Indonesian Journal of Business Analytics (IJBA)
Vol.3, No.4, 2023: 1425-1442

Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa

Ntswaki Petunia Matlala
University of Western Cape
Corresponding Author: Ntswaki Petunia Matlala nmatlala@uwc.ac.za

ARTICLEINFO

Keywords: Digital Banking, Cybersecurity, Consumer Behaviour, South Africa

Received : 10, June
Revised : 15, July
Accepted: 21, August

ABSTRACT

Digital banking is linked with several cybersecurity threats, such as the risk of hackers. Against this background, this study aims to explore behavioural insights into cybersecurity practices among digital banking consumers in South Africa. The researcher gathered data from 338 South African banking consumers. A structured questionnaire was used to survey these consumers, and the obtained data were analysed using structural equation modelling (SEM). The results revealed that subjective norms, self-efficacy, and attitude significantly influence the cybersecurity intention behaviour of digital banking consumers. The implications of the study's findings need to be more readily generalisable due to the sociocultural differences across different provinces and populations. Future research should include a more diverse sample to validate these findings further.

DOI: https://doi.org/10.55927/ijba.v3i4.5515
ISSN-E: 2808-0718
https://journal.yp3a.org/index.php/ijba

INTRODUCTION

The rapid advancement of mobile technologies such as tablets, smartphones and feature phones has provided significant opportunities for financial institution to create new payment solutions and provide value-added services to their consumers (Aldiabat et al., 2019; Limna et al., 2023). Integrating mobile devices and the Internet with financial services has resulted in new kinds of digital finance, such as digital payments, online credit, and intelligent investment advice (Khrais, 2015). Nearly 22 million of the South African population use mobile applications and online services (Taylor, 2023). This technology helps consumers with their daily transactions and activities, minimising the impact of location and time. It allows easy access to bank services and communication with bank servers, regardless of physical location (Gomes et al., 2022).

In contrast, the process remains vulnerable to attacks and hacking attempts, mainly due to user behaviours that can create multiple vulnerabilities in the system. Various security measures have been proposed and implemented in response, such as using sms codes, One Time Password (OTP), mobile tokens and biometric characteristics (Alzoubi et al., 2022). Jennings et al. (2023) and Nobles (2018) argued that financial institutions often prioritise technology to reduce risks but overlook human behaviour's impact. Furthermore, the scarcity of research papers on digital banking cybersecurity behaviour shows that this topic still needs to be explored. The study examines behavioural insights into cybersecurity practices among digital banking consumers in South Africa. Consequently, individuals carry out preventative actions only after the cybersecurity threat has occurred (Haddad et al., 2018; Sulaiman et al., 2022). Subsequently, they adopt various measures for prevention: revising passwords, updating or installing antivirus software, and changing all their credentials (Ncubukezi, 2022). As such, knowledge, awareness and attitude toward cybersecurity are required to prevent online victims from being unaware of the incoming malicious behaviours.

The remainder of this paper is organised as follows. First, the study presents an overview of cybersecurity in general security threats and human cybersecurity behaviour, cyber. Secondly, a preliminary qualitative study explored factors affecting digital banking consumers' cybersecurity behaviour. Thirdly, the research methodology and statistical data analysis were discussed to test digital banking consumers' intention to cybersecurity on a larger scale. Finally, the findings, implications and future research directions were discussed.

THEORETICAL REVIEW

Cybersecurity

Digital banking self-service technology (SST) platform. ms like online, web-based, and auto teller machine (ATM) banking seek to deliver financial services digitally (Khrais, 2015.)Digital banking reduces wait times at brick-and-mortar branches and helps produce the best possible results from sales transactions with the fewest resources and employees. It enables consumers to conduct online transactions through the bank's website at any time and location

(Nohumba et al., 2020). Consumers of digital banks conduct immediate bill payments and financial transfers from any location (Pankomera & Van Greunen, 2018). Due to its many benefits (such as shorter wait times, less paperwork, and more accessibility from anywhere), digital banking is quickly becoming the preferred way of banking (Bansal, 2020).

The growing reliance on Information Technology (ICT) in every facet of our cyber-physical society is heightening the urgency of the need to protect against cyber threats (Haddad et al., 2018; Quiroz et al., 2021). Individuals, governments, and non-profits all need to take steps to protect their data in cyberspace but achieving absolute security can be challenging (Haddad et al., 2018). Cybersecurity integrates tools, policies, security concepts, security safeguards and guidelines (Du Toit et al., 2018). Cybersecurity is an interdisciplinary science (Jiang & Daniel Broby, 2021). It includes hostile engagement, attack, defence, and mitigation. Cyber security can be divided into three critical arenas of threats (1) vulnerability, (2) reaction, and (3) legal recourse. These threats and occurrences are escalating in severity. (Sheth et al., 2021) claim that the threats are mitigated in either a defensive or offensive manner.

Moreover, von Solms and von Solms. (2018) define cybersecurity "as protecting information assets by addressing the threats to information processed, stored and transported by internetworked information systems." It is a field concerned with keeping connected devices and the data they store safe from hackers out to steal or otherwise compromise sensitive data or disrupt service (Quiroz et al., 2021). According to Alzoubi et al. (2022), using digital platforms to transact is not secure despite the security precautions implemented by such sites. Similarly, Kangapi and Chindenga. (2022) reiterate that as organisations and consumers perform more transactions online, the risk of cybercrime rises gradually. Bouveret et al. (2018) reiterate that this issue is a significant risk, as there have been several instances of criminals taking money from individuals utilising digital networks.

Conceptual theory

The theory of planned behaviour assumes that specific characteristics influence an individual's intention to engage in cybersecurity-based preventive actions (Alanazi et al., 2022). Factors that influence a person's behaviour towards cybersecurity include their attitudes, the social influence of subjective norms, and their perceived control over their actions, also known as self-efficacy and controllability. For instance, a person's perception of their ability to practice certain cybersecurity behaviours can impact their actual being (Dinc & Budic, 2016; Pankomera & Van Greunen, 2018).

Prior studies, Alanazi et al. (2022) and Prapavessis et al. (2015) confirm the extent to which individuals believe that their social context can affect their intention to change their behaviour toward compliance with cybersecurity. Kruger and Kearney. (2006) define attitude as a favourable or unfavourable evaluation of a particular behaviour—individuals' intentions to engage in a specific behaviour increase when they hold a favourable attitude towards it. In contrast, when individuals hold a negative attitude towards a particular behaviour, their intention to engage in that behaviour is reduced.

Khan et al. (2011) state that many interventions aimed at increasing information security awareness are based on the Knowledge Attitude and Behaviour (KAB) model, which focuses mainly on the knowledge aspect of individuals (Kruger & Kearney, 2006; Moletsane & Tsibolane, 2020; Nobles, 2018). The KAB model explains that as knowledge accumulates, it leads to a change in attitude and, ultimately, behavioural change (Haddad et al., 2018). In other words, knowledge plays a crucial role in behaviour change, as explained by the KAB model (Khan et al., 2011; Nobles, 2018). Taylor (2023) conducted a study that found that increasing the level of knowledge in cybersecurity and improving consumer behaviour when identifying high levels of privacy concern can reduce the perceived risk of cybercrime during banking transactions. Similarly, a study by Moletsane and Tsibolane (2020) found a significant relationship between students' knowledge and behavioural intentions about information security threats and their security awareness levels.

According to Alanazi et al. (2022) and Dinc and Budic (2016), subjective norm relates to how much the people around an individual either support or discourage a specific behaviour. Subjective norm refers to the extent to which digital banking consumers consider the opinions of others who are important to them and believe they must adopt the specific technology (Ajzen, 1991). Thus, more significant social influence is likely to increase an individual's intentions to change their behaviour toward cybersecurity (Butler, 2020 & Zhou et al., 2020). Researchers typically measure SN by asking participants to what degree they believe their closest relationships, such as family, friends, or colleagues, would encourage them to prevent or reduce data breaches (Alanazi et al., 2022).

Self-efficacy refers to the user's belief in their ability to carry out the required actions to avoid potential threats. In cybersecurity, this usually leads to the person taking the necessary steps to implement the security safeguards (Verkijika, 2020; Zhou et al., 2020). So, when consumers are sure they have the skills to protect their cybersecurity, they are highly motivated. This high motivation makes people act a certain way (Verkijika, 2020). Contrary, consumers with low self-efficacy may be less likely to put security measures in place because they often need help from people who are better at security (Mohanty & Patnaik, 2017). Accordingly, as it has been established that self-efficacy influences user behaviour (Butler, 2020), inaccurate perceptions of ability and efficacy can adversely affect user behaviour. This includes instances where users underestimate or overestimate their abilities.

According to Kruger and Kearney (2006), information security awareness is a dynamic process made more challenging by the constant evolution of threats. As a result, every awareness campaign must be continuously measured and managed to keep up with the evolution of risk profiles. To keep people informed and their memories fresh, any awareness programme must be ongoing and ingrained in the enterprise's culture (Vijayalakshmi et al., 2021). To maintain everyone's interest, the key to raising awareness is to keep the messaging current and constant while modifying the distribution modalities (Wodo et al., 2021). Changes in the information risk profile may affect both the delivery mechanism and the risk areas. Previous research by (McCormac et al., 2018) has explored the effect of resilience and job stress on information security awareness. Research has revealed that individuals with higher levels of resilience tend to exhibit greater Information System Awareness (ISA) and report lower levels of stress at work (McCormac et al., 2018). Individuals with higher levels of resilience showed significantly better knowledge, attitude, and behaviour (McCormac et al., 2018).

According to research (Nowrin & Bawden, 2018), consumers need to understand the relevance of security-related concerns that can influence their decisions when using mobile devices (smartphones, tablets) when transacting. According to (Das & Khan, 2016), the study aimed to determine how users' information security behaviours relate to their evaluation of security threats and their responses to them, as well as to comprehend their apprehensions regarding them. Previous research has asserted the need to follow mobile devices such as smartphones or tablet security behaviours to safeguard sensitive data (Saunders et al., 2019). The findings from this study will establish which of the following human factors (awareness, knowledge, attitude, subjective norm, self-efficacy and cybersecurity intention behaviour) has the highest predictive power for cybersecurity behaviour. Moreover, the study will develop a conceptual framework that can be used to explore human factors toward cybersecurity behaviour.

To resolve the problem for this study, the research question and objective were formulated as follows:
RQ1: Which factors influence digital banking consumers' cybersecurity behaviour?
*RO1: To explore behavioural insights into cybersecurity practices among digital banking consumers***.**

To support the investigation of the stated research questions, the following hypotheses were formulated:
H1: Consumers' attitude positively influences cybersecurity behavioural intention.
H2: Subjective norm positively influences cybersecurity behavioural intention.
H3: Self-efficacy positively influences cybersecurity behavioural intention.
H4: Cybersecurity behavioural intention positively influences cybersecurity behaviour.
H5: Self-efficacy positively influences digital banking consumers' cybersecurity behaviour.
H5: Knowledge positively influences digital banking consumers' cybersecurity behaviour.
H6: Attitude positively influences digital banking consumers' cybersecurity behaviour.
H7: Security awareness positively influences digital banking consumers' cybersecurity behaviour.

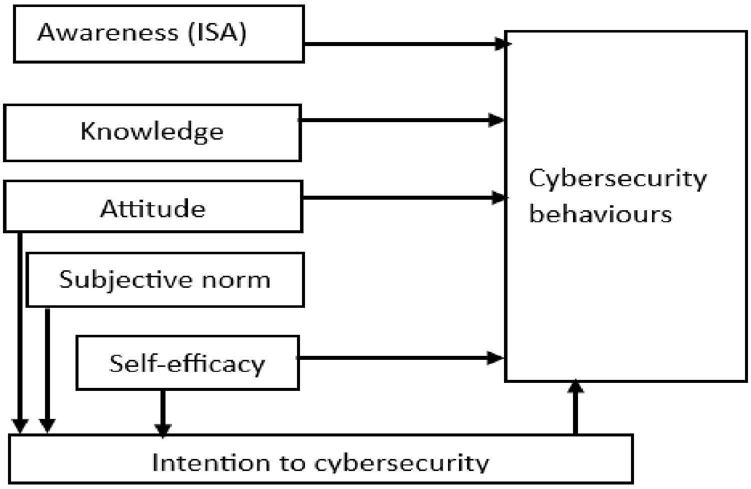

Figure 1: Conceptual framework

METHODOLOGY

This research employed a quantitative approach to investigate the relationship between dependent and independent variables. Several statistical methods outlined by (Saunders et al., 2019) were used. The research tool used was a survey instrument adapted from existing tools designed to assess cybersecurity awareness and the theory of planned behaviour (Alanazi et al., 2022; Farooq et al., 2019). The survey was divided into two parts. The first part aimed at collecting socio-demographic details such as age, gender, education level, and employment status. The study participants were highly representative of the population with bank accounts, thus ensuring the relevance of the findings to this group. The second part of the survey contained all the independent variables. A total of 338 questionnaires were returned and used for data analysis. In accordance with the practices of researchers like (de Vaus, 2013; Fincham, 2008), a response rate of 30% to 70% is considered acceptable for surveys, and this study fell within that range. To investigate the relationships between different variables in the proposed model, factor analysis and structural equation modelling (SEM) were employed. The software packages SPSS version 28, and AMOS version 28 were used for the data analysis.

RESULTS

Table 2 displays the participants' demographic details, such as their gender, age, marital status, province, gross income, and employment status. Of the total respondents, 179 were female, accounting for 55.4%. The largest age group of respondents, comprising 38%, was between 36 and 45 years old, while the majority (52%) possessed postgraduate degrees. Regarding income, 35% of respondents reported earning between R20 001 and R40 000. Additionally, most respondents (51.7%) were married, and 71.6% were employed.

Table 1. Demographic

Demographic characteristics		**Percentage (%)**
Gender	Male	45,6
	Female	55,4
Age	< 35	31.6
	36- 45	38.0
	55+	30.4
Marital Status	Single	43.2
	Married	51.7
	Separated/Divorced	5.1
Highest Qualifications	Undergraduate	48.0
	Postgraduate	52.0
Provinces	Gauteng	64.7
	Northwest	6.1
	Limpopo	13.1
	Mpumalanga	2.4
	Free State	2.4
	Eastern Cape	2.7
	Western Cape	7.3
	KwaZulu-Natal	1.2
Income	< R20 000	32.2
	R20 0001.00 – R40 000	35.0
	>R40 001.00	32.8
Employment	Employed	71.6
	Self Employed	10.1
	Unemployed	18.3

Confirmatory Factor Analysis (CFA) was conducted in this study to validate the constructs and their measurable indicators, following up on the Exploratory Factor Analysis (EFA). CFA is utilised to test EFA's findings and present visualisations and model fit assessments (Dash & Paul, 2021). Upon completion of the CFA, the final structural model, involving seven latent variables, was tested with the empirical data. CFA validates the measurement model, and Structural Equation Modeling (SEM) visualises the path analysis of relationships among the factors (Dash & Paul, 2021).

In the first step, when conducting factor analysis, Kaiser-Meyer-Olkin is used to assess the suitability of data. This involves computing Bartlett's test of Sphericity, correlation matrix, and determinant score to determine whether the data set is appropriate for functioning factor analysis. KMO values ranging from 0.8 to 1.0 indicate adequate sampling, while values between 0.7 and 0.79 are considered average, and values between 0.6 and 0.69 are below average. KMO values less than 0.6 suggest that the sampling is insufficient and remedial action may be necessary (Shrestha, 2021). According to (Shrestha, 2021), Bartlett's test of Sphericity is used to examine the null hypothesis that the correlation matrix is an identity matrix. A matrix of identity correlation indicates that the variables are unrelated and are, therefore, unsuitable for factor analysis. A statistically significant test (typically less than 0.05) demonstrates that the correlation matrix is not an identity matrix (rejection of the null hypothesis), as illustrated in Table 2. The KMO value of 0.896 indicated that the data were suitable for factor analysis, and Bartlett's test of Sphericity was significant (χ2 (11749.), p<0.001)

Table 2: KMO and Barlett's Test – Assessment of the suitability of the data

Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy		0.896
Barlett's Test of Sphericity	Approx. Chi-Square	11749.906
	df	210
	Sig.	0.000

Secondly, the results revealed that all 21 measured items were divided into six factors with eigenvalues greater than 1.0, representing 91.49 percent of the variance. The first factor explained 48.51 percent of the variance, below the benchmark value of 50.0 percent (Harman, 1976), ensuring that data was free from standard method bias (Hoque et al., 2017). This value is sufficient as it exceeds the minimum requirement of 60% (Hoque et al., 2017; Awang, 2012)

Table 3: Extraction Method: Principal Component Analysis

	Total Variance Explained: Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% Of variance	Cumulative %	Total	% Of variance	Cumulative %
1	10.188	48.513	48.513	10.188	48.513	48.513
2	2.519	11.997	60.510	2.519	11.997	60.510
3	2.249	10.710	71.220	2.249	10.710	71.220
4	1.563	7.442	78.662	1.563	7.442	78.662
5	1.526	7.268	85.930	1.526	7.268	85.930
6	1.169	5.567	91.497	1.169	5.567	91.497
7	.898	4.277	95.774			
8	.119	.566	96.340			
9	103	.492	96.831			
10	.093	.445	97.277			
11	.083	.396	97.672			
12	.073	.346	98.018			
13	.070	.334	98.352			
14	.063	.301	98.653			
15	.060	.284	98.937			
16	.056	.269	99.206			
17	.051	.243	99.449			
18	.046	.220	99.668			
19	.038	.183	99.851			
20	.019	.090	99.941			
21	.012	.059	100.000			

Lastly, the study used the rotation Varimax method (Kaiser (1958) created to decrease the number of variables with high loadings on each factor. Furthermore, Varimax aims to maximise the differences between a factor's squared pattern structure coefficients. The results in Table 4 indicate that Cybersecurity behaviour loaded onto Factor 1, followed by subjective norm and awareness, knowledge, cybersecurity behavioural intention, and self-efficacy. Subjective norm refers to the extent to which digital banking consumers consider the opinions of others who are important to them and who believe they must adopt the specific technology (Ajzen, 1991). If friends and family know the consequences of not complying with cybersecurity, they will raise awareness among digital banking consumers and change their behaviour toward cybersecurity. Thus, more significant social influence is likely to increase an individual's intentions to change their behaviour toward cybersecurity.

Table 4: Cross loading

	1	**2**	**3**	**4**	**5**	**6**
icb1				.903		
icb2				.902		
icb3				.891		
sbn1		.614				
sbn3		.615				
see1					.932	
see2					.929	
see3					.897	
csa1		.862				
csa2		.871				
csa3		.840				
kla1			.883			
kla2			.884			
kla3			.880			
att1						.838
att2						.841
att3						.847
cbi1	.916					
cbi2	.925					
cbi3	.914					

The results of testing the reliability and validity of the seven constructs are presented in Table 6. We used Cronbach's alpha and composite reliability to assess the latent construct's reliability. The table indicates that all constructs had high Cronbach's alpha values, ranging from 0.966 to 0.994, which exceeds the 0.70 threshold (Chai et al., 2015; Taber, 2018). These results meet the internal consistency requirements and support composite reliability, one dimensionality, and convergent validity. Table 5: Analysis of convergent validity and internal consistency validity.

Table 5: Depict construct reliability and convergent validity

Construct	Items	Factor loadings >0.5	Cronbach's alpha	Composite Reliability (CR) (.0.7	AVE= $\sum \lambda^2/n$ (>0.5)
ICB	icb1	.903	.974	.974	.926
	icb2	.902			
	icb3	.891			
SBN	sbn1	.614	.969	.970	.941
	sbn3	.615			
SEE	see1	.932	.971	.971	.918
	see2	.929			
	see3	.897			
CSA	csa1	.862	.966	.966	.906
	csa2	.871			
	csa3	.840			
KLA	kla1	.883	.994	.994	.983
	kla2	.884			
	kla3	.880			
ATT	att1	.838	.979	.979	.940
	att2	.841			
	att3	.847			
CB	cbi1	.916	.983	.983	.934
	cbi2	.925			
	cbi3	.914			
	cbi4	.914			

Furthermore, the discriminant validity of the constructs was tested (see Table 6). According to (Henseler et al. (2015), the relationships between shared variances among constructs and AVE values are compared (Hair et al., 2019). Table 6 depicts that all the correlations between constructs are less than the square roots of AVE values, which supports the discriminant validity of the constructs (Fornell & Larcker, 1981; Hair et al., 2019). Reliability and convergent and discriminant validity were acceptable.

Table 6: Discriminant validity

Construct	ICB	SBN	KLA	CB	SEE	ATT	CSA
ICB	**.962**						
SBN	.475***	**.970**					
KLA	.342***	.473***	**.991**				
CB	.379***	.403***	.429***	**.967**			
SEE	.452***	.383***	.277***	.367***	**.958**		
ATT	.410***	.410***	.610***	.480***	.307***	**.969**	
CSA	.449***	.586***	.512***	.413***	.3.83***	.505***	**.952**

The researcher tested the model fit using various indicators, and it was found to be satisfactory and within the acceptable limit recommended by (Hair et al., 2019). As illustrated in Table 7.

Table 7: Model fit measures

Chi-square/df	CFI	RFI	IF	PClose	SRMR	RMSEA
1.662	0.991	.971	0.991	0.844	0.0021	0.044

Table 8 summarises our research model fit, showing satisfactory results meeting the recommended levels. The Chi-square/df ratio was 1.675, GFI was 0.928, AGFI was 0.903, IFI was 0.990, NFI was 0.976, CFI was 0.990, and RMSEA was 0.045 (Chai et al., 2015; Hair et al., 2019). Furthermore, we used the coefficient of determination (R^2) to evaluate the proportion of variance explained by the research model; as suggested by Chin (1998), the value close to 0.67; 0.333 and 0.19 represents substantial, average, and weak explanatory power, respectively. The R-squared value for intention to cybersecurity behaviour (ICB) and behavioural cybersecurity behaviour (CB) is 0.317, respectively (. This means that all the predictor variables together explained 30.1% and 31.7% of the total variances of the endogenous variables.

Table 8: Final Structural model

Final Model Fit Summary			
Model Goodness-Fit Indexes	**Suggested cut-off**	**Result Model**	**Comments**
Chi-square		307.986	Significant
Chi-square/df	≤5.00	1.801	Significant
GFI	≥ 0.90	0.924	Significant
AGFI	≥ 0.90	.0900	Significant
NFI	≥ 0.90	0.974	Significant
CFI	≥ 0.90	0.988	Significant
IFI	≥ 0.90	0.988	Significant
TLI	≥ 0.90	0.986	Significant
RMSEA	≤0.08	0,045	Significant

Table 9 depicts the results of path coefficient and bootstrapping, illustrating that attitude (toward cybersecurity positively influences the digital banking consumers' cybersecurity behaviour intention (ICB) (β=0.202, t=3.618, p< 0.001), thus indicating that H1 is supported. Moreover, subjective norm (SBN) positively influences digital banking consumers' cybersecurity behaviour intention (ICB) (β=0.288, t=4.785, p<0.001), which proves that H2 is supported. Meanwhile, cybersecurity behaviour intention directly influences self-efficacy (β=0.180, t=2.817, p<0.005), which suggests that H3 is supported. Again, cybersecurity behaviour intention is significantly influenced by cybersecurity behaviour (β=0.111, t=2.068, p<0.005), which suggests that H4 is supported.

Knowledge ($\beta=0.128$, $t=2.089$, $p<0.037$), Attention ($\beta=0.252$, $t=4.011$, $p<0.001$) and Information security awareness ($\beta=0.163$, $t=3.189$, $p<0.001$) have direct influence on cybersecurity behaviour., H6, H7, H8 are supported. In contrast, self-efficacy has no direct relationship with cybersecurity behaviour ($\beta=0.110$, $t=1.797$, $p<0.072$, above $p>0.05$; thus, H5 was not supported.

Table 9: Hypothesis testing: Structural assessment

Hypothesis	Path	Beta (β)	SE	t-value	p-value	Decision
H1	ICB<--- ATT	.202	.064	3.618	***	Significant
H2	ICB<--- SBN	.288	.055	4.785	***	Significant
H3	ICB<--- SEE	.180	.054	2.817	0.005	Significant
H4	CB <--- ICB	.111	.050	2.068	0.039	Significant
H5	CB <--- SEE	.110	.048	1.797	0.072	Non-Significant
H6	CB<--- KLD	.128	.053	2.089	0.037	Significant
H7	CB <--- ATT	.252	.068	4.011	***	Significant
H8	CB <--- ISA	.163	.048	3.189	0.001	Significant

DISCUSSION

In the digital age, banking consumers are increasingly transitioning from traditional banking methods to digital platforms for convenience. Even though digital banking technologies are widely used, a significant need remains for enhanced security due to the high risk of cyberattacks. This study sought to identify the key factors influencing digital banking consumers' cybersecurity behaviours. Utilising the Theory of Planned Behavior (TPB) model, the research examined constructs such as subjective norms, behavioural intention, and self-efficacy, among others, and their impact on cybersecurity behaviours among a South African sample with bank accounts.

Analysis via Amos-Structural Equation Modelling (SEM) resulted in successful model evaluation. Results indicate that knowledge, attitude, and awareness correlate with cybersecurity behaviours, consistent with existing literature (da Veiga et al., 2022; Kruger & Kearney, 2006; Parsons et al., 2017). Studies by (Limna et al., 2023) also support these findings, suggesting that cybersecurity knowledge and awareness significantly influence digital consumer cybersecurity behaviour. The results further suggest that subjective norms significantly impact intention behaviour, in line with previous research ((Alanazi et al., 2022; Jang & Kim, 2022; Omidosu & Ophoff, 2017)).

Similarly, customers' opinions are found to be crucial in determining their commitment to cybersecurity measures, supporting previous literature highlighting the strong relationship between a person's attitudes and their willingness to engage in specific behaviours ((Ajzen & Fishbein, 1975; de Kok et al., 2020; Jang & Kim, 2022; Omidosu & Ophoff, 2017)). Consistent with earlier research, this study confirms that self-efficacy impacts a person's intention to practice cybersecurity ((Omidosu & Ophoff, 2017)). However, it does not affect security behaviours (Alanazi et al., 2022). Thus, some digital banking consumers may need to pay more attention to the complexity and time consumption associated with cybersecurity practices.

CONCLUSIONS AND RECOMMENDATIONS

Cybersecurity remains a pressing issue for financial institutions globally, posing intricate challenges that necessitate the active participation of digital banking consumers. Since banks house substantial quantities of personal data and transaction records, implementing robust cybersecurity measures, processes, and practices is paramount. As digitalisation progresses, hackers are increasingly zeroing in on the banking sector. Moreover, studies reveal that human factors often constitute the weakest link in the cybersecurity chain. In South Africa, the central banks hold 89% of the total assets within the banking sector, presenting a significant risk, according to the South African Reserve Bank (SARB, 2022).

Creating a comprehensive and effective cybersecurity strategy is critical to cater to the needs and expectations of digital banking consumers (Limna et al., 2023). Financial institutions can foster greater cybersecurity knowledge by enhancing individuals' understanding of personal ID-sharing risks and promoting awareness of the importance of cybersecurity. Promoting up-to-date software updates, educating consumers about social engineering threats, and imparting knowledge about general information security practices can enhance cybersecurity awareness, attitude, knowledge, and adherence to subjective norms. Regular assessments of computer systems for cyber vulnerabilities are also crucial for minimising harm risks. By actively managing their cybersecurity, digital banking consumers can safeguard their information and uphold the uncompromised performance of business operations.

FURTHER STUDY

While this study presents valuable findings, it has limitations. Most participants were from Gauteng province, which may limit the generalisability of the findings to other provinces or the overall South African population. Future research should include a more diverse sample to validate these findings further. Additionally, though this study utilised a self-administered survey for quantitative analysis, further qualitative research, such as interviews, observations, and focus groups, could provide more in-depth insights.

ACKNOWLEDGEMENTS

My sincere gratitude to my supervisor Prof. Richardson Shambare, thank you for your guidance.

REFERENCES

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, *82*(2). https://doi.org/10.1037/h0076477

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*. https://doi.org/10.1016/j.chb.2022.107376

Aldiabat, K., Al-Gasaymeh, A., & Rashid, A. S. K. (2019). The effect of mobile banking application on customer interaction in the Jordanian banking industry. *International Journal of Interactive Mobile Technologies*, *13*(2). https://doi.org/10.3991/ijim.v13i02.9262

Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). Cyber Security Threats on Digital Banking. *2022 1st International Conference on AI in Cybersecurity, ICAIC 2022*. https://doi.org/10.1109/ICAIC53980.2022.9896966

Bansal, K. M. (2020). *Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis*. *19*(4), 7724–7740. https://doi.org/10.17051/ilkonline.2020.04.765171

Bouveret, A., Christo, S., Gaidosch, T., Haksar, V., Kopp, E., Maino, R., Patnam, M., Rochon, C., Poirson-Ward, H., Stetsenko, N., Touré, A., Tiffin, A., Wilson, C., & Wiseman, K. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment Cyber Risk for the Financial Sector*.

Butler, R. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. In *Information and Computer Security* (Vol. 28, Issue 4, pp. 555–574). Emerald Group Holdings Ltd. https://doi.org/10.1108/ICS-01-2020-0016

Chai, J. C. Y., Malhotra, N. K., & Dash, S. (2015). The impact of relational bonding on intention and loyalty. *Journal of Hospitality and Tourism Technology*, *6*(3). https://doi.org/10.1108/jhtt-08-2014-0035

Chin, W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides(ed.), Modern methods for business research. In *Handbook of Partial Least Squares*.

da Veiga, A., Loock, M., & Renaud, K. (2022). Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. *Electronic Journal of Information Systems in Developing Countries*, *88*(1). https://doi.org/10.1002/isd2.12198

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*, *24*(1). https://doi.org/10.1108/ICS-04-2015-0018

Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, *173*. https://doi.org/10.1016/j.techfore.2021.121092

de Kok, L. C., Oosting, D., & Spruit, M. (2020). The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour. *Information & Security: An International Journal*, *46*(3). https://doi.org/10.11610/isij.4618

de Vaus, D. (2013). SURVEYS IN SOCIAL RESEARCH, 6th Edition. In *Surveys in Social Research, 6th Edition*. https://doi.org/10.4324/9780203519196

DINC, M. S., & BUDIC, S. (2016). The Impact of Personal Attitude, Subjective Norm, and Perceived Behavioural Control on Entrepreneurial Intentions of Women. *Eurasian Journal of Business and Economics*, *9*(17), 23–35. https://doi.org/10.17015/ejbe.2016.017.02

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public Perceptions of Cybersecurity: A South African Context. *Southern African Journal of Criminology*, *31*(3).

Farooq, A., Jeske, D., & Isoaho, J. (2019). *Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model*.

Fincham, J. E. (2008). Response rates and responsiveness for surveys, standards, and the Journal. In *American journal of pharmaceutical education* (Vol. 72, Issue 2). https://doi.org/10.5688/aj720243

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1). https://doi.org/10.1177/002224378101800104

Gomes, L., Deshmukh, A., & Anute, N. (2022). Cyber Security and Internet Banking: Issues and Preventive Measures. *Journal of Information Technology and Sciences*, *8*(2), 31–42. https://doi.org/10.46610/joits.2022.v08i02.005

Haddad, G. E., Shahab, A., & Aïmeur, E. (2018). Exploring User Behavior and Cybersecurity Knowledge - An experimental study in Online Shopping. *2018 16th Annual Conference on Privacy, Security and Trust, PST 2018*. https://doi.org/10.1109/PST.2018.8514190

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (2019). Multivariate Data Analysis, Multivariate Data Analysis. In *Book* (Vol. 87, Issue 4).

Harman, H. H. (1976). Modern factor analysis, 3rd rev. ed. In *Modern factor analysis, 3rd rev. ed.*

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1). https://doi.org/10.1007/s11747-014-0403-8

Hoque, A. S. M. M., Awang, Z., & Siddiqui, B. A. (2017). Technopreneurial Intention Among University Students of Business Courses In Malaysia: A Structural Equation Modeling. *International Journal of Entrepreneurship and Small & Medium Enterprise (IJSME)*, *4*(July).

Jang, J., & Kim, B. (2022). The Impact of Potential Risks on the Use of Exploitable Online Communities: The Case of South Korean Cyber-Security Communities. *Sustainability (Switzerland)*, *14*(8). https://doi.org/10.3390/su14084828

Jennings, J. E., Rahman, Z., & Dempsey, D. (2023). Challenging What We Think We Know: Theory and Evidence for Questioning Common Beliefs About the Gender Gap in Entrepreneurial Confidence. *Entrepreneurship: Theory and Practice*, *47*(2). https://doi.org/10.1177/10422587221102108

Kangapi, T. M., & Chindenga, E. (2022). Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa. *2022 IST-Africa Conference, IST-Africa 2022*. https://doi.org/10.23919/IST-Africa56635.2022.9845633

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, *5*(26), 10862–10868. https://doi.org/10.5897/ajbm11.067

Khrais, L. T. (2015). Highlighting the vulnerabilities of online banking system. *Journal of Internet Banking and Commerce*, *20*(3). https://doi.org/10.4172/1204-5357.1000120

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

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

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security*, *26*(3), 277–289. https://doi.org/10.1108/ICS-03-2018-0032

Moletsane, T., & Tsibolane, P. (2020). Mobile Information Security Awareness among Students in Higher Education : An Exploratory Study. *2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings*. https://doi.org/10.1109/ICTAS47918.2020.233978

Ncubukezi, T. (2022). *Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses*.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Nohumba, I., Nohumba, I., & Nyambuya, G. (2020). Integrating offline and online platforms for seamless banking experience. *Journal of Management & Administration*, *1*(I).

Nowrin, S., & Bawden, D. (2018). Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh. *Information and Learning Science*, *119*(7–8), 444–455. https://doi.org/10.1108/ILS-04-2018-0029

Omidosu, J., & Ophoff, J. (2017). A theory-based review of information security behavior in the organization and home context. *Proceedings - 2016 3rd International Conference on Advances in Computing, Communication and Engineering, ICACCE 2016*. https://doi.org/10.1109/ICACCE.2016.8073752

Pankomera, R., & Van Greunen, D. (2018). Challenges, Benefits, and Adoption Dynamics of Mobile Banking at the Base of the Pyramid (BOP) in Africa: A Systematic Review. *The African Journal of Information and Communication (AJIC)*, *21*. https://doi.org/10.23962/10539/26113

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*. https://doi.org/10.1016/j.cose.2017.01.004

Quiroz, J. T., Oscategui, M. A. A., & Armas-Aguirre, J. (2021). Cybersecurity Taxonomy: Research and knowledge areas. *Proceedings of the 2021 IEEE 1st International Conference on Advanced Learning Technologies on Education and Research, ICALTER 2021*. https://doi.org/10.1109/ICALTER54105.2021.9675075

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). Chapter 4: Understanding research philosophy and approaches to theory development. In *Research Methods for Business Studies* (Issue March).

Sheth, A., Bhosale, S., & Kurupkar, F. (2021). *A Research on Process of Interaction Between Business Intelligence (BI) and SMES View project*. https://www.researchgate.net/publication/352477690

Shrestha, N. (2021). Factor Analysis as a Tool for Survey Analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), 4–11. https://doi.org/10.12691/ajams-9-1-2

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information (Switzerland)*, *13*(9). https://doi.org/10.3390/info13090413

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, *48*(6). https://doi.org/10.1007/s11165-016-9602-2

Taylor, P. (2023, January 18). *Number of smartphone users in South Africa from 2014 to 2023 (in millions)*. Statista. https://www.statista.com/statistics/488376/forecast-of-smartphone-users-in-south-africa/

Verkijika, S. F. (2020, November 25). Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. *2020 2nd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2020*. https://doi.org/10.1109/IMITEC50163.2020.9334097

Vijayalakshmi, P., Priyadarshini, V., & Umamaheswari, K. (2021). IMPACTS OF CYBER CRIME ON INTERNET BANKING. *International Journal of Engineering Technology and Management Sciences*, *5*(2). https://doi.org/10.46647/ijetms.2021.v05i02.005

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Wodo, W., Blaskiewicz, P., Stygar, D., & Kuzma, N. (2021). Evaluating the security of electronic and mobile banking. *Computer Fraud and Security*, *2021*(10), 8–14. https://doi.org/10.1016/S1361-3723(21)00107-X

Zainuddin Hj Awang. (2012). Research Methodology and Data Analysis Second Edition. In *UNIZA.Press*.

Zhou, G., Gou, M., Gan, Y., & Schwarzer, R. (2020). Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01066