Influence of Protection Motivation Theory on Information Security Practices: The Case of Ghanaian Mobile Banking Merchants

P. Danquah, H.A. Matey & K. Asiamah
(pauldanquah@yahoo.com; henraclesgh@hotmail.com; asiamahkenneth7@gmail.com)

Abstract

The mobile banking industry has grown to become Ghana's most popular digital financial service (DFS). Since its inception in 2018, the first interoperable system in Africa has allowed transactions between Ghana's various telecommunication companies and banks. Today, the mobile banking and financial services sectors have seen immense turmoil, including cybercrime on mobile banking transactions. It generally involves the manipulation of customers' accounts without authorization, prompts sent under the pretext of a telco promotion, fake SMS sent to indicate a deposit into a customer's account, and fraudsters posing as delivery companies instructing customers to deposit to a mobile banking account in exchange for delivering goods. This study premises to determine how applicable Protection Motivation Theory (PMT) is to explaining mobile banking-related cybercrime. Therefore, this work seeks to analyze mobile banking merchants' attitudes and intentions to secure transaction-related data in light of mobile banking services in Ghana. Finally, this study empirically tests the theoretical model with a data set representing the survey and the responses of 410 mobile banking merchants in the greater Accra region of Ghana. Partial least squares structural equation models (PLS-SEM) are used in analyzing the data since the method facilitates assessing patterns of causation of target constructs in the proposed model. The study results suggest that the perceived probability of Vulnerability was not a significant predictor of Intention to secure information or Attitude toward securing information. The perceived severity of the threat also has a positive relationship with the Attitude toward securing information but is not significant. Perceived self-efficacy has a negative relationship with the Intention to secure information but is not significant. The most vital relationship emerged where the perceived severity of the threat significantly predicted the Intention to secure information. Perceived response efficacy significantly predicted Intention to secure information and positively predicted Attitude toward securing information. Finally, the results also indicated that perceived self-efficacy significantly impacted attitudes toward securing information.

Keywords: Information Security Practice, Protection Motivation Theory (PMT), Mobile Banking, Threat and Coping Appraisal, Mobile Money

ISSN: 3057-3610

Introduction

Mobile banking is "the type of delivery of financial services that involve the use of mobile communication techniques and mobile devices by the consumer" (Baratti & Mohammandi, 2009). Mobile banking liberates users from spatial and temporal restrictions and permits them to execute distant payments. Mobile banking is a service provided by a bank, licensed individual or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. In this study, the emphasis was on collecting data from licensed individual mobile banking merchants (Brook, 2017). The telecommunications company with the highest market share in Ghana's commission explained mobile banking merchants as "When we say MTN mobile money merchants, we refer to the persons available to offer mobile money services (withdrawals and deposits) using MTN mobile money platforms. These persons are mostly seen in stores, kiosks and others. One notable thing used to identify these persons is their MTN mobile money stickers"(MTN Commission, 2023). This service offers users, particularly those without bank accounts, a great deal of convenience. The services of mobile banking merchants, who act as intermediaries between telecommunication operators and end users, have proven indispensable to the utilization of this service. The mobile banking merchant service facilitates the transmission of payments from Customers to the merchant's mobile money account via transactions initiated by registered Customers on their mobile devices. In Ghana, telecommunications companies such as MTN Ghana, Vodafone, and AirtelTigo offer mobile money services. In January 2021, the Bank of Ghana reported that cleared checks for mobile money transactions totalled $2.82 billion. According to the Bank of Ghana, there were 40.9 million registered mobile money accounts and 17.5 million active accounts in 2021. (Mobile Money Report, 2022). According to the International Finance Corporation, Ghana has Africa's fastest-growing mobile money market. Since the inception of the Mobile Money programme in 2009, the number of registered agents reached 9.1 million by December 2020. (State of the Industry Report, 2020). This study aims to analyze merchants' attitudes and intentions about the security of transaction-related data in light of the spread of mobile banking in Ghana. Using the Protection Motivation Theory (PMT), some research has been conducted to ascertain the causes of information security policy violations, with recommendations for improved compliance. Inconspicuously lacking from research results is a focus on mobile banking merchants, who are often outside a corporate context and are, therefore, not limited by the constraints of a particular policy or legislation. This study's primary purpose is to evaluate the information security practices of mobile banking merchants to identify the extent of the protection motivation theory's influence on merchants' attitudes toward securing information and intent to secure it. The paper begins with model development and formulation of hypotheses on the protection motive theory, mobile money merchants, users, and its associated security challenges, followed by a concise description of the methodology employed in this study. The following part describes the findings of the data gathering, their consequences, and the ultimate conclusions.

Protection Motivation Theory and Related Literature

Protection motivation theory (PMT) (Rogers, 1975) is regarded as one of the essential explanatory theories for predicting an individual's protective intentions and behaviours (Anderson & Agarwal, 2010). Determining a person's behavioural expectations is positively related to their motivation to protect themselves when they feel threatened in dangerous situations (Mohamed & Ahmad, 2012). The protection motivation theory of Rogers (1975) explains that individuals protect themselves based on threat appraisal and coping evaluation. The threat assessment is the individual's evaluation of the likelihood of adverse outcomes posed by a threat (Workman et al., 2008). It consists of the perceived severity, which is the severity of the anticipated consequences of threats.

Additionally, the perceived Vulnerability derived from the assessment of the likelihood of threat events is factored into PMT's risk assessment. "In PMT, perceived severity and perceived vulnerability are crucial in motivating individuals to adopt adaptive behaviour for self-protection" (Rogers & Prentice-Dunn, 1997). The coping assessment evaluates an individual's capacity to deal with and avoid a threatening event (Lee, 2011;

ISSN: 3057-3610

Rogers, 1975). The evaluation of coping includes self-efficacy, response efficacy, and response cost. Self-efficacy is an individual's evaluation of his or her perceived capability to engage in adaptive behaviour in response to a threat. Response efficacy consists of the perceived advantages of coping behaviour and the anticipated outcome. Response cost refers to the potential expenses that the coping mechanism may incur. It may involve money, time, and labour hours. Rogers & Prentice-Dunn (1997) explained that protective motivations are positively associated with response efficacy and self-efficacy and negatively associated with response cost. Information security breaches are numerous, with the cyber-attacks component targeting mobile devices, bank accounts, connected vehicles and cyber-physical systems. "These attacks are becoming more complex and are raising safety problems when targeting the physical environment" (Nguyen, Herbert & Carpov, 2020). The research further suggests that an efficient way to protect against these attacks is by making several security actors collaborate in defining appropriate countermeasures. Literature related to privacy in recent years has highlighted the role of context and situation in individuals' privacy regulation. A typical example is the solution by Kester & Danquah (2012) which proposes the use of public keys to serve as a key for encryption and decryption as well as for authentication. "While most research is focused on understanding situational effects on self-disclosure, the role of situational factors in users' decision to consent for third-party access to information, a common practice with significant privacy implications, has been barely investigated" (Steinfeld, 2020).

Further to this study, it was concluded that due to confusing borders and uncertainties regarding natural uses of information, when it comes to consent for third-party access, predetermined attitudes and preferences are the main factors required for users' decisions to permit access to their information. Beyond the case of individuals are small businesses with challenging cyber security problems that make them particularly vulnerable to cyber-attack due to the often-valuable information they handle coupled with overworked and undertrained IT support. Imsand, Tucker, Paxton, and Graves's (2020)'s survey of cyber security practices in small businesses revealed that small businesses in this field are likely to engage in poor security practices arising from common cyber security misconceptions. This posture was confirmed Longe et al…(2012) and Danquah (2020) in assessing cybercriminal behavioural patterns, and it revealed that both victims and even law enforcement agencies were not very knowledgeable in relevant information security-related laws.

In Ghana, the context of the study, Acts 772 and 775, address Electronic Transactions and Electronic Communications, respectively, are very much relevant for any technology user in the information security space. Both Acts, effected in late 2008, indicate that much as the cybercrime laws are available, it has hardly been used to charge perpetrators. The police use the criminal code Act 29/60 of Ghana's Section 131 and its associated statutes. There is also Act 843, the Data Protection Act, which was approved and operationalized in 2012. In (Breitinger et al., 2020)'s survey on smartphone users' security choices, awareness, and education revealed that smartphones contain significant personal data.

Additionally, users were always in possession hence the possibility of tracking using GPS or WiFi tracking. The study findings showed that "most users have appropriate lock screen settings to protect their phones from physical access; however, they disregard other security best practices, e.g., not using a VPN when connecting to a public WiFi or turning off unused features (regardless of the level of expertise). Compared to desktop computers, smartphones are less secured and fewer third-party security products are installed" (Breitinger et al., 2020). In an attempt to identify factors that could influence smartphone security behaviour, the results showed that media influence, perceived ease of use, perceived usefulness, and self-efficacy are significant predictors of smartphone security behaviour (Masrek et al., 2017). Fielding (2020) also explained that the organizational insider threat has increased as working practices have evolved and new technologies have been adopted. Collaboration platforms, cloud services, smart devices and mobile apps represent varying forms of cyber risk. To tackle this effectively requires a mix of technical and process-driven measures. Liao and Shi (2017) confirmed this assertion in assessing web functionality, web content, information security, and online service continuance. Their results showed that "web functionality, web content, and information security

ISSN: 3057-3610

positively influence consumers' perceived value of online tourism services which significantly mediates the effects of these determinants on continuance intention to use online tourism services". According to Matey, Danquah, and Koi-Akrofi (2022), maintaining situational awareness at all times is a component that is equally as important as the other protection motivation factors; this is further confirmed by Asani et al. (2021) that security experts are caught up in a never-ending cycle which makes protection increasingly tricky.

Research Model and Hypotheses

The hypotheses were developed based on Rogers' (1975) protection motive theory, which posits that individuals protect themselves based on danger appraisal and coping evaluation. This was achieved by integrating variables such as the perceived probability of Vulnerability (PPOV), Perceived severity of the threat (PSOT), Perceived Response Efficacy (PRE), Perceived Self-Efficacy (PSE), Attitude toward securing information (ATWSI), and Intent to secure information (ITSI). Figure 1 depicts our research model and theorized hypotheses.

Intent to secure information (ITSI) is a goal or strategy for protecting sensitive, vital data (Bulgurcu et al., 2010; Wu, 2020). Figure 1 offers an overview of the conceptual model suggested and empirically tested in this work. The conceptual model is mostly based on the protection motivation theory (PMT), which has been empirically utilized to describe merchants' attitudes and purposes toward securing mobile banking transactions and user information. This study contributes to understanding the mediator between mobile banking merchants' Attitude toward information security and the output of the merchants' desire to secure information by extending the PMT theory. PMT theory has been extensively applied in past research (Huang et al., 2021; Kester et al., 2022; Luo et al., 2021; Xiao et al., 2018). This was done to investigate the influence of the Protection Motivation Theory on information security practices within the Ghanaian mobile banking industry, with an emphasis on merchants.

The perceived probability of Vulnerability (PPOV) refers to an individual's perception of a security vulnerability that may be susceptible to exploitation. Johnston and Warkentin (2010). According to previous studies, when people sense danger, it prompts them to modify their behaviour according to the level of risk involved and to evaluate whether or not they are willing to take that risk. (Workman et al., 2008). It explains that when individuals feel exposed to a condition, they are more apprehensive about coping in a "defensive avoidance" manner. The perceived probability of Vulnerability is positively associated with the individual's Attitude toward knowledge withholding (Wu, 2020). In a related study by (Luo et al., 2021), Attitude mediates self-efficacy and response efficacy; hence, the current study would like to establish the mediating role of Attitude. Prior research has identified a positive causal relationship between the perceived probability of Vulnerability and intent to secure information (Sharma & Aparicio, 2022; Tang et al., 2021).

Meanwhile, the study found no substantial relationship between perceived vulnerability and compliance intentions (Kimpe et al., 2021; Mwagwabi, 2015; Ooijen et al., 2022). Perceived Vulnerability of IS security threats is a significant determinant of adopting IS security innovations (Mumtaz & Arachchilage, 2019). We, therefore, hypothesize the following because we assume that mobile banking merchants that consider transaction vulnerabilities severe are more likely to participate in preventive actions concerning the transfer of funds from one mobile wallet to another. We, therefore, hypothesize that:

H1: The perceived probability of Vulnerability has a positive relationship with the Intention to secure information.

H1.1: Attitude toward securing information mediates the effect of the perceived probability of Vulnerability on the Intention to secure information

Perceived severity of the threat (PSOT) refers to the anticipated adverse impacts on the extent and relevance of a prospective external hazard (Sharma & Aparicio, 2022). Tang et al. (2021) also refer to it as the extent of the potential harm posed by specific threats. The threat severity reflects how users perceive the severity of a threat to themselves. Earlier research work has revealed that the perceived severity of a threat could significantly predict people's intentions to comply with information systems security policies (Vance et al., 2012). In a related

ISSN: 3057-3610

study by Ophoff & Lakay (2019), they reveal that perceived threat severity seems to have no direct influence on motivation to protect but does strongly influence fear as an emotional response. If an employee feels threatened by information security risks and has a firm knowledge of the appropriate response, he or she will have a higher level of information security compliance (Rajab & Eydgahi, 2019). Earlier studies also indicate that Perceived Severity influences information policy compliance (Hina et al., 2019); in addition, Attitude was also confirmed to positively influence the Intention to comply with Security Policies. Essentially, this study seeks to establish the mediating role of Attitude between the perceived severity of the threat and the intent to secure information. This study, therefore, hypothesizes that;

H2: Perceived severity of threat has a positive relationship with the Intention to secure information.

H2.1: Attitude toward securing information mediates the effect of the perceived severity of the threat on the Intention to secure information

Perceived Response Efficacy (PRE): This refers to a victim's anticipation of the results he or she will experience in the case of a security breach, Herath and Rao (2009). Prior research on the protection motivation theory suggests a positive relationship between response efficacy and intentions (Ifinedo, (2012); Tsai et al., 2016). Response efficacy is positively associated with individuals' intentions to employ security measures (Tang et al., 2021). Response efficacy has an impact on privacy-protective behaviour (Boerman et al., 2021). In a study by Mills & Sahi (2019), response efficacy was also found to significantly predict protection motivation intention; meanwhile, no such association was found between perceived response efficacy and individual Intention (Kimpe et al., 2021; Ophoff & Lakay, 2019). Individuals' intentions to comply with information security policy are positively correlated with their response efficacy if they feel vulnerable and threatened by security risks and have a strong command over their response course of action. (Rajab & Eydgahi, 2019). In the study by Herath & Rao (2009), it was also discovered that response efficacy significantly influenced attitudes towards responding to security regulations. Therefore, based on the nature of the current study, we hypothesize that;

H3: The perceived response efficacy has a positive relationship with the Intention to secure information.

H3.1 Attitude toward securing information mediates the effect of perceived response efficacy on Intention to secure information

Perceived Self-Efficacy (PSE): Perceived self-efficacy refers to the anticipated outcome of an individual's action in the event of a security breach. Herath and Rao (2009). There is a significant relationship between self-efficacy and motivation, with high self-efficacy enhancing the drive to complete the activity (Voica et al., 2020). Existing literature on the subject has explained that people are more inclined to do things that are less difficult for them or that they are confident of doing well (Bandura, 1977). Essentially, self-efficacy influences and affects people's effort and persistence when they are faced with challenges (Lin & Huang,2010). Recent studies tried to establish the relationship between self-efficacy and what motivates individuals' intentions to secure information (Kimpe et al., 2021; Luo et al., 2021); The likelihood of being a victim of instant message phishing has a positive relationship with self-efficacy (Lee et al., 2023). Self-efficacy has been extensively researched and identified to be a positive predictor of information security behaviour (Luo et al., 2021; Ooijen et al., 2022; Ophoff & Lakay, 2019; Tang et al., 2021). The study by Syed et al. (2019) reveals a positive association between self-efficacy and motivation to protect. It was also established that self-efficacy has an influence on the Intention to use extra security measures (Mills & Sahi, 2019). The Self-efficacy component highlights an individual's confidence in his or her capacity to carry out the specified conduct. In the framework of this study, we are looking at the capabilities and techniques required to secure information. Therefore, the study hypothesizes that;

H4: Perceived self-efficacy has a positive relationship with the Intention to secure information.

H4.1: Attitude toward securing information mediates the effect of perceived self-efficacy on the Intention to secure information

Attitude toward securing information (ATWSI): Attitude toward securing information has been explained as a consistent manner of thinking or acting about the protection of sensitive, critical data. Menard et al. (2018), (Sharma & Aparicio, 2022). Perceived advantages influence perceptions of attitudes and intentions toward

ISSN: 3057-3610

mobile wallet applications favourably (Bhatt et al., 2021). Additionally, prior studies found that Attitude can fully or partially moderate the influence of self-efficacy and the response efficacy of individual continuance intention in taking action (Luo et al., 2021). The current study seeks to investigate the mediating role of attitudes toward securing information by mobile money merchants. Earlier research has revealed that Attitude affects merchants' willingness to adopt mobile payments (Abebe, 2020). In a related study by Zainal et al. (2017), a relationship was also established between trust and behavioural Intention, which was found to be partially mediated by Attitude. Another study also found that Attitude has a mediating effect on users' intentions (Heny Sidanti et al., 2022). It is therefore understood that mobile money merchants' attitudes will serve as a mediating variable in their Intention to secure transaction information. Hence, we proposed the hypotheses below.

H5: Perceived Attitude toward securing information has a positive relationship with the Intention to secure information.

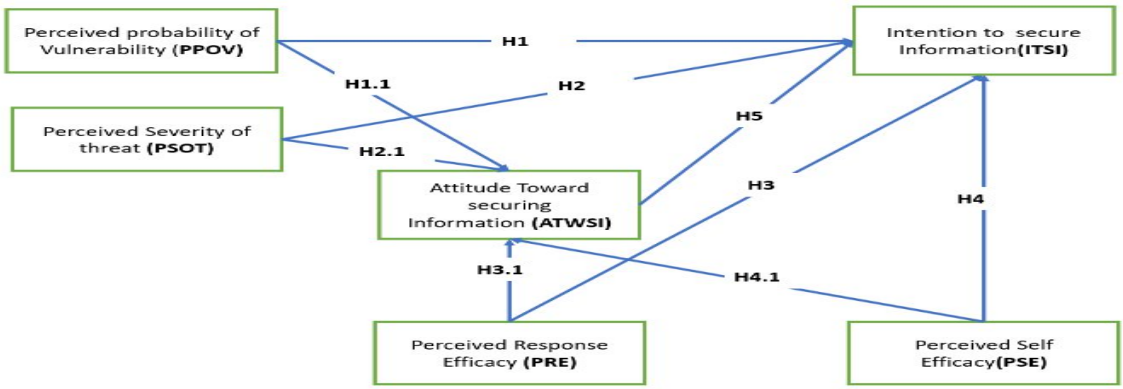

Figure 1 Conceptual Framework

The study applied the Protection Motivation Theory to develop an integrated framework to investigate the influence of the Protection Motivation Theory on information security practices within the Ghanaian mobile banking industry of Ghana with an emphasis on merchants. This is depicted in Figure 1, where the influence of constructs from the protection motivation theory, namely, the perceived probability of Vulnerability (PPOV), perceived severity of the threat (PSOT), perceived response efficacy (PRE) and perceived self-efficacy (PSE) are assessed. The assessment of these constructs is used to determine the influence on the subjects'(mobile banking merchants) Attitude toward securing information (ATWSI) and ultimately their intent to secure information (ITSI). The ATWSI is the mediating variable in this context, whereas the ITSI is the output. Figure 1, therefore, depicts the interrelationships among the outlined constructs. Extending the same reasoning, the researchers in this study hypothesize as detailed below;

H1: The perceived probability of Vulnerability has a positive relationship with the Intention to secure information.

H1.1: Attitude toward securing information mediates the effect of the perceived probability of Vulnerability on the Intention to secure information

H2: Perceived severity of threat has a positive relationship with the Intention to secure information.

ISSN: 3057-3610

H2.1: Attitude toward securing information mediates the effect of the perceived severity of the threat on the Intention to secure information

H3: The perceived response efficacy has a positive relationship with the Intention to secure information.

H3.1 Attitude toward securing information mediates the effect of perceived response efficacy on Intention to secure information

H4: Perceived self-efficacy has a positive relationship with the Intention to secure information.

H4.1: Attitude toward securing information mediates the effect of perceived self-efficacy on Intention to secure information

H5: perceived Attitude toward securing information has a positive relationship with the Intention to secure information.

Methodology

Research Design

According to Aspers & Corte (2019), quantitative research is "the collection of statistical data that are interpreted using numerically based procedures." The primary goal of quantitative research is to collect numerical data to analyze a phenomenon. Therefore, testing the validity of the proposed conceptual framework, a quantitative survey was carried out, with questions focusing on protection motivation theory which posits that individuals protect themselves. A quantitative research technique was used to obtain the relationships established in this study's proposed concept. Therefore, the study examines what motivates mobile banking merchants to protect their information assets. This research used five-point scales to depict the suggested constructs in the proposed frameworks. The measures used in the questionnaire were adopted from extant literature investigating issues related to the study's objectives.(Herath & Rao, 2009; Sharma & Aparicio, 2022; Xiao et al., 2018). The population of this study is general individuals mobile banking merchants in Accra, Ghana, as this study measures merchants' Intention to secure information. The data analysis is based on data collected from mobile banking merchants from the Greater Accra region in Ghana.

Instrumentation

An extensive literature review guides the researchers to address and define the proposed concepts related to the theoretical foundation of the research (Rogers, 1975). It further assists in developing instrumentation to address the research objectives(Habibi et al., 2020). The study, therefore, adapts survey instruments to access factors that motivate mobile banking merchants to protect information assets in their daily mobile banking transactions. The current instrument is based on the adaptation technique mentioned above; the indicators are unique since they were modified to meet the requirements of the inquiries on mobile banking merchants' security intentions. Twenty-eight (28) indicators were selected for the first implementation phase. The indicators were discussed through online meetings as part of the content validity process. Experts on the panel included personnel from both academia and industry. The team of reviewers consisted of two Researchers and cyber security experts to ensure the instrument's suitability. (Lynn, 1986). The revised questionnaire was reviewed to remove any further ambiguity. Field researchers pretested the tool in Achimota, a suburb within the region of Ghana, to eliminate ambiguity. After the instrument pretesting, data realized from 208 mobile money merchants were computed using Smart PLS software. The result calls for the removal of four (4) indicators because the loadings on these constructs were below the threshold of 0 .700 (Hair et al., 2019), leaving the total number of indicators at twenty-four (24) for the final data collection and analysis. Based on the above process, the final questionnaire was designed to collect responses from respondents. It constitutes six (6) constructs adapted from

ISSN: 3057-3610

existing literature and modified according to the context of the present study. Using a five-point Likert scale ranging from "strongly disagree" to "strongly agree," The respondents' anonymity was ensured to reduce social desirability biases. See Appendix 1 for measurement instrument and item source.

Data Collection

As indicated earlier, mobile banking is a service that could be provided by a bank, licensed individual or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. This study emphasized collecting data from licensed individual mobile banking merchants. The survey instrument was distributed through an online survey application for effective data collection. Using Google Form, an application developed by Google Inc., Field researchers were given a few hours of training on collecting data from these mobile banking merchants within the greater region using internet-enabled handheld devices. Field researchers spent about two and half months (Jan to March) in 2023 collecting the required data. According to the 2022 report of the Bank of Ghana (BOG), active mobile merchants within the country in 2021 is 442,375; random sampling was implemented regarding the selection of sample size as recommended by (Altmann, 1974). Mobile Banking Merchants Within the Greater Accra Region; determination of the sample size was achieved; since PLS-SEM, by nature, offers results with a smaller sample size; the ten(10) rule was applied as recommended by (Barclay et al., 1995; Hair et al., 2011), according to the proposed model in the study; the minimum sample size is ninety 90.
Meanwhile, the minimum sample may be too small for this study(Kock & Hadaya, 2018). The inverse square root method was also applied. Hence minimum sample size used for the study is four hundred and ten (410), which forms the basis for the sample size for the analysis.

Data Analysis

The analysis was carried out using the Partial Least Squares structural equation models (PLS-SEM) since the approach strives to facilitate assessing patterns of causation of target constructs in the suggested structural model for the study. It also gives more specific statistical connections to back up variables in a model. PLS-SEM was also employed since it allows for smaller samples than other statistical tools such as Amos and Lisrel. The demographic analysis of mobile banking merchants' profile information is presented in Table 1. These merchants willing to participate in the survey were asked to provide information on their gender, age, years of experience in operating in the mobile banking sector, the merchant's level of privacy knowledge, vendor type (private or public), and educational background. The respondents were primarily males (58.8%), with 41.2% females. Concerning age, 52.4% of mobile banking merchants were between 21 and 30 years, 21% were between the ages of 11 and 20, 20.5% were between the ages of 31 and 40, 4.1% were between the ages of 41 and 50, .2% were the ages of 61+, while 1.7% were between the age of 51 and 60 years. This indicates having most of the teaming youth involved as merchants in the area of mobile banking in Ghana. Most mobile banking merchants (57.8%) had 0 to 3 years of experience, 31.2% had 4 to 6 years of experience, while the minority of the respondents recorded 8.8% and 2.2 % were between 7 to 9 or more years of experience. In considering the security of the transaction and its related data, the respondents were also to indicate their level of privacy knowledge, 14.4% were recorded as being experts in handling security related to privacy issues,12.2% were proficient, 22.2% were competent, 27.1% also consider themselves as advanced beginners whiles 24.1% is recorded as being novice or beginner. The result of the data further shows that 52.7% of the mobile banking merchants were publicly owned, and 47.3% of the respondent were privately owned. Finally, from the perspective of educational qualifications, out of the four hundred and ten (410) respondents recorded., 2%,7.1%,9.8%,10.2%,13.2%,25.4% and 34% representing PhD, HND, Diploma, Professional qualification, Postgraduate degree, First degree and Senior High School respectively. Chin's (1998) two-step structural equation model evaluation was employed. The authors first examined the measurement model to determine instrument reliability and validity and then examined the structural model based on this study's hypotheses.

ISSN: 3057-3610

Table 1: Demographic of respondents

Attributes	Categories	Frequency	Percent
	Male	241	58.8
Gender	Female	169	41.2
Age	11-20	86	21.0
	21-30	215	52.4
	31-40	84	20.5
	41-50	17	4.1
	51-60	7	1.7
	61+	1	.2
Yearsofexp	0 to 3 years	237	57.8
	4 to 6 years	128	31.2
	7 to 9 years	36	8.8
	More than 9 years	9	2.2
PrivacyKnledge	Novice/beginner	99	24.1
	Advanced Beginner	111	27.1
	Competent	91	22.2
	Proficient	50	12.2
	Expert	59	14.4
VendorType	Public	216	52.7
	Private	194	47.3
EducationLevel	Senior High School	140	34.1
	Diploma	40	9.8
	HND	29	7.1
	First degree	104	25.4
	Postgraduate degree	54	13.2
	Professional qualification	42	10.2
	PhD	1	.2

ISSN: 3057-3610

Measurement models

In this section, the authors evaluate the procedures to test and measure the reliability and validity of the result. Measurements addressed; in this section were namely;

1) indicator loadings and internal consistency reliability

2) convergent validity

and

3) discriminant validity;

as recommended by (Shmueli, Sarstedt, et al., 2019) (J F Hair et al., 2021)(Joseph et al. et al., 2019).

Indicator Loadings and Internal Consistency Reliability

PLS-SEM results were utilized for the indicator loadings in this study. See Figure 2 and Table 2 below detailing loadings with threshold values > .708 as recommended by (Shmueli, Sarstedt, et al., 2019)(Joseph F Hair et al., 2018). From the PLS algorithm process in PLS-SEM, FOUR indicators from the Attitude Toward securing Information (ATWSI1), Perceived Response Efficacy (PRE2) and Perceived Probability of Vulnerability (PSOT1), (PSOT4) were removed from the final analysis; Because their loadings were below .708 threshold as indicated by (Hair et al., 2019). Twenty-four (24) indicators were finally considered for the consequent analysis within the PLS-SEM. In considering the internal consistency reliability, statistically across indicators. Internal consistency reliability is reported through Cronbach's alpha (CA) and Composite Reliability (CR). The values of CA and CR in this study were implemented, the threshold for CA should be >.700, and CR should be > .708, as recommended by (Hair et al., 2018). Values for all constructs have good internal consistencies, as shown in Table 2 below, on values regarding Cronbach's Alpha (CA), rho_A, and Composite Reliability (CR), respectively. In addition to the above discussions, convergent validity is also a statistical technique related to construct validity which suggests that the evaluations of identical constructs should be highly related. The Average Variance Extracted (AVE) scores are used to determine convergent validity in this study. A PLS-SEM approach was used to estimate the scores. The threshold recommended by Hair et al., 2018 and Shmueli et al., 2019 for AVE scores is either .500 or higher, which explains 50% or more variation. Table 2 below provides details on AVE value.

Table 2: loadings and internal consistency reliability

Constructs	Items	Loadings	CA	rho_A	CR	AVE
Attitude Toward Securing Information	ATWSI2	0.858	0.819	0.820	0.892	0.734
	ATWSI3	0.854				
	ATWSI4	0.859				
Intention to Secure Information	ITSI1	0.806	0.858	0.858	0.904	0.702
	ITSI2	0.871				
	ITSI3	0.865				

ISSN: 3057-3610

	ITSI4	0.807				
perceived probability of Vulnerability	PPOV1	0.700	0.816	0.820	0.879	0.645
	PPOV2	0.764				
	PPOV3	0.820				
	PPOV4	0.836				
	PPOV5	0.808				
Perceived Self Efficacy	PRE1	0.749	0.853	0.854	0.895	0.630
	PRE3	0.797				
	PRE4	0.823				
	PRE5	0.840				
Perceived Response Efficacy	PSE1	0.783	0.846	0.851	0.890	0.620
	PSE2	0.821				
	PSE3	0.812				
	PSE4	0.796				
	PSE5	0.754				
Perceived Severity of Threat	PSOT2	0.749	0.738	0.750	0.851	0.657
	PSOT3	0.864				
	PSOT5	0.815				

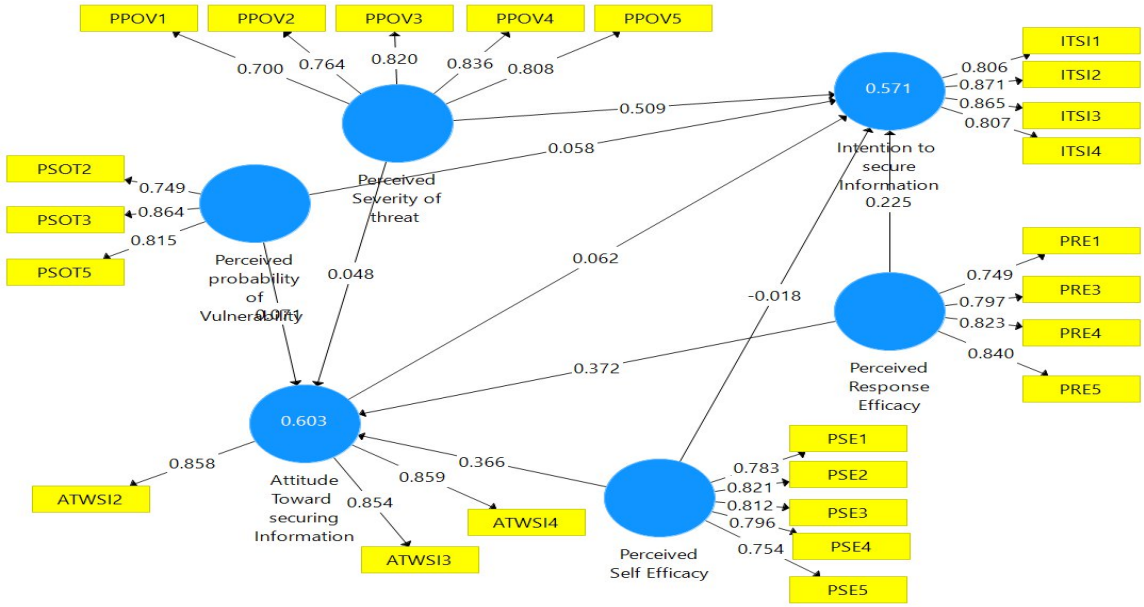

Figure 2 Measurement model

Discriminant Validity

ISSN: 3057-3610

Discriminant validity validates the extent to which a construct differs from each other. In this study, Fornell-Larcker criterion was used to establish the discriminant validity. Further, discriminant validity was evaluated using cross-loadings. Discriminant validity emerges when a construct's loading value is more significant than all of its cross-loading values. Discriminant validity emerges when HTMT values for similar constructs are < 0.90 and then for different constructs are < 0.85. as recommended by (Hair et al., 2019). Hence if a construct shows an HTMT value of > .900, it indicates a lack of discriminant validity. See Tables 3, 4, and 5 below on Fornell Larcker criterion, cross-loadings and HTMT value, respectively.

Table 3: Fornell Larcker criterion

	Attitude Toward Securing Information	Intention to Secure Information	Perceived Response Efficacy	Perceived Self Efficacy	Perceived Severity of Threat	Perceived probability of Vulnerability
Attitude Toward Securing Information	0.857					
Intention to Secure Information	0.545	0.838				
Perceived Response Efficacy	0.722	0.639	0.803			
Perceived Self Efficacy	0.716	0.561	0.728	0.794		
Perceived Severity of Threat	0.587	0.725	0.672	0.654	0.787	
Perceived probability of Vulnerability	0.614	0.599	0.712	0.667	0.698	0.811

Table 4: Cross loadings

	Attitude Toward Securing Information	Intention to Secure Information	Perceived Response Efficacy	Perceived Self Efficacy	Perceived Severity of Threat	Perceived probability of Vulnerability
ATWSI2	0.858	0.453	0.620	0.614	0.490	0.515
ATWSI3	0.854	0.453	0.594	0.615	0.491	0.498
ATWSI4	0.859	0.494	0.640	0.611	0.528	0.562
ITSI1	0.458	0.806	0.569	0.482	0.587	0.531
ITSI2	0.471	0.871	0.536	0.460	0.588	0.492
ITSI3	0.426	0.865	0.471	0.435	0.579	0.442
ITSI4	0.466	0.807	0.557	0.495	0.663	0.531
PPOV1	0.373	0.587	0.461	0.453	0.700	0.465
PPOV2	0.431	0.485	0.498	0.515	0.764	0.483
PPOV3	0.482	0.511	0.527	0.557	0.820	0.533
PPOV4	0.506	0.573	0.586	0.522	0.836	0.620
PPOV5	0.506	0.673	0.562	0.526	0.808	0.621
PRE1	0.560	0.485	0.749	0.571	0.537	0.544

ISSN: 3057-3610

PRE3	0.543	0.502	0.797	0.562	0.561	0.571
PRE4	0.532	0.535	0.823	0.619	0.531	0.582
PRE5	0.671	0.531	0.840	0.586	0.532	0.588
PSE1	0.594	0.502	0.629	0.783	0.505	0.555
PSE2	0.559	0.470	0.588	0.821	0.536	0.528
PSE3	0.564	0.428	0.556	0.812	0.499	0.518
PSE4	0.568	0.411	0.577	0.796	0.554	0.541
PSE5	0.553	0.406	0.530	0.754	0.501	0.500
PSOT2	0.415	0.449	0.490	0.451	0.437	0.749
PSOT3	0.554	0.525	0.639	0.593	0.627	0.864
PSOT5	0.514	0.479	0.592	0.567	0.617	0.815

Table 5: HTMT

	Attitude Toward Securing Information	Intention to Secure Information	Perceived Response Efficacy	Perceived Self Efficacy	Perceived Severity of Threat	Perceived probability of Vulnerability
Attitude Toward securing_ Information						
Intention to Secure Information	0.648					
Perceived Response Efficacy	0.878	0.761				
Perceived Self Efficacy	0.856	0.651	0.871			
Perceived Severity of Threat	0.702	0.841	0.808	0.771		
Perceived probability of Vulnerability	0.783	0.748	0.912	0.834	0.868	

Structural model assessment

(Hair et al., 2019) recommend steps for assessment of the structural model. The assessment process was followed in reporting the Variance Inflation Factor (VIF), establishing the relationship between exogenous and endogenous constructs, coefficient of determination (R2) and predictive relevance(Q2) values. The study examines collinearity which was reported through the examination of VIF value. According to (Hair et al., 2018)(Hair et al., 2019), collinearity becomes an issue if the VIF value is reported to be> 3.000. see Table 6 for details values for collinearity. Collinearity is not an issue in this study since all VIF values are less than 3 (Hair et al., 2019; Muhaimin et al., 2020).

Table 6 Collinearity

		VIF
Attitude Toward Securing Information	ATWSI2	1.848
	ATWSI3	1.834
	ATWSI4	1.792

ISSN: 3057-3610

Intention to Secure Information	ITSI1	1.841
	ITSI2	2.469
	ITSI3	2.421
	ITSI4	1.755
Perceived probability of Vulnerability	PPOV1	1.440
	PPOV2	1.785
	PPOV3	2.079
	PPOV4	2.223
	PPOV5	1.894
Perceived Response Efficacy	PRE1	1.477
	PRE3	1.714
	PRE4	1.921
	PRE5	1.873
Perceived Self Efficacy	PSE1	1.965
	PSE2	2.252
	PSE3	1.973
	PSE4	1.980
	PSE5	1.776
Perceived Severity of Threat	PSOT2	1.358
	PSOT3	1.673
	PSOT5	1.508

Path Coefficient Analysis

To assess the path coefficient between exogenous and endogenous constructs in this study, applying a 5% significance level supported most hypotheses in this research except for H1; this is evidenced in Table 7 and Figure 3. Perceived Probability of Vulnerability was not a significant predictor for Intention to Secure information (β= 0.058; t= 0.7941; p= 0.427). H2: Perceived Probability of Vulnerability was not a significant predictor for Attitude Toward Securing Information (β = 0.071; t= 1.132; p = 0.258). H2.1: Perceived Severity of threat also has a positive relationship on Attitude Toward Securing Information but is insignificant (β= 0.048; t= 0.957; p= 0.339). H4: Perceived Self Efficacy has a negative relationship with the Intention to Secure information and is also insignificant (β= -0.018; t =0.262; p = 0.794). H5: Attitude Toward Securing Information also resulted in a negative relationship with Intention to Secure information (β =-0.062; t = 1.145; p= 0.253). The most vital relationship emerged, supporting H2; Perceived Severity of Threat significantly predicted Intention to Secure information (β =0.509; t =6.326; p = 0.000). H3; Perceived Response Efficacy significantly predicted Intention to Secure information (β =0.225; t =2.980; p =0.003). Additionally, positively significantly predicted Attitude Toward Securing Information H3.1 (β =0.372; t=5.879; p =0.000) and finally, our results also gave an indication of Perceived Self Efficacy having a significant impact on Attitude Toward securing Information, H4.1 (β= 0.366; t=5.534; p = 0.000).

Table 7 Path Result

Hypotheses	Path	β	T Statistics	P Values	Significance
H1	Perceived probability of Vulnerability -> Intention to secure Information	0.058	0.794	0.427	No
H1.1	Perceived Probability of Vulnerability -> Attitude Toward Securing Information	0.071	1.132	0.258	No
H2	Perceived Severity of Threat -> Intention to Secure Information	0.509	6.326	0.000	Yes

ISSN: 3057-3610

H2.1	Perceived Severity of Threat -> Attitude Toward Securing Information	0.048	0.957	0.339	No
H3	Perceived Response Efficacy -> Intention to Secure Information	0.225	2.980	0.003	Yes
H3.1	Perceived Response Efficacy -> Attitude Toward Securing Information	0.372	5.879	0.000	Yes
H4	Perceived Self-Efficacy -> Intention to Secure Information	-0.018	0.262	0.794	No
H4.1	Perceived Self-Efficacy -> Attitude Toward Securing Information	0.366	5.534	0.000	Yes
H5	Attitude Toward Securing Information -> Intention to Secure Information	0.062	1.145	0.253	No

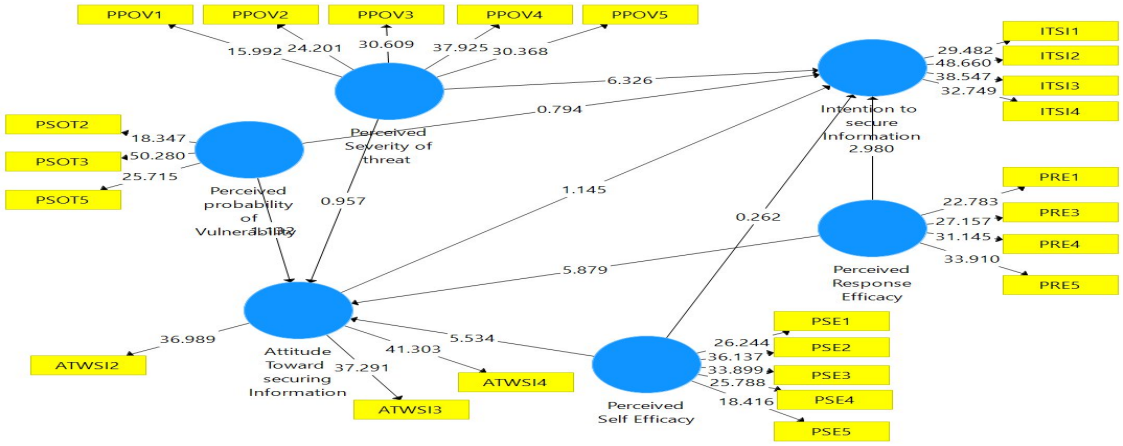

Figure 3: Final Model

Coefficient of Determination (R^2)

The coefficient of determination R2 explains how the exogenous variable may predict the variance percentage in endogenous variables. It examines a given model's prediction accuracy. It is estimated as the squared correlation between the endogenous constructs. The threshold for an R2 value ranges from 0 to 1; the higher the value, the higher the value of R2. 0.75 is, therefore, substantial, 0.50 is moderate, and 0.25 is considered weak, as Hair et al. (2019) recommended. Meanwhile, values of 0.90 and more are usually indicative of overfitting. The study results in Table 8 below provide the details as namely; R2: Attitude Towards Securing Information (0.603, moderate) and Intention to Secure information (0.571, moderate). In conclusion, therefore, the results of R2 show a sufficient level of R2.

Table 8: Coefficient of determination (R^2)

	R Square	Consideration
Attitude Toward Securing Information	0.603	Moderate
Intention to Secure Information	0.571	Moderate

Predictive Relevance (Q^2)

Research demonstrates accuracy in predicting the data points of items if the model performs predictive relevance (Hair et al., 2019). Stone-Geisser's technique was employed in this study to report the predicted

ISSN: 3057-3610

relevance of Q2 using blindfolding techniques in PLS-SEM to estimate Q2 values. Values > 0 indicate the model's establishing meaningful predictive relevance, therefore, values higher than 0, 0.25 and 0.50 depict small, medium and large predictive accuracy, respectively. (Hair et al., 2019; Hair et al., 2018). In the results of this study, Attitude Toward securing information shows the highest predictive significance (Q2 0.589), whereas Intention to secure information reveals the lowest predictive relevance (Q2 0.547). See Table 9 below.

Table 9. Predictive relevance (Q^2)

	Q^2_predict	Consideration
Attitude Toward Securing Information	0.589	Medium
Intention to Secure Information	0.547	Medium

ISSN: 3057-3610

Table 10. Mediation results

	TOTAL EFFECT		DIRECT EFFECT		INDIRECT EFFECT		
	PATH COEFFICIENT	P-VALUES	PATH COEFFICIENT	P-VALUES		PATH COEFFICIENT	P-VALUES
Perceived probability of Vulnerability -> Intention to secure **Information**	0.062	0.392	0.004	0.503	Perceived probability of Vulnerability -> Attitude Toward securing Information -> Intention to secure Information	0.004	0.503
Perceived Severity of Threat -> Intention to Secure Information	0.512	0.000	0.003	0.581	Perceived Severity of Threat -> Attitude Toward Securing Information -> Intention to Secure Information	0.003	0.581
Perceived Response Efficacy -> Intention to Secure Information	0.248	0.001	0.023	0.265	Perceived Response Efficacy -> Attitude Toward securing Information -> Intention to secure Information	0.023	0.265
Perceived Self-Efficacy -> Intention to Secure Information	0.004	0.952	0.023	0.253	Perceived Self-Efficacy -> Attitude Toward Securing Information -> Intention to Secure Information	0.023	0.253

Mediation Result

The authors researched to evaluate the mediating role of Attitude Toward Securing the information on the independent variables (Perceived Probability of Vulnerability, Perceived Severity of Threat, Perceived Response Efficacy and Perceived Self-Efficacy) and the dependent variable (Intention to Secure Information). Table 10 shows the findings of the investigation. Based on the recommendations of Preacher & Hayes (2004), mediation was tested using bootstrapping. In line with H1.1, H2.1, H3.1 and H4.1. The study results in (table 10) above reveal the total effect of the perceived probability of Vulnerability on the Intention to secure information; although there is a positive relationship, it is not significant (H1.1: β = 0.004, P = 0.952). With the introduction of the mediator variable Attitude Toward Securing Information, the impact of the perceived probability of Vulnerability on Intention to secure information shows a positive effect. However, it is not significant (β = 0.023, p=0.253). The indirect effects of the perceived probability of Vulnerability on Intention to secure information through Attitude toward securing information is insignificant (β = 0.023, p=0.253), therefore implies that there is no mediation effect between the association of perceived probability of Vulnerability and Intention to secure information. Hence the findings fail to support H1.1. Assessing the mediation role of Attitude toward securing information between perceived severity of threat and Intention to secure information. The result in (table 10) also shows that the total effect of the perceived severity of the threat on the Intention to secure information has a significant positive impact (β = 0.248, p=0.001). The introduction of the mediator variable Attitude toward securing information shows a positive relationship but is insignificant (β = 0.023, p=0.265). The indirect effect of the perceived severity of the threat on the Intention to secure information through Attitude toward securing information establishes a positive effect but is insignificant (β = 0.023, p= 0.265). The above result, therefore, clearly indicates that there is no mediation effect between the perceived severity of the threat and the Intention to

ISSN: 3057-3610

secure information suggesting that H2.1 fails to support. Evaluating the mediation role of Attitude toward securing information between perceived response efficacy and Intention to secure information provides the results in Table 10 above; the total effect of perceived response efficacy on Intention to secure information has a positive effect and is significant (β = 0.512, p=0.000). With the mediating variable Attitude toward securing information, the results show a positive but insignificant relationship (β = 0.003, p=0.581). The indirect effect between perceived response efficacy on Intention to secure information through Attitude toward securing information establishes a positive effect but is not significant (β = 0.003, p= 0.581); therefore, the findings indicated a complementary partial mediation effect. Hence the above results shown suggest support for H3.1. Finally, assessing the mediating role of Attitude toward securing information between perceived self-efficacy and Intention to secure information. In Table 10 above, the total effect of perceived self-efficacy on the Intention to secure information has a positive and insignificant effect (β = 0.062, p=0.392). Introducing the mediating variable, Attitude toward securing information, the results reveal a positive relationship but not significant (β = 0.004, p=0.503); from the perspective of the indirect effect between perceived self-efficacy on Intention to secure information through Attitude toward securing information, results show a positive effect but is not significant (β = 0.004, p= 0.503). The findings, therefore, indicate that there is no mediation effect. Hence the above results shown suggest no support for H4.1.

Discussion of Key Findings

The study provides significant vital findings as well as theoretical and practical implications. Despite the numerous prior studies on behavioural information security, this study seeks to assess the attitudes of mobile banking merchants' intentions to secure transaction data. Researchers applied Protection Motivation Theory (PMT) to better understand mobile banking-related cybercrime to assess mobile banking merchants' intentions to secure mobile transaction data. The proposed conceptual framework was formed by taking into account dependent variables as being the Intention to secure information (ITSI) and independent variables as being the perceived probability of Vulnerability (PPOV), the perceived severity of threat (PSOT), the perceived response efficacy (PRE), the perceived self-efficacy (PSE), and the Attitude toward securing information (ATWSI). The study's finding suggests that the perceived probability of Vulnerability has no significant influence on merchant intentions to secure information; prior studies have also confirmed that the perceived probability of a security breach has no significant influence on security breach concern. This is confirmed in (Crossler, 2009; Herath & Rao, 2009; Mills & Sahi, 2019; Ophoff & Lakay, 2019); This could imply that although users could be very much aware of the extent of vulnerabilities; it does not necessarily influence the mobile merchant's Intention to secure. Since the impact could sometimes have a negative impact, it may have little or no impact on transactions information being exposed to unnecessary risks, threats and uncertainty.

On the other hand, Mumtaz & Arachchilage (2019) confirmed that perceived Vulnerability is a crucial predictor of information security adoption behaviour. The study further reveals that the perceived probability of Vulnerability also fails to establish a significant relationship with the Attitude toward securing information; the finding of the study means that perceived Vulnerability from the perspective of these merchants has minimal impact on their Attitude toward securing information in the context of withholding Transaction information, using a secure app for the transaction. It was confirmed in prior studies by Martens on privacy cynicism and its role in privacy decision-making.

Analyzing the relationship between the perceived severity of the threat and the Intention to secure information proves a positive significant association; this, therefore, provides support. The findings, therefore, demonstrate when these mobile merchants perceived the severity of the threat turned to influence their Intention to secure and, to a large extent, comply with information security policy; this was confirmed in a related study by (Ooijen et al., 2022). They established the relationship between perceived severity and privacy protection behaviour. The perceived severity of the threat and Attitude toward securing information were insignificant. Hence this result is therefore different from previous studies.(Martens et al., 2019; Tang et al., 2021). The findings imply that, while these mobile banking merchants are well aware of the consequences of viruses and unauthorized individuals accessing such information, this does not directly alter their Attitude toward information security. The finding also reveals that the relationship between

ISSN: 3057-3610

perceived response efficacy and Intention to secure information is positive and significant, consistent with prior research.(Li et al., 2022; Mills & Sahi, 2019); this could imply that The merchant's significant role in protecting and ensuring the security of mobile banking information will influence the merchant's decision to implement security measures. Meanwhile, in a related study, considering mitigation of ransomware threat response efficacy was not significantly related to the Intention to secure (Ophoff & Lakay, 2019). The study further reveals that perceived response efficacy significantly and positively impacts attitudes toward securing information. It could also mean that the crucial role in safeguarding and protecting mobile banking information significantly determines merchants' perspectives concerning information security. The finding is consistent with the earlier position by Herath & Rao (2009). They indicated a significant effect between response efficacy and attitudes towards security policies. The finding Establishes the relationship between perceived self-efficacy and Intention to secure information and also found to have a negative and insignificant relationship. Meanwhile, the relationship between perceived Self Efficacy and Attitude toward securing information was found to be significant, and this was also found to be consistent with earlier studies by(Kimpe et al., 2021; Ooijen et al., 2022) confirming a significant and positive association to take security measures. If a mobile banking merchant fails to recognize the significance of the vulnerabilities that result from failing to provide safety, Protecting and maintaining mobile banking information will have a detrimental influence on their willingness to protect transaction information. Finally, the study findings fail to establish a relationship between attitudes Attitude Toward securing information and intentions to secure information; this finding implies that if the mobile banking merchant does not adopt the proper Attitude toward protecting and withholding transaction information, it will have a detrimental impact on the Intention of safeguarding this transaction information. However, a previous study by Luo et al. (2021) exhibited a positive and significant influence on continued intentions.

Implications

Theory

Theoretically, this investigation contributes to the body of cybercrime research knowledge. In addition, our proposed conceptual model clarifies how cybercrime prevention efforts might change in response to a Threat appraisal and a Coping appraisal from the perspective of the Protection motivation theory (PMT). The Attitude Towards Securing Information variable was utilized as a moderating variable (i.e., withholding transaction information and coping with mobile banking risks), thereby emphasizing the significance of mobile merchants' efforts to improve cybercrime defences. The findings of this study provide a definitive response to the contradictory findings of other studies regarding mobile merchants' perceptions of cybercrime vulnerabilities and actions when they confront cybercrime problems to secure information. Further, the study contributes to the theory by establishing that factors influencing protection motivation behaviour, such as Perceived Severity of Threat and Perceived Response Efficacy, promote mobile banking merchants' Intention to secure.

In contrast, the study reveals that Perceived Response Efficacy and Perceived Self Efficacy significantly impact Mobile Banking Merchants' Attitudes Towards Securing Information. Due to the lack of significance, the researchers concluded that the Perceived probability of Vulnerability, Perceived Self Efficacy, and Attitude Toward Securing Information lose their predictive power for Mobile Banking Merchants' Attitude Toward Securing Information. The results of our mediation analysis indicate that perceived response efficacy on Intention to secure information via Attitude toward securing information establishes a positive effect, albeit one that is not statistically significant. The results also indicated a complementary partial mediation effect.

Practice

As explained in earlier sections, persons who are available to offer mobile money services (withdrawals and deposits) using mobile banking platforms are the primary focus. This research suggests that mobile banking merchants can be motivated to comply with policy measures to influence their Intention to secure information. Their motivation could be further enhanced via their engagement in the telecom operators'

ISSN: 3057-3610

regularly organized in-house cyber security awareness training and campaigns to shape the compliance behavioural intentions of these mobile banking merchants. Considering the perceived probability of Vulnerability, there is a need for mobile banking merchants to adhere to information security policy and avoid the breach of mobile banking information security. The merchants should also endeavour to implement adequate measures to avert the severity of the threat from the perspective of virus attacks on mobile applications, the issue of theft from mobile wallets by cyber criminals and avoidance of indiscriminate mobile banking transactions being widely disseminated online.

Regarding perceived self-efficacy, mobile banking merchants should adhere to the mobile banking industry's information security policies and guidelines and take precautionary measures by employing experienced personnel to handle mobile banking transactions. Finally, concerning mobile banking merchants' Attitudes toward securing information, they need to withhold transaction information 24/7, ensuring that the mobile banking app is secure and safe for transactions. In summary, the industry benefit from this study is that practitioners must engage in regular awareness creation sessions, adhere to information security policy, avoid the breach of mobile banking information security and take relevant precautionary measures to withhold transaction information.

Limitations and Future Research

This paper's introduction explains that mobile banking merchants consist of individual vendors and financial institutions. In the Ghanaian context, individual vendors tend to be in the majority. The primary focus of the research work was the individuals who are licensed or authorized to act as mobile banking merchants for the various telecommunication companies. The fact that the investigation did not include financial institutions and banks may serve as a guidepost for other researchers who, in the future, want to build upon the findings of this work. It is therefore suggested that future research focus on financial institutions offering the same service and possibly juxtapose the outcome with findings from this research.

Conclusion

This current research was conceived against the backdrop of investigating what motivates mobile banking merchants' Intention to secure transaction-related data. Since information security cannot be attained solely by technological means, most institutions invest resources and time into developing, implementing, and maintaining computer security policies. These efforts, however, will only be practical if end users are eager and prepared to adhere to cyber security policies. The study aimed to determine factors that would influence these mobile banking merchants to take the necessary steps to safeguard transactions and the data involved.

Gaining knowledge of the significance of user motivation could guarantee the security of mobile banking transactions; hence the study, therefore, thus contributes to theory and practice. Factors influencing protection motivation behaviour, such as Perceived Severity of threat, Perceived Response Efficacy, may encourage mobile banking merchants' Intention to secure. Meanwhile, the findings of the study establish that. Perceived Response Efficacy and Perceived Self Efficacy Significantly influence Mobile Banking Merchant's Attitude Toward Securing Information. We recommend that organizations develop appropriate cybercrime training and security awareness programs to ensure employees have up-to-date knowledge of cybercrime vulnerability and conditions that will improve their willingness to deal with these mobile banking vulnerabilities. Future studies could build on the current research conceptual framework by introducing other competing new variables that can be statistically tested.

Authors Acknowledgment

The authors would like to thank all mobile banking merchants within the Greater Accra region for their valuable support as respondents for this study.

ISSN: 3057-3610

Scaled variable & Measurement items		Sources
Intention To Secure Information	**ITSI1 :** Compliance with best practices in information security is expected. **ITSI2 :** The future of mobile banking transactions is intended to be secure **ITSI3 :** There is always the desire to protect mobile banking transaction information **ITSI4 :** I plan to continue to use and secure mobile commerce	(Ifinedo, 2011; Luo et al., 2021; Sharma & Aparicio, 2022)
Perceived Probability Of Vulnerability	**PPOV1 :** Failure to adhere to information security policy might put mobile banking transactions at risk. **PPOV2** : Users who breach mobile banking information security rules suffer an attack. **PPOV3 :** Users who ignore information security regulations and standards may compromise mobile banking data and resources **PPOV4 :** Sharing my mobile transactions information exposes me to unnecessary risks, threats, and uncertainty. **PPOV5 :** Sharing my mobile banking details online makes me vulnerable to fraud	(Crossler, 2009; Ooijen et al., 2022; Ophoff & Lakay, 2019; Sharma & Aparicio, 2022; Tang et al., 2021)
Perceived Severity Of Threat	**PSOT1 :** If a virus infects my mobile money app, it might seriously disrupt my ability to conduct financial transactions. **PSOT2 :** It's a major issue if someone else can access my mobile banking details without my knowledge **PSOT3 :** A significant obstacle for our business will be the theft of electronic funds from our mobile wallets by cyber criminals **PSOT4 :** There is a high likelihood that my mobile banking information will be used by a third party elsewhere online. **PSOT5 :** When personal information about your mobile banking transactions is widely disseminated online, you risk incurring damages.	(Boerman et al., 2021; Crossler, 2009; Ooijen et al., 2022; Ophoff & Lakay, 2019; Sharma & Aparicio, 2022; Tang et al., 2021)
Perceived Response Efficacy	**PRE1 :** Everyone has a role to play in protecting the mobile financial information system **PRE2 :** Unfortunately, there is nothing a person can do to ensure the safety of their mobile banking data **PRE3 :** To assist in ensuring the safety of	(Boerman et al., 2021; Crossler, 2009; Luo et al., 2021; Ooijen et al., 2022; Ophoff & Lakay, 2019;

ISSN: 3057-3610

	financial transactions it is crucial to adhere to mobile banking's information security regulations **PRE4 :** Protecting our business's mobile banking data from the public internet will keep it safe from cybercriminals **PRE5 :** Effectively managing mobile transactions will prevent losses	Sharma & Aparicio, 2022; Tang et al., 2021)
Perceived Self Efficacy	**PSE1 :** I will feel more confident adhering to most of the mobile banking industry's information security policies **PSE2 :** Information security guidelines for mobile banking are simple enough to implement **PSE3 :** Without assistance, I could still adhere to the guidelines for protecting sensitive data while using mobile banking. **PSE4 :** Because of my experience, I can use the tools at my disposal to ensure that our mobile money transaction is secure against fraudsters **PSE5 :** I can take precautions to ensure that our mobile banking activities are secure from outside interference	(Boerman et al., 2021; Crossler, 2009; Lee et al., 2023; Luo et al., 2021; Ooijen et al., 2022; Ophoff & Lakay, 2019; Sharma & Aparicio, 2022; Tang et al., 2021)
Attitude Toward Securing Information	Please tick the correct numeric response to each question **ATWSI1 :** Withholding Transaction information on mobile banking transaction information is necessary **ATWSI2 :** Using the mobile banking app and securing it would be a pleasant experience **ATWSI3 :** I want to use e-cash more if this mobile banking app is secure **ATWSI4 :** It is wise to secure mobile banking transactions safely	(Ifinedo, 2011; Lee et al., 2023; Luo et al., 2021; Wu, 2020)

ISSN: 3057-3610

References

Abebe, F. (2020). DigitalCommons @ Kennesaw State University Factors Affecting Mobile Payment Adoption by Merchants in Ethiopia. 0–11.

Altmann, J. (1974). Observational study of behavior: sampling methods. *Behaviour*, **49**(3–4), 227–266.

Anderson, C.L. & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. MIS Quarterly, **34**(3), 613–643.

Asani, E.O., Omotosho, A., Danquah, P.A., Ayegba, P.O. & Longe, O.B. (2021), A maximum entropy classification scheme for phishing detection using parsimonious features, Telkomnika (TelecommunicationComputing Electronics and Control) this link is disabled, **19**(5), 1707–1714

Aspers, P. & Corte, U. (2019). What is qualitative in qualitative research. **1**, 139–160.

Barclay, D., Higgins, C. & Thompson, R. (1995). The Partial Least Squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. *Technology Studies*, **2**(2), 285.

Bhatt, V., Hiteshi, A.A. & Nayak, K. (2021). An empirical study on analyzing a user's intention towards using mobile wallets; Measuring the mediating effect of perceived attitude and perceived trust. *Turkish Journal of Computer and Mathematics Education*, **12**(10), 5332–5353.

Boerman, S.C., Kruikemeier, S. & Borgesius, F.J.Z. (2021). Exploring motivations for online privacy protection behavior: Insights from Panel Data. https://doi.org/10.1177/0093650218800915

Brook, C. (2017), "Mobile banking trojan bankbot identified, removed from Google Play". Digital Guardian. Retrieved 3 October 2018.

Chin, W.W. (1998). The partial least squares approach to structural equation modeling. In *Modern Methods for Business Research*, **295**, 295–336. https://doi.org/10.1016/j.aap.2008.12.010

Crossler, R.E. (2009). Protection motivation theory: Understanding the determinants of individual security behavior protection motivation theory: Understanding the determinants of individual security behavior.

Danquah, P. (2020). Security operations center: A framework for automated triage, containment and escalation, *Journal of Information Security,* **11**(4) DOI: 10.4236/jis.2020.114015

Habibi, A., Yusop, F.D. & Razak, R. (2020). The role of TPACK in affecting pre-service language teachers' ICT Integration during teaching practices. *Indonesian Context. Educ Inf. Technol*, **25**(3), 1929–1949.

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

Hair, J.F., Hult, G.T.M., Ringle, C., Sarstedt, M., Danks, N. & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. In *Springer*.

Hair, Joseph F., Ringle, C. M. & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice*, **19**(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

ISSN: 3057-3610

Hair, J.F., Risher, J.J., Sarstedt, M. & Ringle, C.M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, **31**(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J.F., Risher, J.J. & Ringle, C.M. (2018). When to use and how to report the results of PLS-SEM. **31**(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Heny, S., Dian Citaningtyas A.K., Hari P. & Wahyu S.L. (2022). The effect of easy perception and security perception on the intention of using shopeepay through attitude as intervening variables in madiun. *International Journal of Science, Technology & Management*, **3**(1), 215–228. https://doi.org/10.46729/ijstm.v3i1.430

Herath, T. & Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. February, 106–125. https://doi.org/10.1057/ejis.2009.6.

Huang, R., Wang, Z., Yuan, T., Nadarzynski, T., Qian, H., Li, P., Meng, X., Wang, G., Zhou, Y., Luo, D., Wang, Y., Cai, Y. & Zou, H. (2021). Using protection motivation theory to explain the intention to initiate human papillomavirus vaccination among men who have sex with men in China. *Tumour Virus Research*, **12**, 200–222. https://doi.org/10.1016/j.tvr.2021.200222

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, **31**(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Kester, A., Ong, S., Tri, Y., Ma, J., Salazar, L.D., Jacob, J., Erfe, C., Abella, A.A., Nayat, M., Chuenyindee, T., Nadlifatin, R., Agung, A. & Perwira, N. (2022). Investigating the acceptance of the reopening Bataan nuclear power plant: Integrating protection motivation theory and extended theory of planned behavior. *Nuclear Engineering and Technology*, **54**(3), 1115–1125. https://doi.org/10.1016/j.net.2021.08.032.

Kester, Q.A. & Danquah P. (2012). A novel cryptographic key technique, Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference, Pp 70 – 73

Kimpe, L. De, Walrave, M., Verdegem, P. & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, **0**(0), 1–13. https://doi.org/10.1080/0144929X.2021.1905066

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential method. *Information Systems Journal*, **28**(1), 227–261.

Lee, Y.Y., Gan, C.L. & Liew, T.W. (2023). Thwarting instant messaging phishing attacks: the role of self - efficacy and the mediating effect of attitude towards online sharing of personal information.

Li, L., Xu, L., & He, W. (2022). Computers in Human Behavior Reports The effects of antecedents and mediating factors on cybersecurity protection behavior. *5*(October 2021). https://doi.org/10.1016/j.chbr.2021.100165

Longe, O.B., Danquah, P. & Ebem, D.U. (2012). De-Individuation, anonymity and unethical behaviour in Cyberspace – Explorations in the valley of digital temptations. *Computing Information Systems Journal*, **16(**1), 46–55

Luo, Y., Guiping, W.Y.L. & Ye, Q. (2021). Examining Protection Motivation and Network Externality Perspective Regarding the Continued Intention to Use.

ISSN: 3057-3610

Lynn, M.R. (1986). Determination and quantification of content validity. *Nurs. Res.*, **35**(6), 382–385.

Matey, A.H., Danquah, P. & Koi-Akrofi, G.Y. (2022), Predicting Cyber-Attack using Cyber Situational Awareness: The Case of Independent Power Producers (IPPs), International Journal of Advanced Computer Science and Applicationsthis link is disabled, **13**(1), 700–709

Martens, M., Wolf, R.D. & Marez, L.D. (2019). Computers in Human Behavior Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, **92**(November 2018), 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Mills, A.M. & Sahi, N. (2019). An empirical study of home user intentions towards computer security. Proceedings of the Annual Hawaii International Conference on System Sciences, 2019-January, 4834–4840. https://doi.org/10.24251/hicss.2019.583

Mohamed, N. & Ahmad, I.H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, **28**(6), 2366–2375.

MTN Mobile Money Commission in Ghana (2023), *ICT Catalogue*, https://ictcatalogue.com/mtn-mobile-money-merchant-commission/, Retrieved 7 July 2023.

Muhaimin, M., Asrial, A., Habibi, A., Mukminin, A. & Hadisaputra, P. (2020). Science teachers' integration of digital resources in education: a survey in rural areas of one Indonesian province. *Heliyon*, *6*(8), 04631.

Mumtaz A.H. & Arachchilage, N.A.G. (2019). On the impact of perceived vulnerability in the adoption of information systems security innovations. *International Journal of Computer Network and Information Security*, **11**(4), 9–18. https://doi.org/10.5815/ijcnis.2019.04.02

Mwagwabi, F.M. (2015). A Protection Motivation Theory Approach to Improving Compliance with Password Guidelines.

Ooijen, I. Van, Segijn, C.M. & Opree, S.J. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. https://doi.org/10.1177/00936502211060984

Ophoff, J. & Lakay, M. (2019). Mitigating the Ransomware Threat: A Protection Motivation Theory Approach. In *Communications in Computer and Information Science*, **973**. Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_12

Preacher, K.J. & Hayes, A. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. Behav. Res. Methods Instrum. Comput. *[CrossRef] [PubMed]*, **36**, 717–731.

Rajab, M. & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers and Security*, **80**, 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, **91**(1), 93–114. https://doi.org/doi:10.1080/00223980.1975.9915803. PMID 28136248.

Sharma, S. & Aparicio, E. (2022). Computers & Security Organizational and team culture as antecedents of protection motivation among IT employees. **120**. https://doi.org/10.1016/j.cose.2022.102774

ISSN: 3057-3610

Shmueli, G., Hair, J.F., Ting, H. & Ringle, C.M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. https://doi.org/10.1108/EJM-02-2019-0189

Shmueli, G., Sarstedt, M., Hair, J.F., Cheah, J.H., Ting, H., Vaithilingam, S. & Ringle, C.M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing*, **53**(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189

Syed, A.A.B., Hashim, F. & Amran, A. (2019). Determinants of green banking adoption: A theoretical framework. *KnE Social Sciences*, *2019*, 1–14. https://doi.org/10.18502/kss.v3i22.5041

Tang, Z., Miller, A.S., Zhou, Z. & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 101572. https://doi.org/10.1016/j.giq.2021.101572

Voica, C., Singer, F.M. & Stan, E. (2020). How are motivation and self-efficacy interacting in problem-solving and problem-posing? 487–517

Workman, M., Bommer, W.H. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, **24**(6), 2799–2816.

Wu, D. (2020). Computers in Human Behavior Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior*, **105**(December 2019), 106–229. https://doi.org/10.1016/j.chb.2019.106229

Xiao, H., Peng, M., Yan, H., Gao, M., Li, J., Yu, B., Wu, H. & Li, S. (2018). An instrument based on protection motivation theory to predict Chinese adolescents' intention to engage in protective behaviors against schistosomiasis. *Global Health Research and Policy*, November. https://doi.org/10.1186/s41256-016-0015-6.

Zainal, N.T.A., Harun, A. & Lily, J. (2017). Examining the mediating effect of attitude towards electronic words-of mouth (eWOM) on the relation between the trust in eWOM source and intention to follow eWOM among Malaysian travellers. *Asia Pacific Management Review*, **22**(1), 35–44. https://doi.org/10.1016/j.apmrv.2016.10.004.

ISSN: 3057-3610

AUTHOR PROFILE(S)

Paul Danquah, Ph.D

Dr. Paul Asante Danquah is an IT professional and researcher with over 20 years' experience. He holds a BSc HONS in Computing, MSc in Information Security and a PhD in Information Technology (IT) from the University of Greenwich UK, Anglia Ruskin University UK and Open University of Malaysia respectively. He has various industry certifications, some of which are ISO 27001 Lead Implementer, Certified Ethical Hacker(CEH), Certified Security Operations Center Analyst (CSA), Data Center Infrastructure Expert(DCIE), Cisco Certified Network Professional (CCNP), Microsoft Certified Systems Engineer (MCSE) and Certified EC-Council Instructor (CEI). Dr. Danquah has worked in various capacities over the years, these range from Programmer, Network Engineer, IT Manager, Deputy Director of IT, Lecturer and Research Scientist at various prominent technology companies and Universities in Ghana. Some of these are namely Soft Company Limited (now Soft Tribe), Africa Online Ghana Limited, Net Africa Ghana Limited, Ghana Institute of Management & Public Administration (GIMPA), University of Professional Studies Accra (UPSA), the Council for Scietific and Industrial Research (CSIR) and Heritage Christian University College. He has managed several projects and provided numerous technical solutions to over fifty organizations across multiple countries such as Liberia, UK, Gambia and Ghana, he brings an invaluable experience to the table. He has performed vulnerability assessments and penetration test for over 30 organizations in various sectors ranging from government and banks to fintech and utility companies. Dr. Danquah has over 30 published articles in internationally refereed journals and over 15 published conference proceedings. He also has two books cyber security.

Henry Akwetey Matey

Mr. Henry Akwetey Matey is a Lecturer at the University of Professional Studies in Accra. He holds a Master of Science degree in Information Technology, and the majority of his research interests are focused on the topic of information security practices. In the field of research and education, he has around ten years of experience.

Kenneth Asiamah

Mr. Kenneth Asiamah is an ICT professional with an MSc and BSc in Information and Communication Technology Management. He's an Assistant Research Scientist at CSIR – INSTI, focusing on cutting-edge research and the development of innovative tools and systems. Kenneth's technical expertise extends to web development, computer systems administration, and fundamentals of data security. He's committed to industry knowledge, earning the Google IT Support Professional Certificate in 2023.

ISSN: 3057-3610