 2021). Cybersecurity awareness tends to positively impact the usage of technology (Korpela, 2015). On this note, this study hypothesizes that;

Hypothesis H7: Customer understanding of cybersecurity risks motivate their use of mobile banking services.

Theoretical Framework

Fig 1. Presents the conceptual framework that describes the relationship between dependent and independent variables as modified from PMT. The dependent variable, which is the protective behavior on usage of mobile banking services by customers depends on cybersecurity threat appraisal and coping appraisal (independent variables). Cybersecurity threat appraisal consists of perceived threat, severity, susceptibility, data confidentiality and data integrity, whereas coping appraisal consists of self-efficacy and cybersecurity awareness.

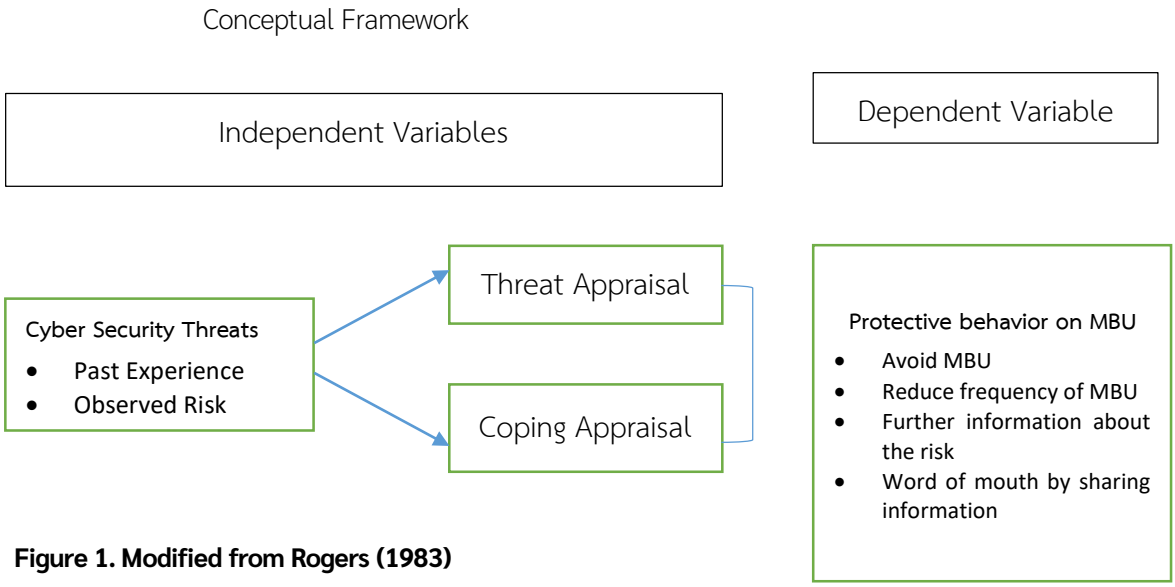

Figure 1. Modified from Rogers (1983)

3. Methods

This study employed a mixed-method approach in which both quantitative and qualitative were collected. The quantitative approach was used for the overall operationalization of the study whereas the qualitative part was intended to validate and elaborate on the former. This was a cross-sectional research in which data were collected at a particular point in time. A survey strategy was also employed, which is typically connected with the deductive approach and allows for the collecting of large amounts of data from a big population in a cost-effective manner (Saunders *et al.,* 2012). Data was mainly obtained by using a questionnaire and key informants open ended questionnaire.

The study employed a closed-ended questionnaire for data collection. The questionnaire items were developed by the researchers based on previous research. Moreover, the questionnaire

was pre-tested on 30 respondents. Measuring instruments' reliability and validity were also evaluated. According to Si Dah et al. (2022), it is crucial to comprehend that the validity of an instrument refers to how well it measures the researcher's conceptual framework or hypothesis. Limna *et al.,* 2023). The main variables in this study were evaluated using a five-point Likert Rating Scale with the following classifications: strongly agree with a value of 5, agree with a value of 4, neutral with a value of 3, disagree with a value of 2, and strongly disagree with a value of 1.

The study was conducted in Dar es Salaam city because of being the capital business city with 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). Financial inclusion statistics show that more than 73% of individuals in the city have access to formal financial services of which 40% of these individuals use bank services (Fin Scope, 2017). The Cochran (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.

$$n_0 = \frac{Z^2 pq}{e^2} = \frac{(1.96)^2 x 0.5 x 0.5}{0.05^2} = 384\ respondents$$

where *n* is the sample size, *z* is the selected critical value of 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 10 commercial banks for the study. Convenience sampling was employed to obtain 478 commercial mobile banking users as respondents. A convenience sample is a non-probability sampling method that takes a sample from a group of people who are easy to contact or reach. Participants in this study were customers of one of the following banks: National Microfinance Bank (NMB), CRDB, Kenya Commercial Bank (KCB), National Bank of Commerce (NBC), Diamond Trust Bank (DTB), Azania Bank, First National Bank Tanzania (FNBT), Tanzania Postal Bank (TPB) (now Tanzania Commercial Bank (TCB), Stanbic and Equity Bank. The selection of these banks was based on their number of branches countrywide, level of information technology development, number of customers, and number of years in operations. The number of respondents reached during data collection was higher than 384. This is because, firstly, more data are more preferable as it improves the decision to be more accurate and the error of the parameter estimate will be minimized. Secondly, the acceptable range of sample size when using Structural Equation Model (SEM) is between 200 and 500 as recommended by Hair *et a,* (2019). Twenty key informants were specifically chosen

and supplied with open-ended questionnaires based on their knowledge and understanding of cybersecurity risks concerns and use of mobile banking services.

Partial least squares structural equation modeling (PLS-SEM) was used to gauge bank clients' protective behavior on cybersecurity risk and usage of mobile banking services. PLS-SEM is a statistical technique that allows researchers to test and estimate predicted associations in a conceptual model at the same time, allowing them to determine probable correlations between dependent and independent variables. Mobile banking usage was investigated using confirmatory factor analysis (CFA), which assessed the overall validity of the measures to see if the constructs (perceived threat, severity, susceptibility, data confidentiality, integrity, perceived self-efficacy, and cybersecurity awareness) fit the data set. Because the research goal is to predict and explain the variance of dependent variables as explained by distinct independent factors, PLS-SEM was deemed appropriate.

Qualitative data were processed using thematic analysis as adopted and improved from Salleh *et al.* (2017). This involved reading transcripts and interviews from key informants and then coding manually. Sorting the coded information followed to define potential themes and sub-themes based on importance, relevance, and relation to the theory and objectives of the study.

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 is acceptable (Nyongesa *et al*., 2020). The results demonstrate that all of the items were significant. All factors passed the test, according to the results (see Table 1).

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

Aspects	Items	Loadings	VIF	CR	AVE
MB Usage	MBU1	0.913	2.001	0.864	0.682
	MBU2	0.856	1.875		
	MBU3	0.700	1.329		
Perceived Self-Efficacy	PSE1	0.855	1.484	0.842	0.641
	PSE2	0.818	1.488		
	PSE3	0.723	1.332		
Perceived Threat	PT1	0.857	1.272	0.794	0.597
	PT2	0.714	1.228		
	PT3	0.700	1.292		
	PT4	0.724	1.506		
Perceived Severity	PSV1	0.757	1.203	0.840	0.637
	PSV2	0.809	1.723		
	PSV3	0.826	1.706		
Perceived Susceptibility	PSC1	0.781	1.854	0.834	0.502
	PSC2	0.700	1.975		
	PSC3	0.701	1.885		
	PSC4	0.700	1.809		
	PSC5	0.711	1.578		
Security Awareness	SA1	0.719	1.252	0.804	0.577
	SA2	0.787	1.300		
	SA3	0.771	1.210		
Perceived Confidentiality	PC1	0.739	1.361	0.809	0.514
	PC2	0.730	1.264		
	PC3	0.700	1.249		
	PC4	0.705	1.347		
Perceived Integrity	PI1	0.812	1.402	0.832	0.501
	PI2	0.775	1.434		
	PI3	0.776	1.665		
	PI4	0.810	1.814		
	PI5	0.713	1.298		

Source: Data from Field (2021)

Discriminant Validity test

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

Table 2. Discriminant Validity (Fornell-Larcker Criterion)

	MBU	PSE	PT	PSV	PSC	SA	PC	PI
MBU	0.826							
PSE	0.441	0.801						
PT	0.842	0.623	0.705					
PSV	0.475	0.541	0.669	0.798				
PSC	0.523	0.824	0.720	0.793	0.709			
CSA	0.543	0.475	0.603	0.550	0.588	0.760		
PC	0.540	0.504	0.610	0.457	0.558	0.629	0.717	
PI	0.535	0.457	0.612	0.547	0.565	0.631	0.596	0.708

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)

Findings

This section presents findings from a questionnaire-based survey and key informant interviews (KII). Data from the questionnaires were largely quantitative and are presented in graphic and tabular forms, whereas data from KII were qualitative and are presented in descriptive form. The section also presents the discussion and interpretation of these findings.

Hypothesis testing and path coefficient analysis were used to answer the study's research topic. To examine the link between the construct elements, Smart PLS –SEM software was used to compute structural equation modeling (SEM) procedures employing path analysis and partial least squared estimates. The necessary association is specifically between cybersecurity

protective behavior and mobile banking service usage. To assess how cybersecurity affects mobile banking consumers' use of mobile banking services, two criteria were investigated: cybersecurity risk and coping appraisal as shown in Figure 2.

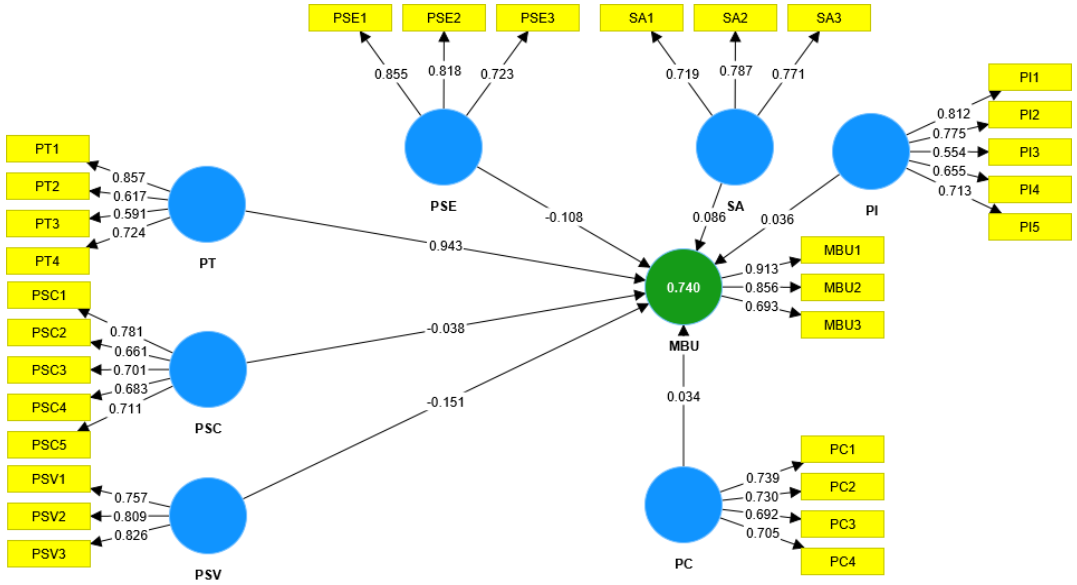

Figure 2: Cybersecurity threat and Coping Appraisal Coefficient Path Analysis

SRMR=0.102611055, d_ULS=4.895998296, d_G=0.538643, chi Square=408.0775588, NFI=0.510862912

Table 4: Partial Least Square results

	$R^2 = 0.740$			
Hypothesized path	Path Coef	t	p - value	Remark
H1: PT -> MBU	0.943	13.994	0.000	Significant
H2: PSC -> MBU	-0.038	1.814	0.070	Not significant
H3: PSV -> MBU	-0.151	2.777	0.006	Significant
H4: PC -> MBU	0.034	0.626	0.032	Significant
H5: PI -> MBU	0.036	0.736	0.623	Not significant
H6: PSE -> MBU	-0.108	3.514	0.008	Significant
H7: SA -> MBU	0.086	1.783	0.002	Significant

Source: Data from Field (2020)

The findings in Table 4 indicate that perceived threat (PT) ($\beta = 0.943$, $p < 0.01$), perceived confidentiality (PC) ($\beta = 0.034$, $p < 0.05$), security awareness (SA) ($\beta = 0.086$, $p < 0.01$) and perceived self-efficacy(PSE) ($\beta = -0.108$, $p < 0.01$) have positive significant effects on mobile banking services usage. However, perceived severity ($\beta = -0.151$, $p < 0.01$) has a negative significant effect on mobile banking services usage. Perceived susceptibility and perceived integrity have no significant effects toward usage of mobile banking services. Therefore, these findings indicate that perceived cybersecurity risks influence customers' decisions to use mobile banking services. Overall, the findings indicate that nearly three-quarters ($R^2 = 74\%$) of the variance in mobile banking services usage was explained by these factors.

Discussions

Perceived threat and mobile banking services usage

The findings indicate that using mobile banking services is positively and significantly impacted by customers' protective behavior in light of their awareness of cybersecurity threats. The respondents who were questioned and provided their responses were aware of potential cybersecurity issues in advance prior to adopting and using mobile banking services. Because of this, the results show that users of mobile banking platforms, services, and applications are more likely to be informed about cybersecurity. This result is also consistent with the study by (Nam, 2019; Zwilling *et al.,* 2022). That study found that perceived threat, preparation, and understanding of cybersecurity issues boosts confidence in using online services. When asked to name reasons for using mobile banking services, the KII revealed that security, dependability of services, service accuracy, and awareness of the service are some of the reasons. Those findings are in line with several ongoing corrective actions conducted by government entities such as TCRA, TPF, e-Government, Judiciary, BOT, and relevant banks to secure cyberspace. Development of a legislative framework, safe ICT infrastructure, cybersecurity awareness, regulating and enforcing cyber-related offenses are all part of the massive effort.

Perceived confidentiality and mobile banking services usage

The findings indicate that mobile banking clients place a high level of trust in their commercial banks' handling of financial information confidentially. In Tanzania, all banks are required to follow BOT legislation, frameworks, and standards in order to guarantee that their ICT systems and infrastructure are secure and well-managed. During an interview with a key informant from the BOT's directorate of banking and financial supervision, he indicated that all banks are

audited using a physical security checklist that includes information, personnel, and asset security.

This security preparation of banks builds banks customers' faith in the confidentiality of their financial data, which, in turn, favorably promotes their use of mobile banking services. Furthermore, these findings imply that data confidentiality is a critical consideration for mobile banking service users, as a compromise of personal information, might result in large losses. This is in line with a study by Lim *et al*., (2019), who stated that security protection of personal information and privacy in financial transactions is a critical prerequisite for extending the desire to use mobile banking services. This conclusion is supported by mobile banking service providers' current innovations, which include investments in a variety of security technologies and initiatives in order to develop trust with future and present mobile banking consumers regarding the protection of their personal information.

Cybersecurity awareness raises mobile banking services usage.

In this study, cybersecurity awareness refers to knowing what cyber dangers are and the possible impact a cyber-attack will have on mobile banking consumers. The findings show that customers' knowledge and awareness of cybersecurity will encourage them to use mobile banking applications, platforms, and services more frequently.

A key informant from the Tanzania Police Force stated that the vast majority of reported financial cybercrime incidents include social engineering of mobile banking users. That is why TPF and TCRA collaborated to raise awareness about cybersecurity tips such as sim card registration, PIN number management, password management, and scams via SMS and mailing. In Hungary and Vietnam, Mai and Tick, (2021) discovered that the threat of cybersecurity prompted a desire to learn more about cybersecurity. Tanzania is also dealing with cybersecurity concerns such as SMS scams and information phishing via mobile phones affecting mobile banking consumers. Commercial banks are also developing cybersecurity policies, educating their workers, and planning and outsourcing cybersecurity specialists, among other measures. During an interview with a key informant from BOT's directorate of banking and financial supervision about what is done to raise cybersecurity awareness among bank employees, he stated that BOT holds cybersecurity and fraud prevention training for banking institutions twice a year.

Perceptions self-efficacy and mobile banking services usage.

The results reveal that a causal relationship exists between perceived self-efficacy on cybersecurity risks and mobile banking service utilization, as the levels of customer's self-efficacy on cybersecurity may lead to reduced mobile banking services usage. This means that mobile banking customers will not use the services and platform if they are unsure of their knowledge and skill in using the services. When asked what factors impact the use of mobile banking services, key informants mentioned time efficiency, cost effectiveness, accuracy, dependability, emergencies, and avoiding lines at the bank. Those findings are consistent with those of (Foroughi *et al*., (2019), Makayenza (2017), Abayoni *et al*., 2019), who identified self-efficacy as a key factor influencing mobile banking usage in developing countries. These findings may be the result of commercial banks, TPF, and TCRA continuing to disseminate, sensitize, and alert customers about cybersecurity dangers to mobile banking clients.

Perceived Severity of Mobile Banking Services and their Use

The finding suggests that bank customers, usage mobile banking services decline as the levels of perceived severity or risky increases. This may be due to unawareness of the security severity or risks connected with the platform and the possibility of becoming a victim of a cyber-attack. "The decision for using mobile banking can be facilitated by other factors such as availability physical banks as banks are not well distributed particularly in remote areas, then application of mobile banking's remain to be the only option," (key informant from Exim Bank).

A study by Wang *et al*. (2016), found that when utilizing mobile banking, people place a higher priority on prospective rewards than on potential risks or severity. This is why, in order to close the financial inclusion gap, commercial banks encourage their consumers to use mobile banking and receive bank services anywhere and at any time. Mobile banking is also becoming increasingly useful, advantageous, and cost-effective as the number of online stores and e-businesses grows. If users are aware of security concerns and follow security guidelines supplied by banks, there will be minimal cybersecurity risks on the present mobile application platform. TCRA and the police force, on the other hand, employ social engineering to raise knowledge about current security dangers while utilizing mobile banking services.

Theoretical, Research and Policy Implications of the Study

The study's findings urge further investigation into the motivations for bank customers to protect themselves from cybersecurity dangers, as well as the development of pertinent

theories and frameworks. To better understand the intricate relationships between bank customers' protective motivations for cybersecurity and use of mobile banking services, it is methodologically required to use a mixed-methods design. To be in line with national ICT Policy and Strategy, policy actions are required to raise social engineering and cybersecurity awareness. The study's findings are consistent with PMT since five of the seven components obtained from risk and coping appraisals were found to influence mobile banking usage. The perceived threat, severity, confidentiality, self-efficacy, and cybersecurity awareness of mobile banking clients influence their use of mobile banking services. This finding suggests that PMT is the optimal theory for studying cybersecurity and commercial mobile banking clients' perceptions of the services.

This study had some limitations, including the inability to generalize to different types of online banking channels, such as internet banking and telebanking. There are however other aspects that have been overlooked and could be the subject of future research, such as financial constraints, trust, and habits. However, because this study was conducted in Tanzania, the generalizability of the current findings is limited. Future research could benefit from comparative studies that take into account technological, cultural, and human variations between developed and developing nations. Finally, while this study focused on mobile banking customers' protection motivation of cybersecurity and usage of mobile banking, other factors such as customer happiness, word-of-mouth, and customer loyalty can influence usage of mobile banking services. The practical benefit is that mobile banking application service providers may better understand the impact of cybersecurity concerns about mobile banking usage, allowing them to plan and implement strategies to better serve and attract more clients.

Conclusions and Recommendations

Conclusions

This study looked at how mobile banking users behaved in terms of cybersecurity and usage. The study comes to the conclusion that users' protective behavior when using mobile banking services depends on how seriously they take the cybersecurity threat and compliance assessments, and that users' decisions to use mobile banking services are influenced by how seriously they take cybersecurity concerns. Knowing how much of an impact this has on how people use mobile banking applications can help banks increase their understanding of cybersecurity in those areas. On the other hand, by creating regulations, strategies, and providing accurate information regarding cybersecurity in mobile banking services, policymakers, law

enforcement officials, and service providers can generate confidence. Perceptions of data confidentiality can influence how data protection laws are developed for mobile banking, and guarantee that customers are aware of data security.

Recommendations

Commercial banks and other cyberspace security organizations should focus on developing skills and knowledge on cybersecurity awareness for mobile banking consumers through social engineering. The findings from this study suggest that banks to construct a secure mobile banking platform, which will aid in the development of confidence among bank clients who might benefit from electronic banking services. Banks should continue to provide cybersecurity awareness for their consumers, especially now that cyberspace scams are on the rise. The findings from this study suggest that the unproven hypotheses be investigated further. It is proposed that more research be done to find out why perceived susceptibility and perceived integrity had no effect on the intention to utilize mobile banking services.

It is also suggested that banks prioritize customer care by using social engineering to increase self-efficacy in mobile banking services. The willingness to employ mobile banking technology is influenced by the perceived ability to take recommended security precautions. The study also suggests that policymakers, law enforcement, regulators, and banks increase their cybersecurity awareness as a factor in retaining mobile banking consumers. Meanwhile, mobile service providers should reduce the perceived seriousness of a data breach involving consumers' personal information. Users will be less likely to share personal information if they believe their data is being misused by mobile service providers

Conflict of Interest

The Author declares that there is no conflict of Interest

References

Abdullah, F., & Ward, R. (2016). Developing a general extended technology acceptance model for e-learning (GETAMEL) by analysing commonly used external factors. *Computers in Human Behaviour,* 56, 238 – 256.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016, December). A survey of cyber-security awareness in Saudi Arabia. In 2016 International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 154-158). IEEE.

Awan, J. H., Memon, S., Khan, R. A., Noonari, A. Q., Hussain, Z., & Usman, M. (2017). Security strategies to overcome cyber measures, factors and barriers. *Eng. Sci. Technol. Int. Res. J, 1*(1), 51-58.

Alexandrou, Alex, and Li-Chiou Chen. (2019): "A security risk perception model for the adoption of mobile devices in the healthcare industry." *Security Journal, 32*(4), 410-434.

Akinyede, R. O., & Esese, O. A. (2017). Development of a secure mobile e-banking system. *International Journal of Computer* (IJC), *26*(1), 23-42.

Bank of Tanzania. (2020). *The directory of Banks and Financial Institutions Operating in Tanzania*. Tanzania: Bank of Tanzania

Chawla, D., & Joshi, H. (2017). Consumer perspectives about mobile banking adoption in India–a cluster analysis. *International Journal of Bank Marketing*, *35*(4), 558-582.

Chang, S. H., Hsu, H. M., Li, Y., & Hsu, J. S. C. (2018). The influence of information security stress on security policy compliance: a protection motivation theory perspective. AIS Electronic Library (AISeL), Pacific Asia Conference on Information Systems (PACIS)

Choudrie, J., Junior, C. O., McKenna, B., & Richter, S. (2018). Understanding and conceptualizing the adoption, use and diffusion of mobile banking in older adults: A research agenda and conceptual framework. *Journal of Business Research, 88*, 449-465.

Cudjoe, A. G., Anim, P. A., & Nyanyofio, J. G. N. T. (2015). Determinants of mobile banking adoption in the Ghanaian banking industry: a case of access bank Ghana limited. *Journal of Computer and Communications, 3*(02), 11-18.

Dijkstra, T.K. and Henseler, J. (2015), "Consistent partial least squares path modeling", *MIS Quarterly 39*(2), 297-316.

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.

Fin Scope Tanzania. (2017), *Insights that drive innovations*. Tanzania: Mimeo.

Foroughi, B., Iranmanesh, M., & Hyun, S. S. (2019). Understanding the determinants of mobile banking continuance usage intention. *Journal of Enterprise Information Management, 32*(6), 1015-1033

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior,* 58, 214-220.

Hajian, S., Shariati, M., Mirzaii Najmabadi, K., Yunesian, M., & Ajami, M. I. (2015). Use of the Extended Parallel Process Model (EPPM) to Predict Iranian Women's Intention for Vaginal Delivery. *Journal of Transcultural Nursing, 26*(3), 234-243.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, *31*(1), 2-24.

He, W., Tian, X., & Shen, J. (2015). Examining Security Risks of Mobile Banking Applications through Blog Mining. *Computers in Human Behavior*, *31*, 103-108.

Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. Computers in Human Behavior, Vol. 87, 371-383.

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. *In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270)*. Academic Conferences and publishing limited.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior*, *79*, 111-122.

Kamdjoug, J. R. K., Wamba-Taguimdje, S. L., Wamba, S. F., & Kake, I. B. E. (2021). Determining factors and impacts of the intention to adopt mobile banking app in Cameroon: Case of SARA by afriland First Bank. *Journal of Retailing and Consumer Service, 61*, 102-509.

Khedmatgozar, H. R., & Shahnazi, A. (2018). The role of dimensions of perceived risk in adoption of corporate internet banking by customers in Iran. *Electronic Commerce Research, 18*(2), 389-412.

Kessy, S. S. (2021). Adoption of Internet Banking Service in Tanzania. *University of Dar es Salaam Library Journal, 16*(1), 84-97.

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.

Lin, T. T., & Bautista, J. R. (2016). Predicting intention to take protective measures during haze: The roles of efficacy, threat, media trust, and affective attitude. *Journal of health communication*, *21*(7), 790-799.

Limna, P., Kraiwanit, T., Siripipattanakul, S., Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research, 7*, 1133-1151.

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In International Conference on Cyber Conflict 8: 65-80.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung 18*, 67-89.

Marafon, D.L., Basso, K., Espartel, L.B., de Barcellos, M.D. and Rech, E. (2018), "Perceived risk and intention to use internet banking: The effects of self-confidence and risk acceptance", *International Journal of Bank Marketing, 36*(2), 277-289.

Makanyeza, C. (2017). Determinants of consumers' intention to adopt mobile banking services in Zimbabwe. *International Journal of Bank Marketing, 35*(6), 997-1017.

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.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203-1230.

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* Vol 59, 101-151.

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 5th International Conference on Information Society and Technology, ICIST2015*. pp. 273-278

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*,7(3), 135-142.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society*, *58*, 101-122.

Nambiro, A., Wabwoba, F., & Wasike, J. (2020). Cyber security challenges to mobile banking in SACCOs in Kenya. *International Journal of Computer* (IJC), *27*(1), 133-140

Normalini, M. K., Ramayah, T., & Shabbir, M. S. (2019). Investigating the impact of security factors in E-business and internet banking usage intention among Malaysians. *Industrial Engineering & Management Systems, 18*(3), 501-510

Nyongesa, M. K., Mwangi, P., Koot, H. M., Cuijpers, P., Newton, C. R., & Abubakar, A. (2020). The reliability, validity and factorial structure of the Swahili version of the 7-item generalized anxiety disorder scale (GAD-7) among adults living with HIV from Kilifi, Kenya. Annals of general psychiatry, *19*(1), 1-10.

Rahi, S., Ghani, M. A., & Ngah, A. H. (2020). Factors propelling the adoption of internet banking: the role of e-customer service, website design, brand image and customer satisfaction. *International Journal of Business Information Systems*, *33*(4), 549-569.

Salim, A. M. (2020). Exploring Customers' Perception on Adoption and Use of Electronic Banking Services in Tanzania Commercial Banks. *International Journal of Innovation and Applied Studies, 30*(2), 477-486.

Semboja, H. H., Silla, B. S., & Musuguri, J. N. (2017). Cyber Security Institutional Framework in Tanzania: A policy Analysis. Gsj 5(6), 13-28

Serianu. (2017). Tanzania cyber security report 2017: Demystifying Africa's cyber security poverty line. Retrieved from www.serianu.com/downloads/TanzaniaCyberSecurityReport2017. pdf

Shaju, S., & Panchami, V. (2016). BISC authentication algorithm: An efficient new authentication algorithm using three factor authentications for mobile banking. In 2016 Online *International Conference on Green Engineering and Technologies (IC-GET)*: IEEE. pp. 1-5.

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

Si Dah, N., Siripipatthanakul, S., Phayaphrom, B., & Limna, P. (2022). Determinants of Employee Innovation: A Case of NGOs and CSOs in Mae Sot, Thai-Myanmar Border. *International Journal of Behavioral Analytics, 2*(1), 1-15.

Stewart, H. and Jürjens, J. (2018), "Data security and consumer trust in Fin Tech innovation in Germany", *Information and Computer Security, 26*(1), 109-128.

Tanzania Banking Overview Sector, Review report of 2020. Bank of Tanzania

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce, 23*(2), 1-11.

Towbin, R. S. (2019). A protection motivation theory approach to healthcare cybersecurity: A multiple case study (Doctoral dissertation, Northcentral University). Performance: The Case of Europe. Procedia. *Social and Behavioral Sciences,* Vol 195, 363–368.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: *A protection motivation theory perspective. Computers & Security, Vol* 59, 138-150.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security,* 77, 860-870.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management, 36*(4), 531-542.

Wambalaba, F., Musuva, P., Ouma, M. J., & Nicos, K. (2021). *Cybersecurity Risk Minimization Best Practices-African Experiences, 1*, 1-42

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.

Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. *Trends and Issues in Crime and Criminal Justice,* Vol. *592*, 1-18.

Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior, 105*, 106-229.

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.