PERCEIVED INFLUENCE OF CYBERSECURITY ON THE INTENTION TO USE MOBILE BANKING APPLICATIONS.

A Masters Research thesis presented to
The Department of Information Systems
University of Cape Town

By

Ishmael Chikoo

CHKISH003

Supervisor: Assoc Prof Salah Kabanda

in partial fulfilment of the requirements of the INF5005W
Information Systems Course

17 January 2020

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this INF5005W thesis from the work(s) of other people attributed and has been cited and referenced.
3. This INF5005W thesis is the researcher's work.
4. I have not allowed, and will not allow, anyone, to copy this work to pass it off as his or her own work.
5. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is our own work.
7. I acknowledge that part of this work was covered in my management summary, Literature review and Research design submissions of my thesis.

Signature: Signed by candidate

Date: 24 July 2019

Name: Ishmael Chikoo (CHKISH003)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Banking institutions see the adoption and usage of mobile devices for banking namely mobile banking as an innovative financial service delivering strategy that bridges the gap between customers and banks. Mobile banking eliminates the need to visit bank branches for banking services and it eliminates the need to only perform banking services within fixed business hours. In mobile banking, mobile devices such as a cellphone, smartphone, or tablet' are used to conduct non-financial and financial transactions such as checking account status, transferring money, making payments, or selling stocks. Mobile banking is suggested to take over the banking sector because it is economising and timesaving benefits.

Despite these benefits, the adoption rate amongst consumers remains low, especially in developing countries where there is a knowledge gap in understanding why consumers do not engage in the frequent use of mobile banking applications. Apart from several factors identified in previous literature on mobile banking as influencers of limited usage and adoption of mobile banking, trust remains an important factor in the intention to adopt or use mobile banking applications. Also, because of the increasing prevalence of cyber threats in developing countries, the influence of cybersecurity is still questionable on their influences on the intention to adopt or use mobile baking applications. The increase in cyber threats and attacks has birthed the need for cybersecurity to be addressed. Given that most financial institutions see mobile banking as a strategy for their competitive advantage; it is important that they understand how best to address consumer's fears brought about by cybersecurity threats. Literature has not covered more ground on the analysis of mobile banking applications (Uduimoh., Osho., Ismaila, & Shafi'i, 2019). The purpose of this study is to investigate the perceived influence of cybersecurity on the user's intentions to use mobile banking applications.

The study identified seven salient cybersecurity factors that influence the intention to use mobile banking applications. These cybersecurity factors were grouped into two groups, namely intrinsic factors and extrinsic factors and resulted in the development of a conceptual model. With this model, hypothesises were developed and tested statistically using quantitative data from an online self-administered Qualtrics survey questionnaire. Data collected from 90 participants was statistically analysed in Smart PLS 3 (a quantitative data analysis software). Structural Equation Modeling (SEM) and Partial Least Squares path modelling approaches were adopted for data analysis.

Hypothesis testing was performed on salient factors that influence the perception of cybersecurity on the intention to use mobile banking applications. The findings concluded that salient significant factors that influence the perception of mobile banking cybersecurity on the intention to use mobile banking applications were perceived data confidentiality and cybersecurity awareness. As a result, the study concluded that one's perception on ability to avert cybersecurity threats and attacks, how they perceived the protection of their data from being modified by unauthorised users, how they perceive their data to be kept confidential and their knowledge of cybersecurity from legitimate sources influences their intention to use mobile banking applications. Finally, this study investigated the empirical evidence of the knowledge gap concerning the perceived influence of cybersecurity on the intention to use mobile banking applications.

CHAPTER 1: INTRODUCTION

1.1. Background to the study

Exponential growth in mobile banking, mainly due to technological advancement, has caused a drastic change in the way most businesses deliver their products or services to their targeted and current customers (Sun, Sun, Liu, & Gui, 2017). The adoption and usage of mobile banking technology as a business strategy and as a tool to expand the market reach is the current and future objective of both financial and non-financial firms in both developing and developed countries (Yu, 2012). Mobile banking as a business strategy implies the ability to deliver financial services to reach the banked and unbanked population via cyber internet connections (Tunay, Tunay, & Akhisar, 2015). As a result, banks are maximising the use of mobile banking devices as a strategy to expand the market to reach the unbanked population without the time and geographical constraints (Martins, Oliveira, & Popovič, 2014).

Many studies have explored mobile banking adoption and usage (Govender & Sihlali, 2014 ; Maduku, Mpinganjira, & Duh, 2016; Nasri & Charfeddine, 2012; Sharma, Govindaluri, Al-Muharrami, & Tarhini, 2017). However, according to He, Tian, and Shen (2015), there is still lack of systematic discussion in the literature about the security risks with mobile banking applications. In addition, SMS banking has been the main mobile banking researched area in developing countries and virtually the influence of security on mobile banking applications via portable devices and smartphones has not been broadly addressed (Shaikh, A. A., & Karjaluoto, 2015). Significant factors that influence the adoption and usage of mobile banking have been identified to include, amongst others trialability, complexity, compatibility, observability and relative advantage (Govender & Sihlali, 2014; Sharma et al., 2017). One factor that has not been extensively explored is cybersecurity and how it influences the user's intention to adopt mobile banking technologies (Martins et al., 2014). Mobile banking security threats and attacks are increasing to date and technology users are at risk. As a consequence, the adoption and usage rate of mobile banking applications, specifically in developing countries, have not reached the industrial expected usage and adoption level (Yao & Zhong, 2011; Joubert & Van Belle, 2013) and the overall usage of mobile banking is perceived to be below the assumed and predicted usage rate (Joubert & Van Belle, 2013). Even though security risk as an influence towards in mobile banking use and utility is well researched (Njenga and Ndlovu, 2013), according to He, Tian, and Shen (2015), there is still lack of systematic discussion in the literature about the security risks with mobile banking applications. In addition, SMS banking has been the main mobile banking researched area in developing countries and virtually the influence of security on mobile banking applications via portable devices and smartphones has not been broadly addressed (Shaikh & Karjaluoto, 2015). Literature has not covered more ground on the analysis of mobile banking applications (Uduimoh., Osho., Ismaila, & Shafi'i, 2019). With this background, the purpose of the study is to explore how cybersecurity influences the user's intention to adopt mobile banking applications. Specifically, the focus is on exploring the perceived influence of cybersecurity on the intention to use mobile banking applications in a developing country context.

1.2. Research problem

The advancement of technology has birthed an exponential growth in the usage of mobile technology; businesses are migrating to delivering their products and services via the usage of mobile devices (Sun

et al., 2017). The banking sector has adopted the usage of mobile devices for business and service delivery to its customers, and it is called mobile banking (Sharma et al., 2017). Mobile banking is a strategy to expand the financial service delivery market and means to reach the unbanked population, remotely and without time constraints (Sun et al., 2017). Mobile banking implies the delivery of financial and non-financial services to customers via telecommunication channels on mobile devices (Govender & Sihlali, 2014; Sharma et al., 2017; Tunay et al., 2015). Banks have recorded an increase in the development of mobile applications for mobile banking service delivery to reach both the banked and unbanked population (Martins et al., 2014).

Despite these advantages of increased market reach without the time and geographical constraints, the adoption and usage of mobile banking have not been fully embraced by customers (Joubert & Van Belle, 2013; Yoon & Steege, 2013). Martens, Roll, and Elliott (2017) stated that the usage of mobile devices for banking have limited acceptance. The rate of diffusion towards the adoption of mobile banking was stated as lower than the expected technology adoption rate (Arif, 2016). The rate of adoption and usage of mobile devices for banking has not reached the expected industrial rate, and customers still use the traditional banking way of visiting bank branches to have face-to-face financial and non-financial banking services fulfilment (Arif, 2016; Yao & Zhong, 2011). Customer behaviour and perception towards technology adoption and usage were found as a contributing factor towards the limited use of mobile banking (Arif, 2016). Yoon and Steege (2013) found website usability, openness and users' perception of security concern as influencers for usage. However, there exists a knowledge gap in understanding the influence of technology users' security perception on why consumers do not engage in the frequent use of mobile banking applications.

Among the other factors that influence the adoption and usage of mobile technology, specifically in mobile banking, is trust due to the cybersecurity challenges presents in online environments. Security and privacy were found as customer perspective barriers towards the adoption of mobile banking (Karjaluoto, Riquelme, & Rios, 2010). A global increase in cybercrime, cyber threats and cyber-attacks (Kim, Kim, & Park, 2015; Mbelli & Dwolatzky, 2016), has birthed questions about the influence of cybersecurity on the intention to adopt or use mobile banking applications (Martins et al., 2014). Cybersecurity is the protection of data, or users' cyber environment against any misuse, illegal access, unauthorised manipulation of resources involved in cyberspace (Balzacq & Cavelty, 2016; Stallings, Bauer, & Hirsch, 2013). Cybersecurity was observed as an essential factor in the adoption of mobile banking (Balzacq & Cavelty, 2016; Joubert & Belle, 2013). Mujinga, Eloff and Kroeze (2016) concluded that security remained a major inhibitor for cyberbanking and noted technology users' perceptions of security as a potential contributor.

As a result, cyber threats and attacks have birthed the need to investigate the role played by the perception of security on the intention to use mobile banking applications by investigating the influence of perceived cybersecurity on the intention to use mobile banking applications. Addressing fears that can be brought by cybersecurity on mobile technology users is an important strategy to understand how best to address trust issues and consumer's fears that influence the intention to use mobile banking applications. This study is focused on investigating the perceived influence of cybersecurity on the intentions to use mobile banking applications in a developing country context.

1.3. Research goal and research question

The goal of this study is to explore the perceived influence of cybersecurity on the intention to use mobile banking applications in a developing country context. On this basis, the question that the study seeks to investigate is "To what extent does cybersecurity influence the intention to use mobile banking applications?"

1.4. Structure of the thesis

This chapter introduces the literature review. The literature review will present the previous background literature on mobile banking, cybersecurity and the theoretical approach to the study. The next chapter after the literature review is chapter 3, which presents for the methodology. Under the methodology, the philosophy, choice of methods, purpose of the study and the research strategy for the study is presented. Sampling method found for the study, data collection method, research quality discussion, projects plan, and instrument used to collect data are also part of chapter 3. The methodology ends with the ethical consideration for the study, which explains the influence of ethics for this study and how the study considered ethics.

Findings and discussion of the study are presented in Chapter 4. The last chapter of the study is chapter 5, which presents the conclusion, provides a summary of the study, research contributions and limitations for the study. The study ends with the reference list and appendixes.

CHAPTER 2: LITERATURE REVIEW

2.1 Background

The previous chapter provided the background to the study – outlining the research goal and objectives. This chapter presents the theoretical background and leads to a conceptual model that will guide the rest of the study. Related scholarly works on the study phenomenon of mobile banking and associated applications are discussed.

The rest of the chapter is organised as follows: first, the mobile banking arena will be presented, leading to section 2.3 that outlines the cybersecurity aspects of mobile banking. Then, section 2.4 discusses the factors that influence the adoption of mobile banking applications and leads to the development of a conceptual framework. Section 2.5 summarises the chapter.

2.2 Mobile banking

Mobile banking as an application of mobile commerce 'refers to an interaction in which a customer is connected to a bank through a mobile device such as a cellphone, smartphone, or tablet' (Laukkanen, 2017,p. 1042) to conduct transactions such as checking account status, transferring money, making payments, or selling stocks (Shaikh & Karjaluoto, 2015, p. 131). This interaction has the potential to accelerate the delivery of financial services via mobile telecommunications carriers and in so doing, offer several benefits such as true freedom from time and place, and efficiency for banking transactions (Assensoh-Kodua, Migiro, & Mutambara, 2016; Laukkanen, 2017, p. 1042). As a result, most banking institutions see mobile banking as an innovative financial service delivering strategy that bridges the gap between customers and banks (Sun et al., 2017). Mobile banking bridges the gap between customers and banks by eliminating the need to visit geographical bank branches and eliminating the time bound of banks that operate within fixed business hours as per traditional banking (Paulo, Rita, Oliveira, & Moro, 2018; Sun et al., 2017). Most scholars see the primary goal of mobile banking as the need to meet customers' financial and non-financial needs remotely and without time constraints (Hayikader, Nurafiqah, Hadi, & Ibrahim, 2016).

Despite the benefits associated with mobile banking, the adoption rate amongst consumers remains low, especially in developing countries (Yao & Zhong, 2011). Legner, Urbach, and Nolte (2016) noted that even companies had found it challenging to implement mobile applications successfully and to gain user acceptance. Although this is partly due to the availability of other banking service channels, there remains limited understanding as to why consumers do not engage in the frequent use of mobile banking applications in developing countries. Earlier studies such as Alalwan, Dwivedi, and Rana, (2017), have shown that consumer's behavioural intention is significantly and positively influenced by performance expectancy, effort expectancy, hedonic motivation, price value and trust. Tran and Corner (2016) found that the most significant influential factor of usage intention was perceived usefulness, followed by perceived credibility and perceived costs. Their findings show that face-to-face communication with bank staff and close acquaintances was perceived as the most reliable and persuasive sources of banking-related information. The implications are that trust remains an essential factor in the intention to adopt or use mobile banking, especially with the increasing prevalence of

cyber threats 'from attackers, spammers, and criminal corporations' in developing countries that tend to be shaped by a security landscape characterised by (Kabanda, Tanner, & Kent, 2018, p. 270):

> (1) poor "security hygiene," i.e., the degree to which it runs with up-to-date software patches and recent malware protection; (2) unique usage patterns not commonly seen in the developed economies such as reliance on mobile technology for conducting financial transactions even in places where credit cards and the web have not penetrated; (3) novice users who have joined the Internet and do not have exposure to the risks posed online and disseminating security educational material and tools is extremely challenging; (4) the use of pirated software which may not necessarily pose as a security risk, but challenging to verify that such software is not malicious; and (5) limited understanding on the adversaries' of cybersecurity.

Given that, mobile banking involves the exchange of sensitive data in cyberspace; there is need to protect data transferred via telecommunications channels belonging to both service providers and technology users (Martins et al., 2014). It is therefore important that service providers such as financial institutions who see mobile banking as a strategy for their competitive advantage understand how best to address consumer's fears brought about by cybersecurity threats.

2.3 Cybersecurity

Hackers are advancing and becoming more sophisticated in breaching confidential data transferred between devices and platforms via telecommunication channels (Cavusoglu, Mishra, & Raghunathan, 2018). Doing business in the cyberspace via telecommunication networks raises the need for businesses to address cybersecurity, especially in the light of the increase in cyber attacks and the inability to identify cyberattackers - the most significant risk associated with the business in cyberspace (Kader & Minnaar, 2015). He, Tian, and Shen (2015) provide an in-depth review of the security aspect of mobile banking applications. They note mobile malware such as Trojans, rootkits and viruses as one of the security threats, which 'are kept refined by cybercriminals to target mobile devices for access to bank accounts and make them more resilient to security defences' (3) for example mobile banking applications. These fake banking applications or application updates contain malicious codes to steal users' bank account information. Another security threat associated with mobile banking applications is unencrypted Wi-Fi networks, which allow cybercriminals to eavesdrop and steal sensitive information. He et al. (2015) also identified the vulnerability of mobile banking apps as a form of security threats because cybercriminals can analyse the source code to steal account information and other sensitive information. With these mobile banking security threats, there is a need for organisations and individuals to engage in cybersecurity protective practices.

Cybersecurity is the protection of data, organisation or users' cyber environment against any misuse, illegal access, unauthorised manipulation of resources involved in cyberspace (Balzacq & Cavelty, 2016; Stallings et al., 2013). Nambiro Alice, Wabwoba, and Wasike (2017, p. 134) identified several challenges facing organisations in developing countries with regards to cybersecurity associated with mobile banking. They identify inadequate technical skills; the lack of awareness from all parties involved on cybersecurity threats; legislation that is not mature to address cybersecurity threats; low prioritisation from national leaders on cybersecurity; poor technical design; and social engineering practices.

An empirical survey study on technical staff about skills profile found that there exists a significant shortage of technical skills which ultimately affects service delivery (Van Der Waldt, Fourie, Jordaan, & Chitiga-Mabugu, 2018). Nambiro et al. (2017) agree that a lack of technical skills has an impact on cybersecurity.

Lack of awareness of cybersecurity was another critical issue that plays a significant role in the intention to use technology because the more the customers are aware of the dangers involved in cybersecurity, the more they can become proactive in using technology (de Bruijn & Janssen, 2017). Apart from the awareness of cybersecurity, the immaturity of legislature plays a significant role in cybersecurity (Nambiro et al., 2017). Lack of critical, thorough, documented ways and laws to govern cybersecurity and control cyber-attacks has an open room for cyber attackers to get away with serious cyber-attack offenses (Nambiro et al., 2017). In addition, technical tools have proved to be insufficient because the human factors have a significant influence in security a safe cyber business environment (Eastin, Brinson, Doorey, & Wilcox, 2016).

Awan et al. (2017) identified cybersecurity defense strategies to include setting up cyber-crime and protection policies and competence; increasing cyber flexibility; collecting cyber intelligence and acting against criminals as defined under predefined international cyber law; offering training programmes to cyber personnel and cyber military; increasing global unions in cyber environment; and establishing policies, strategies for international cyberspace. With these security measures, cybersecurity is a costly exercise, especially for developing countries who tend to have fewer resources, to ensure business continuity, disaster recovery, costs associated with the installation of security features on business devices and expenses to cover losses resulting from cyber-attacks (Balzacq & Cavelty, 2016; Stallings et al., 2013). The cost of cyber-attacks and data breaches are exponentially growing. As a result, the security breaches is negatively associated with cyber service providing firms market value (Cavusoglu et al., 2018). It is, therefore, crucial for both practitioner and scholars, to see cybersecurity as an essential factor in mobile banking (Kim et al., 2015).

2.4 Development of a conceptual model

A range of factors usually influences consumer's adoption and use of any innovation. According to de Almeida, Lesca, and, Canton, (2016), two factors motivate an individual decision to engage in an activity or event: intrinsic and extrinsic factors. While intrinsic factors are ingrained, extrinsic factors are external motivators. Figure 1 presented the proposed model and explained in the subsequent sections that follow.

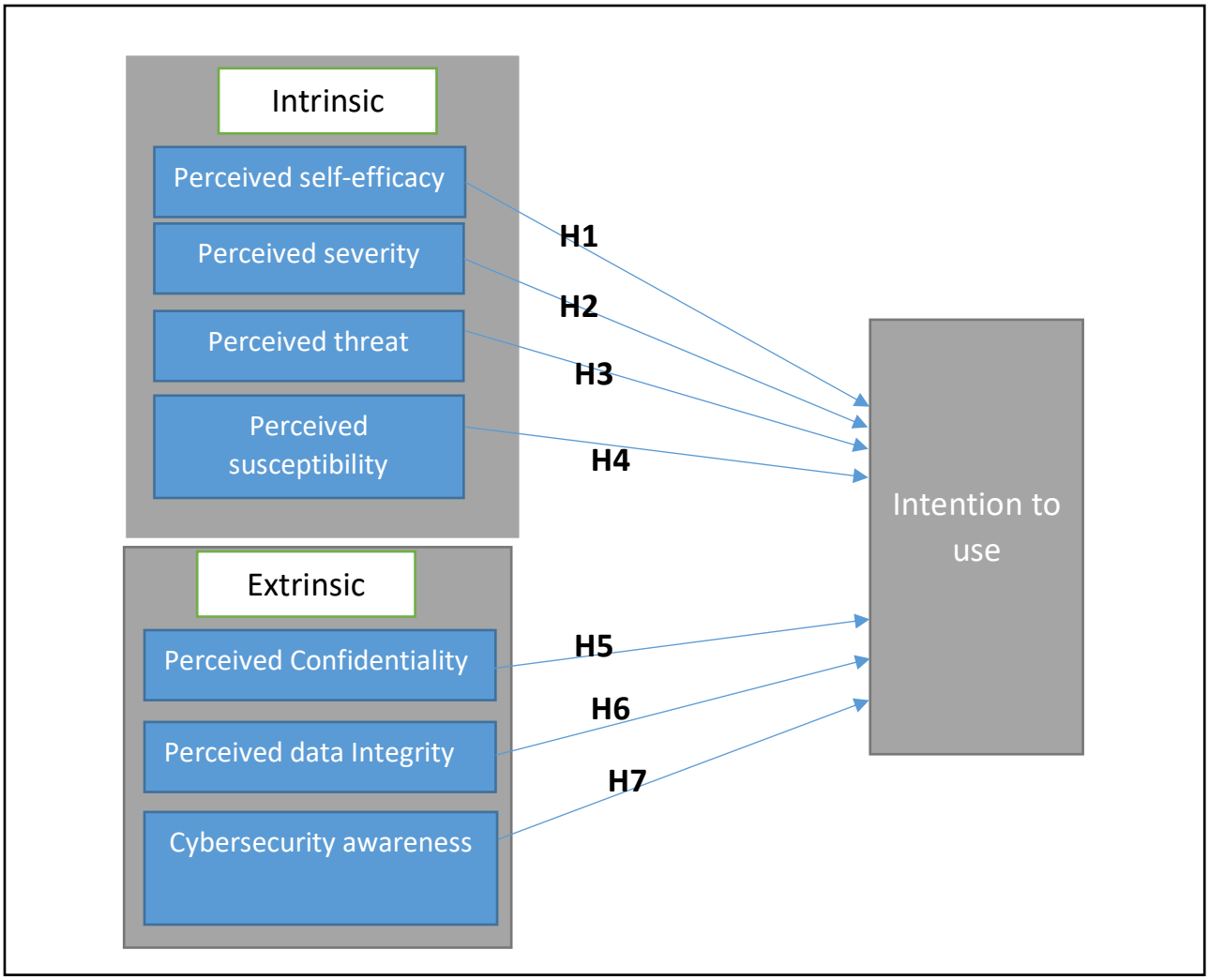

Figure 1: Conceptual model

Intrinsic factors

a) Perceived self-efficacy

Cudjoe, Anim, and Tetteh Nyanyofio, (2015) see self-efficacy as the 'judgments of how well one can execute courses of action which is required in dealing with prospective situations' (p. 7). This is a necessary construct to consider in mobile banking due to the 'novel kind of self-service banking technologies requiring the customer to conduct financial transactions by himself and away from any support of banking staff' (Alalwan, Dwivedi, Rana, Lal, & Williams, 2015). Most studies have found a positive relationship between technological experience and the effects, which it has on computer usage (Cudjoe et al., 2015). For example, Abayomi et al. (2019) and Makanyeza (2017) found that self-efficacy is a crucial factor to consider when adopting mobile banking services in Nigeria and Zimbabwe, respectively.

In South Africa, Maduku et al., (2016) found that high familiarity with the mobile medium, increases self-efficacy in its use, eliminating the importance of complexity in determining behavioral intention.

Self-efficacy tends to have a generally positive impact on willingness to adopt and continuance intention to use (Koksal, 2016; Thakur, 2018). It, therefore, follows that the higher the level of perceived self-efficacy, the greater the level of motivation that users have to practices security measures (Yoon, Hwang, & Kim, 2012). The perceived ability to perform recommended protective measures in order to avert security threats, influence the intention to use mobile banking technologies. On this note, this study hypothesize that:

Hypothesis H1: *Perceived self-efficacy influences the intention to use mobile banking applications.*

b) Perceived severity

Perceived severity implies one's internal perception of the seriousness of dealing with a prospective situation (Chen & Cheng, 2017). Perceived severity can be explained as the magnitude of economic, psychological or physical harm that is anticipated from a threat or any prospective situation (Hajian, Shariati, Mirzaii Najmabadi, Yunesian, & Ajami, 2015). Lawson et al. (2016) see perceived severity as the perceived degree of harm that can result from security threats and or attacks in the context of cybersecurity. In mobile banking, perceived severity implies the implicit perception of the magnitude of harm that can result in the use of mobile baking technology (Alexandrou & Chen, 2019). Understanding the degree to which people perceive the seriousness of security in mobile banking applications is suggested to reveal the influence cybersecurity on mobile banking applications intention to use.

Perceived severity in mobile banking covers the degree of perceived loss or cost that is associated with the use of mobile banking technology (Alexandrou & Chen, 2019). The negative effect of the prospective situation triggers fear (Hajian et al., 2015). In mobile banking, fear is mostly associated with the financial loses that can result because of cyber-attacks and threats to an individual or a business. In a risk information avoidance study, Deline & Kahlor (2019) stated that the concept of assessing the likelihood of being harmed by a prospective situation has a central effect in danger perception. The more an individual perceive being harmed or negatively affected by a potential situation, the more they can avoid the prospective situation perception of being (Deline & Kahlor, 2019). Perceived severity has a high effect on the user's plan of actions and can influence their intention to use mobile banking technologies (Lin & Bautista, 2016). As a result, this study posits the following hypothesis:

Hypothesis H2: *Perceived severity influences the intention to use mobile banking applications.*

c) Perceived Threat

The more advanced technology becomes, the higher the risk of threats in the cyberspace. In mobile banking, the traditional banking strategy of visiting physical bank branches for banking services during office hours is no longer relevant in a digital era (Sun et al., 2017). The banking sector has become the fastest growing sector in technology adoption and usage because of a highly competitive market share (Farah, Hasni, & Abbas, 2018). Despite the more secureness of traditional banking because of direct contact between bank tellers and bank stakeholders with customers, traditional banking is losing market growth (Zhou, 2018). Banks are migrating to remote service delivery through the usage of technology (Lawson, Yeo, Yu, & Greene, 2016). However, despite the significant advantage of reaching the unbanked population remotely and timeously for service delivery through the usage of technology, remote banking involves cyber-attacks and threats (Malaquias & Hwang, 2016). The usage

of technology for remote business processes is highly associated with cyber threats (Wazid, Zeadally, & Das, 2019).

Perceived threat implies the assumed magnitude of uncertainty that can be experienced by an individual when facing a specific situation or stimulus (Alexandrou & Chen, 2019). Cyber threats are mostly anonymous remote attacks targeting devices and infrastructure used for cyber business processes (Mbelli & Dwolatzky, 2016). In banking, perceived threat implies cyber uncertainties perceived by technology users when using technology for business processes, for example, when processing financial transactions (Wazid et al., 2019). There exists a negative correlational relationship between perceived threats and mobile banking usage (Baptista & Oliveira, 2015). Khedmatgozar and Shahnazi, (2018) defined mobile banking threats as risks and categorised threats involved in mobile banking into six groups, namely performance, financial, time, and social, privacy and psychological risk. Performance risks or threats are uncertainties associated when the expected outcome of technology usage is not effectively mating (Njenga & Ndlovu, 2016). Financial risks or threats are uncertainties that involve monetary loss when using intended services. Time risks or threats are uncertainties that include loss of time when using services. The psychological risk or threats involve users' uncertainty of peace of mind and emotions that can negatively affect the usage of mobile banking services. The social risk or threats involve adverse effects that are tied to service usage that involves social setting negative influences and perceptions. Privacy risk or threats involve the loss of personal data when using services (Khedmatgozar & Shahnazi, 2018). The higher the level of perceived threat, the less the user's and potential users' intent to use technology (Jansen & van Schaik, 2018). With this background, this study hypothesize that:

Hypothesis H3: *Perceived threat influences the intention to use mobile banking applications.*

d) Perceived susceptibility

Perceived susceptibility is the degree to which one feels likely to be in the danger of the prospective situation being communicated (Lawson et al., 2016). In an internet security perception and behaviour investigation, Chen and Zahedi, (2017) stated that perceived susceptibility implies technology users' internal view about the magnitude of being vulnerable to cyber or online security attacks. Perceived susceptibility has been studied in varies fields of study, for example, in Health Sciences (Seitz et al., 2018), social studies (Olofsdotter, Åslund, Furmark, Comasco, & Nilsson, 2018) and several others.

Information systems studies have investigated perceived susceptibility on its influence on technology usage (Alexandrou & Chen, 2019; Awan et al., 2017). In information systems, perceived susceptibility implies the degree to which a user views the probability of negatively affected by the threat associated with the usage of technology (Marafon, Basso, Espartel, de Barcellos, & Rech, 2018). Alsaleh, Alomar, and Alarifi (2017) concluded that a misperception of security susceptibility by smartphone users influences their desire to take preventive security actions. In a cybersecurity behaviour study, Awan et al. (2017) stated that there is a direct relationship between perceived susceptibility and technology user's security behaviours. The higher the level of perceived susceptibility of security, the less users are motivated to use technology.

Lawson et al. (2016) concluded that there is a direct influence between the technology user's perception of being in a harmful state and magnitude of fear being perceived. Lawson et al. (2016) study focused on the impact of the usage of fear appeals as a tool for security. Understanding one's

susceptibility to cybersecurity issues exposes current and potential threatening cybersecurity issues in a given population (Hadlington & Chivers, 2019). The higher the perceived susceptibility in the form of a high degree of being affected by security attacks, the higher the intention to use (Marafon et al., 2018). The more vulnerable technology users feel concerning the usage of technology, the less likely they will intend to use technology. This study, therefore, hypothesize that:

Hypothesis H4: *Perceived susceptibility influences the intention to use mobile banking applications.*

Extrinsic factors

a) Perceived data confidentiality

Perceived data confidentiality implies humans' perceived belief about how their data will be kept confidential and only shared with agreed upon parties (Bertino & Ferrari, 2018; Stallings et al., 2013). In mobile banking, data shared between customers and banking services providers via telecommunication channels must be kept confidential (Donovan, 2014). The protection of customer's information is one of the significant challenges faced by banks when doing business in the cyberspace (Mbelli & Dwolatzky, 2016). Soomro, Shah, and Ahmed (2016) stated that the advancement of technology implies more data shared in cyberspace. As a result, data breaches have become a very critical concern for doing business in cyberspace or via telecommunication networks. Breach of confidential data in both small and large organisations has caused millions of US dollars in the UK (Soomro et al., 2016). Loss of data confidentiality can be because of cyber data being stolen or disclosed to unauthorised parties (Bertino & Ferrari, 2018). In mobile banking applications usage, the confidentiality of data involves how sensitive data can be kept confidential between service providers, customers and sometimes third parties involved in business processes (Ohk & Park, 2016).

Wazid et al. (2019) alluded data confidentiality as a crucial mobile banking security requirement. Loss of data confidentiality influences user's behaviour towards technology intention to use. Misperception of data confidentiality can reduce the level of trust between technology users and online service providers, and that influences the intention to use technology (Stallings et al., 2013). Confidentiality of data tends to have a generally positive impact on the intention to use technology (Thakur, 2018). It, therefore, tails that the higher the perceived level of data confidentiality in mobile applications using the greater the desire to use technology (Akram, Chen, Lopez, Sauveron, & Yang, 2018). Stewart and Jürjens (2018) concluded that it is crucial to address data confidentiality in order to increase users confidence in financial technology or mobile banking (Stewart & Jürjens, 2018). On this note, this study hypothesise that:

Hypothesis H5: *Perceived data confidentiality influences the intention to use mobile banking applications.*

b) Perceived data integrity

Perceived integrity of data implies the guarantee that data in transit between two or three parties cannot be modified by unauthorised entities (Stewart & Jürjens, 2018). Data integrity involves timeously delivery of data in an accurately desired format (Yu, Balaji, & Khong, 2015). In mobile banking, transactional or general service data is shared in the cyberspace for mobile banking services and the data must be kept inaccessible from unauthorised parties to avoid data breach (Ohk & Park, 2016). Hackers or unauthorised third parties can modify or alter transactional data or personal data that is exchanged for business process in cyberspace for their gains (Zissis & Lekkas, 2012). Cyber attackers target unprotected entry points associated with technology usage such that they can modify

data being transmitted in order to gain more access to more sensitive data (Wazid et al., 2019). Bojjagani and Sastry (2017) proposed cryptography as a solution to satisfy data integrity requirements in technology usage. However, despite the usage of technical tools like cryptography, the perception of how data will be collected and used by technology users is an area of concern to many scholars (Eastin et al., 2016).

Technology users need the assurance that their data will remain accurate, unmodified and trustworthy while in transit and while stored on applications (Wazid et al., 2019). Yu, Balaji, and Khong, (2015) stated that the more technology users have confidence in the integrity of their data used for online banking, the more they develop a positive attitude towards the intention to use technology. As a result, technology users with high-perceived data integrity are most likely intended to use mobile baking application. Thus, this study proposes that:

Hypothesis H6: *Perceived data integrity influences the intention to use mobile banking applications.*

c) *Cybersecurity awareness*

Despite the usage of advanced technical tools and controls as a strategy to handle cyber threats and attacks, organisations and individuals are increasingly affected by security breaches (McCormac et al., 2017). The human factor of cybersecurity has become the central and source of most organisational and individual security breaches (Öłütçü, Testik, & Chouseinoglou, 2016). Cybersecurity awareness implies the degree to which technology users or potential users are knowledgeable on the uncertainties tied to the adoption or usage of technology (Bada, Sasse, & Nurse, 2019). Cybersecurity awareness advocates for technology users to be aware of the threats and the impact that is involved in technology usage (Öłütçü et al., 2016).

In a study focusing on building cybersecurity awareness, de Bruijn and Janssen (2017) stated that the less informed technology users are on cybersecurity issues can lead to reckless technology usage behaviour, which can cause serious security breaches. Bendovschi (2015) alluded that cybersecurity awareness is a countermeasure to handle cyber-crime, beginning with individual level awareness to international cybersecurity awareness. Lack of awareness of cyber security attacks or threats can expose potential users to security breaches that can result in substantial financial loses (van Schaik et al., 2017). To address the cybersecurity awareness issue, Alexandrou and Chen (2019) suggested that educational programs could be implemented in order to educate users on most likely security threats as a significant strategy to minimise human causes of security breaches.

In mobile banking, cybersecurity awareness involves addressing technology users about security threats and attacks associated with technology used for banking and the preventions and procedures that can be followed to ensure secure transaction processing and data protection (Heemskerk, Caws, Marais, & Farrar, 2015). The more informed technology users are with the right information about cybersecurity, the more likely they will desire to use mobile banking (Li, Xu, He, Chen, & Chen, 2016; van Schaik et al., 2017). Cybersecurity awareness tends to have a generally positive impact on the intention to use technology (Korpela, 2015; Öłütçü et al., 2016). The awareness of cybersecurity influences technology intention to use. On this note, this study hypothesise that:

Hypothesis H7: *Cybersecurity awareness influences the intention to use mobile banking applications*

2.5 Summary

Technology advancement has birthed an exponential growth in the day-to-day usage of mobile technology for business (Sun et al., 2017). Mobile banking applications are the emerging innovative business strategy utilised by banks for mobile banking. However, research on cybersecurity as a limiting factor for mobile banking has not been well understood. The purpose of this study, therefore, is to explore how cybersecurity influences the user's intention to adopt mobile banking applications. In this chapter, related work on previous studies on mobile banking and cybersecurity was presented, and this helped to arrive at conceptual model illustrated in Figure 1. According to the model, intrinsic factors of perceived self-efficacy, perceived threat, perceived susceptibility and perceived severity and extrinsic factors of perceived data integrity, perceived data integrity and cybersecurity awareness, influence one's perception in adopting mobile banking applications.

CHAPTER 3: METHODOLOGY

This chapter presents the research methodology that guided the study. The methodology presents procedures used to gather, select and analyse the data. The chapter is organised as follows: In Section 3.1, the philosophical stance of the researcher and the approach to theory development is presented. Next, the research strategy for the study and the sampling method used to select study respondents is presented. Section 3.3 and Section 3.4 present data collection procedures and data analysis. Section 3.5 will present the quality procedures the research adhered to. Finally, Section 3.6 discusses ethical considerations. Then, Section 3.7 presents the ethical considerations for the study. The last section for the chapter presents a summary of the methodology.

3.1 Philosophy and approach

Philosophical stances and understanding are crucial for every researcher in evaluating certain assumptions about the nature of human knowledge. There are three philosophical assumptions or ways in which data about a phenomenon can be gathered, analysed and used, namely epistemology, ontology and ontology (Bhattacherjee, 2012; Rotolo et al., 2016). The choice of a philosophical assumption to adopt depends on the nature of research and the researcher's stance in philosophical assumptions (Rotolo et al., 2016). The current study adopts a positivistic research paradigm to allow the exploration of cybersecurity and mobile banking as a social phenomenon without being part of and being influenced by the emergent social realities of the research respondents.

The study is deductive, as literature from previous studies informed the development of the conceptual model that guided the research. With a positivistic stance and a deductive approach towards theory development, this study sees quantitative method as a good fit. Quantitative research methods have been successfully adopted and used in previous mobile banking adoption studies (Arif, 2016; Makanyeza, 2017; Shaikh & Karjaluoto, 2015). Quantitative research methods tend to "seek regularities in human lives, by separating the social world into empirical components called variables which can be represented numerically as frequencies or rate, whose associations with each other can be explored by statistical techniques, and accessed through researcher-introduced stimuli and systematic measurement." (Payne & Payne, 2004, p. 180).

3.2 Research strategy and sampling

This study adopted a survey strategy. According to Singh and Srivastava (2014), a survey using questionnaires allows the standardisation and aggregation of findings. As a result, a survey in the form of a questionnaire was distributed online to reach true representatives of individuals with some commonality remotely. Since this study focused on South African mobile devices users, the ability to remotely distribute the questionnaire online is advantageous as smartphones can connect to the internet. The study questionnaire can reach mobile users in different provinces in South Africa; hence, the study can be generalised to the South African population. Further, surveys are economical in terms of time and cost because of the ability to remotely distribute online, and surveys are suitable for this cross-sectional time framed study (Bhattacherjee, 2012). In information systems research, the use of survey instruments for positivist research is the norm and accepted method to collect research data (Church & Waclawski, 2017). A survey has several advantages as a data collection tool. For example,

research hypotheses can be tested from data collection, the relationship between constructs and constructs items can be evaluated numerically, and they are easy to distribute for general responses (Church & Waclawski, 2017). The researcher is not ignorant of the biases that are associated with survey research strategy, for example, chances of no responses, or social undesirability. Non-responses were not considered for data analysis to minimise the biasedness of data.

3.3 Data collection

The research instrument used as part of the online questionnaire consisted of two main sections – Section A and B. Section "A" covers general user demographic related questions, and Section B covers questions on research constructs derived from Figure 1. To ensure the validity of the instrument, the researcher formulated questions for each construct using pre-validated questions from previous mobile banking and cybersecurity studies. Constructs and their measuring item or research questionnaire questions are shown in appendix 1. The measure for each construct was based mostly on previous research papers (Akturan & Tezcan, 2012). Perceived severity factor was included four items from Akturan and Tezcan (2012) and Chen (2013). To investigate the perceived influence of cybersecurity awareness on the intention to use, five items from Al-omari and El-gayar (2012) were adopted. A copy of the questionnaire used for the study is shown in appendix 2.

A five-point Likert Scale was applied with 5 - implying Strongly Agree, 4 - implying Agree, 3 - implying Neither Agree nor Disagree, 2 - implying Disagree and 1 - meaning Strongly Disagree was adopted for the questionnaire answers. The respondents could determine and indicate their attitude towards constructed research questions by choosing how they strongly disagree or agree to the question using a Likert scale (Singh & Srivastava, 2014). The instrument for the study was pre-tested using a pilot study. The questionnaire was distributed by email to twenty respondents in the Department of Information Systems at the University of Cape Town. The purpose of pre-testing was to reduce ambiguity, grammatical errors and other self-hidden mistakes. Feedback from pre-test respondents was considered and validated if fit for the study. No modifications were suggested from the pilot study, and the instrument proved to be reliable and valid.

A Qualtrics online survey questionnaire was purposively distributed heterogeneously to potential mobile banking users on Facebook, LinkedIn and Twitter and link to the questionnaire was purposefully send to South African based respondents in the researcher's contacts list. The internet protocols (IP) addresses for technology used to access the questionnaires were recorded to avoid people from filling the questionnaire multiple times. All recorded IP addresses were checked and verified to remove duplicates and ensuring data validity.

3.4 Data analysis

Data analysis began after data collection. Numeric data from online Qualtrics survey questionnaire was exported as numerical values in CSV file format that was imported into SmartPLS 3 for data analysis. The researcher made sense of the data, which included data cleaning and deletion of anomalies based on valid research agreed principles. Data accuracy was conducted through excel data checking formulas and data validation. Invalid entries were identified, checked, and necessary changes were effected. Data collected and checked was saved as an excel workbook.

Partial Least Squares - Structural Equation Modeling (PLS-SEM) method was adopted for data analysis. SEM is a non-parametric data analysis method that used to analyse data without the need for

data to meet a certain distributional assumptions (Hair, Hult, Ringle, & Sarstedt, 2017). PLS-SEM uses a nonparametric bootstrap procedure to assess the significance of various statistical results such R^2 values, path coefficients and several others (Sanchez, 2013). Hair et al. (2017) supported the use of SEM to test the relationship between independent research variables and research dependent variables. Byrne (2013) and Yu (2014) supported the use of SEM to investigate how the latent variables relate. Also, Arif (2016) adopted SEM on their quantitative study to investigate the resistance of mobile banking in a developing country; hence, the current quantitative study in a developing country adopts SEM to test hypotheses and the goodness of fit of the conceptual model for the study. SEM adds its tremendous flexibility in specifying models of substantive interest (Hair et al., 2017) to the study which increases data analysis accuracy. Bryrne (2013) stated that SEM is more appropriate in order to verify constructed hypothesis of the study and also the frame work's validity, hence suitable for the current study.

Independent variables for the study are categorised into a) Intrinsic factors: perceived self-efficacy, perceived severity, perceived a threat, and perceived susceptibility; and b) extrinsic factors: perceived data confidentiality, perceived data integrity, and cybersecurity awareness. Extrinsic and Intrinsic factors were tested on how they influence the intention to use mobile banking applications through hypothesis testing method. The extrinsic and intrinsic factors formulated the inner and outer model of the conceptual model presented in Section 2.4.

SEM supports studies that adopt a positivistic philosophical (Hair et al., 2017), hence suitable for this current positivistic study. In information systems, SEM has been adopted by several studies (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014; Hair et al., 2017). Partial Least Squares (PLS) SEM known mostly as PLS Path Modelling was used to assess the difference in variance between dependent and or independent variables (Hair et al., 2017; Rönkkö, McIntosh, Antonakis, & Edwards, 2016). PLS-SEM a non-parametric method used to assess and test the significance in the relationship between the dependent and or independent variables (Sanchez, 2013). PLS-SEM is suitable for theory testing (Hair et al., 2017). Path coefficients, R^2 values, Cronbach's alpha and other various PLS-SEM result, a nonparametric procedure called bootstrapping was adopted to test for research data statistical significance (Hair et al., 2017). A normality test was carried out to determine the

In bootstrapping, the original set of data is randomly observed as subsamples to estimate the PLS path model (Rönkkö et al., 2016). Bootstrapping follows a process of randomly drawing subsamples from the data set until a large number of subsamples is created and observed to determine PLS-SEM results. The results from the bootstrapping of subsamples were observed to determine standard errors of PLS-SEM results. As a result, the significance of PLS-SEM results was assessed by observing p-values, t-values and confidence intervals from the subsamples bootstrapping process (Hair et al., 2017).

3.5 Research quality

There are four categories used to assess the validity of one's research: (i) authenticity, (iii) transferability, (iii) dependability and (iv) creditability (Saunders et al., 2016). Dependability evaluates the trustworthy of data considered for the research and the appropriateness and consistency of the research results to be considered acceptable (Saunders et al., 2016). No data alteration occurred in data collected for research. Authenticity implies the ability to ensure that research data is protected from unethical manipulations during or before data analysis while ensuring that information is processed, as it is (Saunders, Thornhill, & Lewis, 2015). The researcher ensured that data was not manipulated in

order to suit expected results by using original research data for all tests. Data variables were tested for internal validity using statistical tests. Constructs triangulation and other principals were applied to ensure the internal validity of research constructs (Saunders et al., 2016). External validity implies the same principals, as transferability. The researcher will allow generalizability of finding and the use of scholarly language.

3.6 Ethical consideration

For ethical reasons, the researcher applied for ethics from the University of Cape Town. The ethics process requires that a cover letter and consent form be attached to allow respondents to voluntarily agree or decline to participate in the study. To guarantee participants anonymity, the researcher did not collect participants personal details. Data collected from research participants were not exposed to third parties and cannot be shared with third parties unless participants agree (Manhas & Oberle, 2015). To ensure confidentiality, the research questionnaire was not tracking personal information of participants, and the researcher declared assurance of confidentiality in the consent form. The researcher ensured that participants agreed with the confidentiality and anonymity of their data by accepting to proceed with the study after reading the consent form.

CHAPTER 4: FINDINGS AND DISCUSSION

4.1 Introduction

The purpose of this study was to investigate the perceived influence of cybersecurity on the intention to use mobile banking applications. To achieve this, a survey instrument was designed and administered online to mobile users. Ninety mobile users participated in the study. Table 1 shows the demographic status of 90 mobile users that participated in the study.

Demographic Factor	Item	Number of respondents	Percentage
Age	<25 years 25<=Age<= 30 30< Age<= 40 >40	31 30 26 3	34% 33% 29% 3%
Gender	Male Female	55 35	61% 39%
Employment Status	Fulltime Part-time Student Not employed	51 8 29 2	57% 9% 32% 2%
Owning a smartphone	Yes No	89 1	99% 1
Region	Western Cape Eastern Cape Free State Gauteng KwaZulu-Natal Limpopo Mpumalanga	63 1 1 18 3 2 2	71% 1% 1% 20% 3% 2% 2%

Table 1: Participants demographic status

Most mobile user respondents (34%) were of the age 25 and below, as shown in Table 1. The second highest was the age group between 25 and 30 years, at 33%. The third most significant age group category was the age group between 30 and 40 years, with 29 %. The last and smallest value was those above age 40 with 3% of total respondents. The implications are, therefore, that the majority of respondents (97%) were under the age of 25 to the age of 40. Male respondents were the majority with 61%, while female respondents had a percentage of 39%.

Most of the respondents (66%) were employed (either full time or part-time). 32 % of respondents were students, and only 2% were unemployed. 90% of the respondents own a smartphone, implying they have a probability of installing mobile baking applications in their phones. Majority of

respondents were from Western Cape (71 %) of the total number of respondents, followed by Gauteng (20%).

In summary, the demographics show that the majority of respondents were below the age of 40, mostly male and were relatively fully employed. An average respondent owned a smartphone and resided in the Western Cape Province.

4.2 Outer model assessment findings

The relationship between independent variables and their measuring items was defined as the outer model of the conceptual model developed in Section 2.5. The outer model was assessed by testing the internal consistency of dependent variables or exogenous variables of the study. The convergent reliability of the outer model was assessed by investigating discriminant validity, and the average variance explained, including the assessment of the construct's item reliability as previously adopted in a quantitative study that focused on investigating perceptions of senior management towards their behaviour on information sharing (Yoon & Steege, 2013). The previously discussed assessment methods for the outer model were also suggested as valid tests for a quantitative study by previous studies (Byrne, 2013; Hair et al., 2017).

Internal consistency reliability assessment

Testing for the consistency of the items (indicators) of conceptual model variables is very crucial to validate the reliability of each construct (Hair et al., 2014). Reliability implies the measure of consistency and or dependability of the conceptual model's constructs (Bhattacherjee, 2012; Saunders et al., 2016). Internal consistency reliability of constructs for this study was assessed by observing, Cronbach's Alpha, Dillon-Goldstein's (rho_A) and 1st Eigenvalues after running a complete bootstrapping in Smart PLS (Alexandrou & Chen, 2014; Hair et al., 2017).

Studies stated that the observation of Dillon-Goldstein's rho (rho_A) as a valid test to test the internal consistency reliability of conceptual model's constructs (Hair et al., 2014; Sanchez, 2013). This study observed Dillon-Goldstein's rho (rho_A) to test for the internal consistency reliability of constructs. Dillon-Goldstein's rho value is a statistical test to evaluate the internal consistency reliability of data, which implies an evaluation of constructs the best fit (Sanchez, 2013).

A complete bootstrapping was performed to evaluate the internal consistency of constructs in Smart PLS (Hair et al., 2014). A complete bootstrapping is a nonparametric statistical analysis procedure that is used to test the significance of path coefficients by observing R^2 values, rho_A, Cronbach's alpha, and other resulting values in SMART PLS (Hair et al., 2017). After running a complete bootstrapping in SMARTPLS, the observed statistical significance values for the internal consistency and reliability of constructs are as shown in Table 2.

Construct	Cronbach's Alpha	Dillon-Goldstein's (rho_A)	1st Eigenvalues
Cybersecurity awareness	0.809	0.845	2.18
Intention to use	0.701	0.763	1.54
Perceived data confidentiality	0.898	0.975	3.07
Perceived susceptibility	0.891	0.958	3.02
Perceived threat	0.935	0.990	3.97
Perceived data Integrity	0.912	0.928	3.70
Perceived severity	0.873	0.921	2.91
Perceived self-efficacy	0.907	0.911	3.66

Table 2: Internal reliability test results

The lowest rho_A was 0.763 that of intention to use and the highest rho_A was 0.99 that of perceived threat. According to Hair et al. (2017), the accepted rho_A value is 0.7 and above. As a result, with the observed rho_A values ranging between 0.763 and 0.990 for the study, all constructs passed the internal constructs consistency reliability test. The results agreed with Hair et al. (2014), who stated that a rho_A value higher than or equals to 0.7 of a construct implies that items of the construct are consistent with each other.

The other observed significant values were Eigenvalues (Sanchez, 2013). Eigenvalues are statistical significance values that are observed to measure the unidimensionality of the model in order to verify the internal consistency reliability of constructs (Arif, 2016; Hair et al., 2014). The acceptable threshold of greater than or equal to 1 for eigenvalues represents good internal consistency reliability (Falissard, 2011). The observed first eigenvalues for this study ranges from 1.54 to 3.97, and that is above the threshold of greater or equal to 1, which indicated that internal consistency reliability was good.

Cronbach's alpha is another statistical significance value used to measure the reliability of constructs (Hair et al., 2014). Cronbach alpha was observed to assess the internal consistency reliability of constructs (Hair et al., 2014). Cronbach alpha of value greater than 0.7 is acceptable for internal consistency reliability of the outer model (Hair et al., 2014). On the other hand, an alpha value of 0.6 is also acceptable for exploratory studies as agreed by Henseler, Hubona, and Ray (2016), and Hair et al., (2014). According to results shown in Table 2, Cronbach alpha values greater than 0.7 were observed hence, according to Hair et al., (2014) and Ketchen (2013), the internal consistency reliability of the outer model for the study is reliable.

The results for rho_A, Eigenvalues and Cronbach's alpha implies that the internal consistency of the constructs was reliable. As a result, the model did not have unidimensionality.

Constructs items reliability assessment

The previous section focused on assessing the reliability of constructs in relationship to each other. In this section, the focus is on assessing the relationship between items of each construct to each other and how they are related to items of other constructs.

The reliability of constructs items or indicators was assessed by observing the outer loading of the model from the SmartPLS bootstrapping run test. Constructs Items reliability is valid if the absolute loading of the exogenous latent variable items is greater than 0.7 (Henseler, Ringle, & Sarstedt, 2014). The observed absolute outer loadings for each construct items loaded higher than 0.7, as shown in appendix 5; hence, construct items are reliable. No indicators were removed since all 32 outer loadings for items were above 0.7; therefore, the results approve that the items are reliable as supported by Hair et al. (2014). The results implied that items for each construct truly represent the construct.

Discriminant validity test

In this section, the assessment of the discriminant validity for constructs will be explained. Discriminant validity or divergent validity is a test used to assess if there is truly no relationship on the constructs that are not supposed to be related (Hair et al., 2017). A complete bootstrapping was run in SmartPlS, and the cross loading of constructs items was observed as a means to test for the discriminant validity of the construct's items, (Hair et al., 2014). Cross-loading asses' discriminant validity by expecting items or indicators of a construct to load higher together on their construct than they can do on other constructs or latent variables (Arif, 2016; Hair et al., 2014). Cross-loadings for constructs were observed to load higher together on their construct than they loaded on other constructs, as shown in appendix 4. Cross-loading results showed that measures of different constructs were distinct.

Another measure of discriminant validity used is the Fornell-Larcker criterion (Hair et al., 2017). Fornell-Larcker criterion assesses' discriminant validity by ensuring that for each construct, its squared correlation value is above its squared correlation values on other constructs (Fornell & Larcker, n.d.; Hair et al., 2017). Table 3 shows discriminant validity results presented by the squared correlation values of each construct.

Fornell-Larcker Criterion								
	Cybersecurity Awareness	**Intention to Use**	**Perceived Data Confidentiality**	**Perceived Susceptibility**	**Perceived Threat**	**Perceived data Integrity**	**Perceived severity**	**perceived Self-efficacy**
Cybersecurity Awareness	**0.849**							
Intention to Use	0.572	**0.875**						
Perceived data confidentiality	-0.123	-0.087	**0.870**					
Perceived susceptibility	-0.037	-0.176	0.519	**0.865**				
Perceived threat	-0.162	-0.215	0.447	0.567	**0.889**			
Perceived data integrity	-0.040	-0.195	0.544	0.495	0.486	**0.858**		
Perceived severity	0.028	-0.065	0.318	0.223	0.133	0.059	**0.852**	
Perceived self-efficacy	0.046	0.187	-0.117	-0.019	-0.104	-0.062	0.016	**0.855**

Table 3: Fornell-Larcker criterion test results

All latent variables have squared correlation values that are above their squared correlation values on other exogenous latent variables. According to Fornell-Larcker criterion, if the squared correlation value of each construct's items is above its squared correlation values on other constructs, the items of the constructs are more related to their construct than to other latent variables items (Hair et al., 2014; Henseler et al., 2014), hence, the observed results passed the discriminant validity test.

Convergent validity test

The previous section focused on the assessment to check if constructs that are supposed to be different are truly different. In this section, the convergent validity test, which implies the test on assessing if theoretically related constructs have measures that truly represent the assumed relationship (Hair et al., 2017) was applied. If the measure of two constructs corresponds to each other, convergent validity is established. The Average Variance Explained (AVE), and Composite Reliability was used to test for the convergence validity of the construct's items (Arif, 2016; Hair et al., 2014). The AVE evaluates the resultant variance based on the influence of measurement error on the construct's captured variance (Henseler et al., 2014). An AVE greater than 0.5 proves that a construct's convergence validity is sufficient (Arif, 2016; Hair et al., 2014). Table 4 shows the results for convergent validity test.

Construct	Composite Reliability (CR)	Average Variance Extracted (AVE)
Cybersecurity Awareness	0.885	0.720
Intention to Use	**0.866**	**0.765**
Perceived Data Confidentiality	0.926	0.757
Perceived Susceptibility	0.922	0.748
Perceived Threat	0.949	0.790
Perceived data Integrity	0.933	0.737
Perceived severity	0.913	0.725
Perceived Self-efficacy	0.931	0.731

Table 4: Convergent validity assessment (CR and AVE) results

The lowest AVE value was 0.72 that of Cybersecurity Awareness and the highest AVE value was 0.935 that of Intension to use, as shown in Table 4. The minimum accepted value of AVE for a valid convergent validity test is 0.7 (Hair et al., 2014). The observed AVE values for this study are all above 0.7. Hence according to Hair et al. (2014) and Henseler et al. (2014), all constructs passed the convergent validity test. As a result, all items of each construct have measures that truly represent that they are related.

Composite reliability is another way to assess how well the construct items correlate within the construct (Hair et al., 2014). Literature has recommended composite reliability for PSL approach when applying the structural equation modeling to assess the overall reliability of heterogeneous items of a construct that are similar that just observing Cronbach alpha coefficients (Arif, 2016; Hair, 2014; Hair et al., 2017) Composite reliability values greater than 0.7 implies an acceptable composite reliability value (Hair et al., 2014). Results shown in Table 4 proves that constructs pass convergent reliability test since the highest composite value is 0.949 that of the perceived threat and the minimum value of composite reliability is 0.866, that of cybersecurity awareness hence all composite reliability values were above the minimum required value of CR greater than or equal to 0.7 criteria.

Normality test

The normality for the study was test normality as a preliminary undertaking for understanding how to treat data was not carried out by observing the skewness and kurtosis of a bootstrapping results from SmartPLS run. The observed normality test was 0.95, as a result, since it ranges between 2 and -2 (George & Mallery, 2010), the results implies that data distribution was normal (Reinartz, Haenlein, & Henseler, 2009). This is especially so in determining the structural equation model of data and for the model to be believable.

In summary, the observed outer model proved to have valid internal consistency reliability implying that items (indicators) of conceptual model variables are reliable. All variables had observed rho_A values above the acceptable rho_A value of 0.7 (Hair et al., 2017). The resultant eigenvalues for all variables ranged between 1.54 and 3.97, and that was above the accepted threshold of greater or equal to 1 (Falissard, 2011) to indicate good internal consistency reliability. All variables had Cronbach alpha values greater than 0.7; hence, according to Hair et al., (2014), the internal consistency reliability was valid. The indicators for each variable was reliable since the resultant outer loadings for each

construct's items loaded higher than expected thresh hold of greater than or equal to 0.7 (Arif, 2016 Hair et al., 2017). Measures of different constructs were distinct since the observed cross-loading results showed that cross-loadings for constructs were observed to load higher together on their construct than they loaded on other constructs. The resultant AVE values were greater than the minimum accepted value of AVE of greater than or equal to 0.7 (Hair et al., 2014). Also, the resultant values of CR were all greater than the minimum expected value of 0.7 (Arif, 2016; Yoon & Steege, 2013), implying that all attempts to measure the same constructs agreed.

According to Rönkkö et al., (2015) the outer model assessments (internal consistency reliability, indicator reliability, discriminant validity and convergent validity assessments) proved that the outer model or the relationship between constructs and their indicators is valid and reliable since all tests were successful. As a result, the outer model is significant for the study.

4.3 Inner model assessment findings

The previous sections focused on assessing the validity of the outer model or the relationship between independent variables with their items. This section presents the relationship between the dependent variable (intention to use) and independent variables (perceived self-efficacy, perceived severity, perceived a threat, perceived susceptibility, perceived data confidentiality, perceived data integrity, and cybersecurity awareness) of the conceptual model defined in section 2.5. The relationship between the dependent variable and independent variables of the conceptual was defined as the inner model of the conceptual model. The assessment of the relationships between independent variables and the dependent variable of the inner model enabled the researcher to address and answer the questions through hypothesis testing (Arif, 2016; Hair et al., 2013). The coefficient of determination, path coefficient and model goodness of fit (Hair et al., 2017), were statistically tested in SmartPLS 3 using data collected from online questionnaires to assess the inner model of the proposed conceptual model.

The coefficient of determination (r^2)

The coefficient of determination evaluation is a measure to evaluate the inner model of the proposed conceptual model's hypothesised relationships (Hair et al., 2017). The coefficient of determination (R^2) predicts the variability in one latent variable and how the variation of a different latent variable can explain it (Hair et al., 2014). R^2 value ranges between 1 and 0; the closer the value of R^2 is to 1, the more accurate the constructs can predict variability (Hair et al., 2017). The coefficient of determination values below 0.190 are considered very weak, the coefficient of determination values between 0.333 and 0.670 is interpreted as moderate and, R^2 values greater than 0.670 are considered perfect predictive accuracy (Hair et al., 2014). Table 5 shows the resultant value of R^2 after running a complete bootstrapping in SmartPLS.

Dependent variable	**Coefficient of Determination (R^2)**
Intention to Use	0.414

Table 5: Coefficient of determination result

Observed coefficient of determination was 0.414 for the relationship between the dependent variable (intention to use) and independent variables (perceived self-efficacy, perceived severity, perceived susceptibility, perceived threat, cybersecurity awareness, perceived data confidentiality, and perceived data integrity), as shown in Table 5. According to Cangur and Ercan, (2015), and Hair et al., (2014), the model has a valid predictive accuracy for predicting future outcomes. As a result, the inner model

is valid based on the coefficient of determination assessment since the dependent variable proved to be predictable from the independent variables. The results agreed

The model's goodness of fit test

The goodness of fit test was conducted to assess the inner model's best fit. According to Arif (2016), Byrne (2013) and Hair et al (2017), Goodness-of-Fit Index (GFI), Root Mean Square Error of Approximation (RMSEA), Normed Fit Index (NFI), Adjusted Goodness-of-Fit Index (AGFI), Tucker-Lewis Index (TLI), Comparative Fit Index (CFI) and Normed Chi-square (CMIN/DF) can be observe to measure the model fitness. In Smart PLS only Standardized Root Mean Square Residual (SRMR), Exact fit criteria (the squared Euclidean distance (d_ULS) and the geodesic distance (d_G)), Chi-Square and Normed Fit Index (NFI) (Hair et al., 2017) were observable after running a complete bootstrapping in Smart PLS 3 version used by the researcher. NFI is a model fit test proposed by Bentler and Bonett (1980). NFI compares the chi-squared computed value of the proposed model and compares it with the benchmark (Hair et al., 2017). However, NFI is not a recommended fitness test since it does not cater the model's complexity and is an incremental fit measure (Lohmöller, 1989); this study did not consider the values of NFI. Since the values of d_ULS and d_G does not pertain to any value and since, Chi-squared as a model fit measure involves the calculations of degrees of freedom that are not well determined in PLS-SEM (Dijkstra & Henseler, 2015), this study only considered SRMR as a model fit measure.

The difference between implicit correlation matrix of the model and the observed correlation matrix defines SRMR (Hair et al. 2017; Cangur & Ercan, 2015). As a measure of model fit, SRMR was observed to assess the discrepancies between expected correlations and observed correlations as an average (Hair et al., 2017; Henseler et al., 2014). SRMR values less than 0.1 of 0.08 and less defines a good fit for the model (Hair et al., 2017; Henseler et al., 2014; Cangur & Ercan, 2015). Table 6 shows the results of the SmartPLS PLS Algorithm test for goodness of fit test.

Test Observed	**Saturated Model**
SRMR	0.078
NFI	0.92

Table 6: SRMR and NFI results

The observed results for the conceptual model were represented as the saturated model, which implies the usage of the original conceptual model data. The observed SRMR after running the PLS Algorithm bootstrapping was 0.078. To achieve the above SRMR value for acceptable and valid goodness of fit SRMR value which is supposed to be less than 0.08 (Hair et al., 2017), one construct item was adjusted from the model since the initially SRMR value was 0.08. Indicator PerceivedDataConfidentiality_5, which had the least model loading of 0.756, was removed from the model, and the model PLS Algorithm test was rerun. According to Cangur and Ercan (2015), and Hair et al. (2014), model indicators can be removed to allow the model to have a good fit. The indicator addresses the influence of data being accessed by unauthorised third parties, as a perceived data confidentiality security concern and participants might not have adequately understood the indicator since clarity on third parties was not well stated hence resulted in the lowest loading compared to other indicators.

The observed SRMR of value 0.078 is considered a good fit since it agrees with Hair et al. (2017) and Henseler et al. (2014) who stated that SRMR values are acceptable and valid only if they the values are below the threshold of 0.08. After running a complete bootstrapping in Smart PLS, the observed Normal Fit Index for the test was 0.92. According to (Reinartz,Haenlein, & Henseler, 2009) the resultant NFI of 0.92 also justifies a good fit together with the observed results standardized Root Mean Square Residual, Exact Model fit, and the geodesic. As a result, the conceptual model shown in Figure 1 has a good fit. The results observed from the SRMR goodness of fit test suggested that data used for the study fitted well to the conceptual model of the study.

4.4 Hypothesis testing and path coefficients

To address the research question posed by the study, hypothesis testing and path coefficient analysis was performed. Roky and Al-Meriouh (2015) used and suggested hypothesis testing and path coefficient test as appropriate tests for the researcher to answer research questions. The relationship between the dependent variable and independent variables was hypothesised using constructs from previous studies in mobile banking namely: perceived self-efficacy (Abayomi et al., 2019; Makanyeza, 2017), perceived severity (Chen & Cheng, 2017; Alexandrou, 2016); perceived threat (Farah et al., 2018; Zhou, 2017), perceived susceptibility (Alexandrou, 2016; Awan et al., 2017; Marafon et al., 2018), perceived data confidentiality (Bertino & Ferrari, 2018; Stallings et al., 2013), perceived data integrity (Stewart & Jürjens, 2018; Wazid, Zeadally, & Das, 2019); cybersecurity awareness (Bada, et al., 2019; Öğütçü, et al., 2016) and intention to use (Chen, 2013).

The current study observed path coefficients to assess the relationship between latent variables (Roky & Meriouh, 2015). Path coefficients were adopted to assess the statistical significance between latent variables; path coefficients have an algebraic sign, which must not contradict with theoretically proven assumptions concerning the relationship among latent variables for the path coefficient to be valid (Hair et al., 2017). To perform a statistical test, the relationship between latent variables was defined as paths, and the measure of significance on latent variables relationship was called the path coefficient (Cangur & Ercan, 2015). Path coefficients with values greater than 0.2 are considered significant for quantitative research data analysis (Cangur & Ercan, 2015).

Structural Equation Modeling was used to test the relationship between latent variables (Byrne, 2013). This study assessed the hypothesises formulated in section 2.4 and the relationships of constructs for the inner model assessment and path coefficients were observed after running a nonparametric bootstrapping analysis in Smart PLS 3 (Hair et al., 2017). Smart-PLS was used to assess the model because it takes latent variables that were used as a construct for the structural model and assesses the psychometric attributes of the model and computes approximate parameters of the path coefficients (Yoon & Steege, 2013).

A good significance is achieved based on certain t-values with corresponding p-values, implying that for p values less than 0.05, t-values must be more significant than 1.95 or 1.96 and above (Hair et al., 2014; Roky & Al-Meriouh, 2015). Roky and Al-Meriouh (2015) also stated that p values less than 0.001 require t-values greater than or equal to 3.29. When p values are less than or equals to 0.001, the relationship is statistically interpreted as highly significant (Roky & Al-Meriouh, 2015). When p values are less than or equals to 0.01, implies that the relationship between latent variables is statistically significant, and p values higher than 0.05 implies an insignificant relationship (Roky & Al-Meriouh, 2015).

The resultant path coefficients for the hypothesis testing after running a bootstrapping in Smart PLS on data collected for the current study are shown in Table 7.

Hypothesis	Relationship	Path Coefficients	Std Beta (β)	Std Error	|t-value|	Decision	5% CI LL	95% CI UL	P values
H1	perceived self-efficacy -> Intention to Use	0.169	0.165	0.093	1.877**	Not supported	0.008	0.301	0.064
H2	Perceived severity -> Intention to Use	-0.116	-0.104	0.1	1.131**	Not supported	-0.257	0.076	0.261
H3	Perceived Threat -> Intention to Use	-0.013	-0.03	0.117	0.111**	Not supported	-0.206	0.168	0.912
H4	Perceived Susceptibility -> Intention to Use	-0.136	-0.117	0.114	1.197**	Not supported	-0.289	0.096	0.232
H5	Perceived Data Confidentiality -> Intention to Use	0.228	0.182	0.148	1.54**	supported	-0.072	0.411	0.124
H6	Perceived data Integrity -> Intention to Use	-0.205	-0.174	0.141	1.457**	Not supported	-0.394	0.066	0.146
H7	Cybersecurity Awareness -> Intention to Use	0.581	0.551	0.079	7.378**	supported	0.411	0.663	0.000

Table 7: Hypothesis testing, path coefficient and t-values results

Findings and discussion on Intrinsic factors hypothesis testing

Intrinsic factors are congenital motivations that influence one's decision to engage in an activity or event (de Almeida et al., 2016). This study defines cybersecurity intrinsic factors as natural or inborn perceptions or worldviews that determine one's course of actions after being exposed or encounter a cybersecurity threat, attack or any threatening cyber stimulus. The following sections present hypothesis-testing findings for intrinsic factors.

a) Perceived self-efficacy

In this study, perceived self-efficacy implies one's perception of how capable they believe they can avert security threats by following cybersecurity protections recommendations. The influence of perceived self-efficacy on the intention to use mobile banking applications was tested using the following hypothesis:

Hypothesis H1: *Perceived self-efficacy influences the intention to use mobile banking applications.*

Table 7 shows that Hypothesis H1 was not supported, implying perceived self-efficacy did not have a positive influence on the intention to use mobile banking applications. The effect of perceived self-efficacy had a value of 0.169, meaning that the influence of perceived self-efficacy on the intention to use mobile banking applications was very low. The observed moderate positive effect size ($\beta = 0.165$) for perceived self-efficacy ($p<0.01$, t-value = 1.877**) suggests that mobile users do not see self-efficacy as influencing their intention to use mobile banking applications.

This finding does not mirror previous studies such as those of Abayomi et al. (2019) and Makanyeza (2017) who found, self-efficacy as a crucial factor that influence the adoption of mobile banking services in developing countries. This study suggests a limited understanding of the impact of consequences associated with cyber-attacks as the reason for mobile users not considering perceived self-efficacy as a major concern. This is because cybersecurity has not been widely addressed in developing countries (Maduku, Mpinganjira, & Duh, 2016; Makanyeza, 2017), and the usage mobile devices for banking have limited acceptance (Martens, Roll, & Elliott, 2017), as a result this study states that mobile users are not fully informed on the cybersecurity consequences, especially from a banking perspective. Nevertheless, the dangers associated with insecure security behaviours has material consequences in mobile banking (Arif, 2016).

The findings imply that self-efficacy does not influence self-conviction about one's ability to mobilise, be motivated and take security prevention courses of action to protect themselves from cybersecurity-related threats and attacks. As a result, the influence of perceived severity on the intention to use mobile banking technology is not significant.

b) Perceived severity

Perceived severity is applied as the degree of perceived loss or cost that is associated with the use of mobile banking technology in this study. The influence of perceived severity on the intention to use mobile banking applications was tested using the following developed hypothesis:

Hypothesis H2: *Perceived severity influences the intention to use mobile banking applications.*

Hypothesis H2 was not supported, as shown in Table 7. As a result, this study concludes that the influence of perceived severity on the intention to use mobile banking applications is not significant. A path coefficient value of - 0.116, was observed suggesting that the influence of perceived severity on the intention to use mobile banking applications was found very low. A low standard Bita of β = -0.104 for perceived severity ($p<0.01$, t-value = -1.131**), implies that the influence of perceived severity on the intention to use mobile banking applications is also below zero hence not significant.

The implications of the findings are that mobile users do not foresee security as an inhibitor towards their desire to use mobile banking applications. The results imply that technology users do not need to feel or perceive being secure for them to intent use mobile banking applications. Since, mobile

banking usage and adoption has increased even though at a very low rate (Arif, 2016), this study suggested that technology users' curiosity towards the easy of use of mobile banking applications out weight the security perception factor. Martens, Roll, and Elliott (2017) found perceived usefulness as the strongest predictor on the intention to use mobile banking payments. Martens, Roll, and Elliott (2017)'s study tested technology readiness and acceptance across South African and German. Hence the current study agrees with their findings by assuming that the technology users desire to easily and remotely access mobile banking services can take their focus from understanding security perception. Also, this study suggests a limited understanding of the impact of security leakages when using mobile banking as a contributor to why users did not consider perceived severity as a contributor towards the intention to use mobile banking. The findings support the observations by Li et al., (2019), who concluded that perceived severity does not influence users' behaviour in taking protective measures when using technology. As a result, this study concludes perceived severity, not a significant factor to influence the intention to use mobile banking applications.

c) Perceived Threat

Perceived threat implies negative persuasion associated with processing a presented message or stimulus. In this study, perceived threat implies the perception of cybersecurity uncertainties or dangers associated with the usage of mobile banking applications. The influence of perceived threat on the intention to use mobile banking applications was tested using the following developed hypothesis:

Hypothesis H3: *Perceived threat influences the intention to use mobile banking applications.*

The results indicate that Hypothesis H3 was not supported; meaning that perceived threat has a very profound influence on the intention to use mobile banking applications. A path coefficient (R-squared) value of -0.013 was observed suggesting that the influence of perceived severity on the intention to use mobile banking applications was found low. A low standard Bita of β = - 0.030 for perceived threat ($p<0.01$, t-value = 0.111**) means that perceived threat is not a significant factor for mobile users' intention to use mobile banking applications.

The results found that technology users are not concerned about the threats associated with the usage of mobile banking. The influence of perceived threat on the intention to use mobile banking applications was not significant. Since mobile banking security is costly to technology users when they lose their data or information via cyber attacks (Nambiro et al., 2017), this study suggests lack of cybersecurity knowledge as a contributing factor to why research participants could not perceive cybersecurity threat as significant to their intention to use mobile banking applications. Chigada and Hirschfelder (2017) who concluded that there is a need to educate South Africans are pertaining to the importance of technology support the previous suggestion. As a result, the implications of the findings are that mobile users need to be informed with the right information concerning the impact of cybersecurity when using mobile banking applications before their perception is altered by less informed information from unreliable sources.

The observed results agree with the findings of Akturan and Tezcan (2012), and Hanafizadeh, Keating, and Khedmatgozar (2014) who concluded that perceived threat was not a significant influencing factor on the intention to use mobile banking or internet banking. This study concludes that the perceptions

of uncertainties associated with mobile banking applications usage do not influence the intention to use mobile banking applications.

d) Perceived susceptibility

Perceived susceptibility implies the degree to which a technology user feels likely to be in danger while using technology. This study considered perceived susceptibility as the internal perception or belief possessed by technology users on how they feel vulnerable to cybersecurity dangers. The degree to which technology users' views the probability of negatively affected by the dangers associated with the usage of mobile banking was investigated using the following hypothesis:

Hypothesis H4: *Perceived susceptibility influences the intention to use mobile banking applications.*

The results show that Hypothesis H4 was not supported. As a result, this study concludes that perceived susceptibility did not have a positive influence on the intention to use mobile banking applications. A path coefficient (R-squared) value of - 0.136 was observed, implying that the influence of perceived susceptibility on the intention to use mobile banking applications was very low. A low standard Bita of $\beta = 0.117$ for perceived susceptibility ($p<0.01$, t-value = 1.197**), supports that perceived susceptibility does not have a significant influence on the intention to use mobile banking applications.

The results did not support the findings by Awan et al. (2017), who stated that perceived susceptibility has a positive influence on the usage of technology. Also, the findings did not agree with findings by Alsaleh et al. (2017), who concluded that a misperception of security susceptibility by smartphone users influences their desire to take preventive security actions in technology. However, the finding agrees with Das and Khan (2016), who found that susceptibility and severity in mobile devices usages does not drive security behavior change. As a result, the findings imply that perceived susceptibility does not significantly influence security behavior in mobile banking applications usage. Mobile users do not foresee mobile banking security dangers and attacks as harmful.

Mobile users do not feel liable for being harmed or encounter significant loss from cybersecurity incidents. As a result, limited understanding concerning the risks associated with the use of mobile devices for banking is the main contributor to why mobile users do not feel likely being in danger of cybersecurity incidents. Also, lack of previous cyber attack incidents could be the cause for the findings since a study by Geil, Sagers, Spaulding, and Wolf (2018) suggested that previous security incidents are determining contributors of higher perceived susceptibility on technology users. As a result, the mobile user's perceived susceptibility does not significantly influence the intention to use mobile banking applications.

Findings and discussion on Extrinsic factors

Extrinsic factors are external motivations that influence one's decision to engage in an activity or event (de Almeida et al., 2016). This study defines extrinsic cybersecurity factors as external motivations that determine one's course of actions after being exposed to a cyber-threatening stimulus mostly to gain a reward or to avoid the negative impact of the stimulus. The following sections present hypothesis-testing findings for extrinsic factors.

a) Perceived data confidentiality

Perceived data confidentiality implies the technology user believes about how their data can be kept inaccessible by unauthorised parties. Data that is exchanged via telecommunication channels while using mobile technology need to be kept confidential between parties that agreed to exchange the data only. In mobile banking applications usage, data confidentiality implies sensitive transactional and non-transactional data can be kept inaccessible between service providers, customers and sometimes third parties as per agreement. The influence of how people perceive data confidentiality on the intention to use mobile banking applications was tested using the following developed hypothesis:

Hypothesis H5: *Perceived data confidentiality influences the intention to use mobile banking applications.*

The observed path coefficient for perceived data confidentiality on the intention to use mobile banking applications is 0.228. Hypothesis H5 was therefore supported. The results imply that perceived data confidentiality has a positive influence on the intention to use mobile banking applications. The observed path coefficient of 0.228 suggests that influence of perceived data confidentiality on the intention to use mobile banking applications was moderate. A moderate effect size ($\beta = 0.182$) of perceived data confidentiality ($p<0.01$, t-value = 1.54**) means that perceived data confidentiality significantly influence the intension to use mobile banking applications.

Mobile banking involves the transfer of financial and non-financial data via telecommunication channels; the findings imply that mobile banking users are afraid of how their data can be kept confidential between themselves and services providers (Whitman & Mattord, 2018). A breach in financial data can result in a significant financial loss (Von Solms & Van Niekerk, 2013); hence, the monetary value of data breaches is suggested to influence the significant influence of perceived data confidentiality on the intention to use mobile banking applications. The findings agree with Zissis and Lekkas, (2012), who concluded that how customers perceive the protection of their sensitive or personal data has a significant influence on customer's intention to use technology for business. According to Whitman and Mattord (2018), and Zissis and Lekkas (2012), there is a need to assure potential users of technology that their data will not be accessed or misused by unauthorised parties.

The findings imply that confidentiality of data is a very crucial factor to mobile users on their intention to use mobile banking application since a breach of confidential information can result in significant loss especially in mobile banking applications usage. Data transferred between mobile banking applications and service providers have a financial or monetary value especial when processing financial transactions (Donovan, 2014; Von Solms & Van Niekerk, 2013). As a result, this study suggests mobile banking applications service providers invest in programs that can help to build trust with their potential and current mobile banking users to positively maximise the influence of perceived data confidentiality on the in intention to use mobile banking applications.

b) Perceived data integrity

Data integrity is about ensuring that unauthorised entities can not modify data exchanged between two or more parties. In mobile banking, data integrity involves ensuring that data used for mobile banking is delivered timeously and in an exact or unaltered format. Transactional or general information data is exchanged via telecommunication channels to fulfil mobile banking services and the data exchanged must be kept inaccessible from unauthorised parties to avoid data breach. Perceived data integrity in mobile banking implies the belief about the secureness of mobile banking

data from modification by unauthorised entities. The following hypothesis was used to investigate the perceived influence of data integrity on the intention to use.

Hypothesis H6: *Perceived data integrity influences the intention to use mobile banking applications.*

The resultant path coefficient value of - 0.205 implies that the proposed hypothesis was not supported since Cangur and Ercan, (2015), stated that only path coefficients with values greater than 0.2 are considered significant for research data analysis. The low standard Bita of $\beta = 0.182$ for perceived data integrity ($p<0.01$, t-value = 1.547**), supports that influence of perceived data integrity on the intention to use mobile banking applications was not significant.

The findings mean that potential mobile banking applications users do not view the protection of their data from being modified by unauthorised parties as a hindrance to their intention to use mobile banking applications. The findings imply that the accuracy and consistency of data used in mobile banking is not a concern that is valid enough to influence their intention to mobile banking applications significantly. As a result, mobile devices users do not consider the assurance of data consistency and accuracy as a hindrance to mobile banking applications intention to use. The results defy the finding by Yu et al., (2015) who stated that timeously delivery of data in an accurately desired format is a crucial factor to technology users' security behavior. Also, Wazid et al., (2019), stated that technology users need the assurance that their data will remain accurate, unmodified and trustworthy while in transit and while stored on applications, however, this study did not support these findings. The study suggests limited understanding about the dangers associated with data integrity as a contributor to the findings. As a result, this study concluded that the perceived protection of mobile banking data from being modified by unauthorised parties does not influence the intention to use mobile banking applications.

c) Cybersecurity awareness

Human factor remains the top cybersecurity factor to be considered by most organisations. Security tools are not enough for complete security when using technology. How humans interact with technology has open doors for security threats and attacks. The awareness of cybersecurity issues is critical for security I technology usage. Cybersecurity awareness implies users' knowledge about the uncertainties associated with technology usage or adoption. In mobile banking, cybersecurity awareness implies how technology users are aware of the threats and the impact that is involved in mobile banking usage or intention to use. The influence of cybersecurity awareness on the intention to use mobile banking applications was tested using the following developed hypothesis:

Hypothesis H7: *Cybersecurity awareness influences the intention to use mobile banking applications*

The observed path coefficient for cybersecurity awareness on the intention to use mobile banking applications is 0.581, implying that hypothesis H7 was supported. The results imply that cybersecurity awareness has a positive influence on the intention to use mobile banking applications. The observed path coefficient of 0.581 suggests that influence of cybersecurity awareness on the intention to use mobile banking applications was between high and moderate. A moderate effect size of standard bita of $\beta = 0.551$ for cybersecurity awareness ($p<0.01$, t-value =7.378**), with a significant path coefficient, implies that the influence of cybersecurity awareness on the intension to use mobile banking applications is positive. The results mean that cybersecurity awareness significantly influences the intention to use mobile banking applications.

The implication of the findings is that mobile users see cybersecurity awareness as a potential influence on their intention to use mobile banking. The more mobile users are informed about cybersecurity threats, attacks and cybersecurity protective measure, the more they can make informed decisions on whether they intend to use mobile devices for business (So, 2013). Mobile users that understand or are well informed about available protective measures are most likely to intend to use mobile banking applications than those that are not informed or are miss informed. The suggested reason for the because mobile users that only aware of dangers associated with mobile banking applications usage without knowing how to minimise or securely utilise mobile banking applications for banking can feel victimised since the solution to the problem is not provided. The findings agree with Dlamini and Modise (2012), who stated that how mobile users are knowledgeable about the uncertainties tied to the usage of technology has a significant influence on the intention to use mobile banking. As a result, this study recommends both technology users and mobile banking service providers to be aware of the threats and the impact of threat that are involved in technology usage for banking.

4.5 Discussion of findings

The findings observed that perceived self-efficacy, perceived severity, perceived threat, perceived susceptibility and perceived data integrity were found not having a significant influence on the intention to use mobile banking applications as discussed in Section 4.3.3. The following sections further discuss the findings on perceived data confidentiality and cybersecurity awareness, which are the factors that were found significantly influencing the intention to use mobile banking applications.

Perceived data confidentiality

Perceived data confidentiality was found as a cybersecurity factor with a significant influence on the intention to use mobile banking applications. The findings agree with (Mbelli & Dwolatzky, 2016), who concluded that data confidentiality has a significant influence on the intention to do business in the cyberspace. Since mobile banking applications usage involve the exchange of sensitive data, how potential users perceive the protection of their sensitive data (Whitman & Mattord, 2018; Zissis & Lekkas, 2012) significantly influence their intention to use mobile banking applications. As a result, mobile banking applications service providers must assure potential customers that unauthorised parties can not access their personal information. As a result, this study concludes that potential mobile banking applications users need assurance about the confidentiality of their data (personal, transactional and others) for them to use mobile banking applications.

The study found the perception of data confidentiality as a significant cybersecurity factor that influences the intention to use mobile banking applications. The results implied that how people perceive the protection of their sensitive data from being modified by unauthorised third parties significantly influence their intention to use mobile banking applications. The findings agree with Zissis and Lekkas (2012) who stated that there is need to guarantee that data exchanged in cyberspace between two or three parties will be protected from being modified by unauthorised parties by keeping it confidential. The findings agree with Thakur (2018), who concluded that perceived data confidentiality influences the intention to use technology. As a result, it tails that the higher the magnitude of perceived data confidentiality in mobile applications, the more likely users intend to use the technology (Akram et al., 2018). Stewart and Jürjens (2018) concluded that it is crucial to address data confidentiality in order to increase users confidence in financial technology or mobile banking

The study suggests that mobile banking service providers must assurance customers' that their data will remain accurate, unmodified and trustworthy while using their services. Ability to assure customers can boost customers' trust; hence, that can potentially increase customers desire to use mobile banking applications for banking. As a result, potential customers' perception of how their sensitive data can be kept unmodified while using mobile banking applications influences their desire to use mobile banking applications.

Cybersecurity awareness

Cybersecurity awareness was found as a salient significant factor that influences the intention to use mobile banking applications. Cybersecurity awareness as a cybersecurity influencer implies that the degree to which potential mobile banking users are knowledgeable and well informed with legitimate information about cybersecurity determines their intention to use mobile banking applications. The finds agreed with several studies (Dlamini & Modise, 2012; Grobler, Jansen van Vuuren, & Zaaiman, 2011) that found cybersecurity awareness as a salient significant factor that influences the intention to use technology. This study recommends mobile banking service providers to educate or make legal information about cybersecurity readily available to their potential customers. Service providers can use Cybersecurity awareness programs, for example, workshops and digital advertisements as cybersecurity awareness strategy. The more well-informed technology users are about cybersecurity, the less they fall prey of wrong or biased information that can distort their level of trust and intention to use mobile banking applications. Cybersecurity awareness programs will inform potential users of the dangers associated with mobile banking and prevention measures that can be followed to ensure secure transaction processing and data protection.

4.6 Summary

Cybersecurity awareness and perceived data confidentiality were the factors with supported hypothesises. Perceived self-efficacy, perceived severity, perceived threat, perceived susceptibility and perceived data integrity had hypothesised that did not support their influence on the intention to use mobile banking applications.

The findings imply that the knowledge of cybersecurity that technology users have and how technology users believe that their data can be kept confidential within agreed parties when using mobile technology influences the intention to use mobile banking applications. The implication of the final conceptual model is that technology users are more concerned about how they perceived that their data would not be shared with unauthorised stakeholders and their knowledge of cybersecurity as determining factors for them to use mobile banking applications. As a result, mobile banking application providers or banks must have strategic solutions in place to guarantee the confidentiality of data and inform or make technology users aware of the right cybersecurity issues and protective measures.

CHAPTER 5: CONCLUSION

The study focused on mobile banking and builds on the influence of mobile banking security perception on the intention to use mobile banking application. Although studies in information systems have examined mobile banking, there has not been an in-depth investigation on understanding the perceived influence of cybersecurity on the intention to use mobile banking applications. The benefits of using mobile banking have identified, but the adoption rate amongst consumers' remains low, mostly in developing countries. The implementation of mobile banking application is still in its infancy stage, and user acceptance is still a significant challenge in developing countries. The understanding of why consumers do not engage in the frequent use of mobile banking applications in developing countries is minimal. Even though alternative ways of banking for example traditional way of visiting bank offices for all banking services have been suggested as a reason for limited usage and acceptance of mobile banking applications, trust remains a crucial factor in the intention to adopt or use mobile banking, mainly because of the increasing prevalence of cyber threats. The study investigated the perceived influence of cybersecurity on the intention to use mobile banking applications.

The study followed a positivist paradigm. Survey questionnaires were used as a technique to collect data. The literature review identified seven factors that were suggested as cybersecurity influencers. The identified cybersecurity influencers were categorised into intrinsic and extrinsic factors. Intrinsic factors were perceived self-efficacy, perceived threat, perceived susceptibility, perceived severity and extrinsic factors were perceived data confidentiality, perceived data integrity and cybersecurity awareness. A conceptual model was developed from the intrinsic and extrinsic factors, and hypothesises were formulated to test the theoretical model.

Smart PLS 3 was used to test the significance of intrinsic and extrinsic factors on the intention to use mobile banking applications. Structural equation modelling and Partial Least Squares path-modelling approaches were adopted for data analysis of quantitative data collected from ninety participants. Statistical tests were performed to test the validity of the proposed conceptual model, the internal consistency, the convergent reliability, discriminant validity and the average variance explained, and construct item reliability assessment of constructs was performed. The coefficient of determination assessment, path coefficient test and model goodness of fit test in SmartPLS 3 was tested. All tests were success full, and the model had a good fit. Hypothesis testing was performed on salient factors that influence the perception of mobile banking cybersecurity on the intention to use mobile banking applications.

The findings concluded that salient significant factors that influence the perception of mobile banking cybersecurity on the intention to use mobile banking applications were perceived data confidentiality and cybersecurity awareness. Perceived data confidentiality had an observed path coefficient weight of 0.228 on the intention to use mobile banking applications. The results concluded that the hypothesis was supported and with a moderate effect size (β = 0.182) of perceived data confidentiality ($p<0.01$, t-value = 1.54**) with a significant coefficient value, hence this study concluded that perceived data confidentiality significantly influence the intension to use mobile banking applications. Cybersecurity awareness had an observed path coefficient weight of 0.581 on the intention to use mobile banking

applications and this was the strongest of all the hypotheses. The results concluded that the hypothesis was supported and with a moderate effect size (β = 0.551) for cybersecurity awareness ($p<0.01$, t-value = 7.378**) significant coefficient values, hence this study concluded that cybersecurity awareness significantly influence the intension to use mobile banking applications.

The study suggests further investigation on the unsupported hypothesis of the study. Further research is suggested to investigate why perceived self-efficacy, perceived severity, perceived threat, perceived susceptibility and perceived data integrity did not have a significant influence on the intention to use mobile banking applications.

5.1 Research contribution

The findings for the study have both a knowledge gap and a practical contribution. On the knowledge gap, the model can be used to understand the influence of cybersecurity factors in the intention to use technology. The practical contribution is that mobile banking application service providers can understand the influence of cybersecurity factors on the intention to use mobile banking applications hence develop and implement strategies to serve better and attract more customers. Understanding the magnitude of influence enforced by cybersecurity awareness on the intention to use mobile banking applications can help service providers to build trust with users by conveying the right information about cybersecurity in mobile banking. Perceived data confidentiality can practically influence the making of policies about data protection in mobile banking and assure customers about the protection of their data. In summary, the results can be used by banks to address why consumers do not engage in the frequent use of mobile banking applications and customer challenges with cybersecurity.

5.2 Limitations

The population comprised dominantly of Western Cape-based users of mobile technology, which may affect their overall cybersecurity understanding. There is a probability of the results differing with sample size. A more general sample size that might include users without mobile banking technology and based in other provinces is suggested for future research. Besides, the study can be extended to include other developing countries. The study had a cross-sectional time horizon implying that the study was contacted within a fixed time horizon, and that is during the academic period. The study did not consider moderating factors for the analysis, and that might have an impact on the results. However, the study recommends further analysis of results based on demographic factors.

ACKNOWLEDGEMENT

With a grateful heart, l would like to acknowledge people that walked with me through this great learning and personal growth journey. Finishing this thesis reminds me of the relevance of every person in my life.

To my supervisor Assoc Prof Salah Kabanda, thank you for the support and the help. To Gordon, my IS colleagues, and everyone in UCT IS department, thank you for the support and encouragement. I want to thank my SCF family for the prayers and support to unleash greatness.

To my Mom and my late Dad, thank you for the wise counsel and trusting me with major academic decisions, you remain the best, and you are forever loved. To all my friends, God bless you for making a difference in my life. To Best and Tumelo Pops, thank you guys for the war room, God bless you. To the Moshal family, thank you for the opportunity to advance my career through your exceptional support and sponsorship.

Above all, "unto him, that is able to keep me from falling and to present me faultless before the presence of His glory with exceeding joy, to the only wise God, our Saviour, be glory and majesty, dominion and power, both now and ever".

Victory Belong to Jesus.

Thank you all.

Ishmael Chikoo

REFERENCES

Abayomi, O. J., Olabode, A. C., Reyad, M. A. H., Tetteh Teye, E., Haq, M. N., & Mensah, E. T. (2019). Effects of Demographic Factors on Customers' Mobile Banking Services Adoption in Nigeria. *International Journal of Business and Social Science*. 10(1), 63-77. https://doi.org/10.30845/ijbss.v10n1p9

Akram, R. N., Chen, H. H., Lopez, J., Sauveron, D., & Yang, L. T. (2018). Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems*. 80, 417-420. https://doi.org/10.1016/j.future.2017.11.026

Akturan, U., & Tezcan, N. (2012). Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence and Planning*. *30*(4), 444-459. https://doi.org/10.1108/02634501211231928

Al-omari, A., & El-gayar, O. (2012). Information Security Policy Compliance : The Role of Information Security Awareness, 16, 1–10.

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., Lal, B., & Williams, M. D. (2015). Consumer adoption of Internet banking in Jordan: Examining the role of hedonic motivation, habit, self-efficacy and trust. *Journal of Financial Services Marketing*, 20(2), 145-157. https://doi.org/10.1057/fsm.2015.5

Alalwan, Ali Abdallah, Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*. *37*(3), 99-110. https://doi.org/10.1016/j.ijinfomgt.2017.01.002

Alexandrou, A., & Chen, L. C. (2014). The Security Risk Perception Model for the Adoption of Mobile Devices in the Healthcare Industry. *Csis.Pace.Edu*, 1–6. Retrieved from http://csis.pace.edu/%7B~%7Dctappert/srd2014/a7.pdf%5Cnhttp://csis.pace.edu/~ctappert/srd2014/a7.pdf

Alexandrou, A., & Chen, L. C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal*. 32(1), 1-25. https://doi.org/10.1057/s41284-019-00170-0

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*. *12*(3), 0173284 https://doi.org/10.1371/journal.pone.0173284.

Alexandrou, A., & Chen, L. C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal*. https://doi.org/10.1057/s41284-019-00170-0

Arif, I. (2016). Resistance to Mobile Banking Adoption in a Developing Country : Evidence from Modified TAM Literature Review Theoretical Background. 1(1), 25–42. https://doi.org/10.20547/jfer1601104

Assensoh-Kodua, A., Migiro, S., & Mutambara, E. (2016). Mobile banking in South Africa: a systematic review of the literature. *Banks and Bank Systems*, *11*(1), 34–41. https://doi.org/10.21511/bbs.11(1).2016.04

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

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 1(1), 1-11. Retrieved from http://arxiv.org/abs/1901.02672

Bankole, F. O., Bankole, O. O., & Brown, I. (2017). Influences on Cell Phone Banking Adoption in South Africa: An Updated Perspective. *Journal of Internet Banking and Commerce,* 22(3), 1-16.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(02), 176–198. https://doi.org/10.1017/eis.2016.8

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, *50*, 418–430. https://doi.org/10.1016/j.chb.2015.04.024

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*. *28*, 24-31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bertino, E., & Ferrari, E., (2018). Big data security and privacy. *In A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years.* Springer, Cham, 31, 425-439.

Bhattacherjee, A. (2012). Introduction to Research, Social Science Research: Principles, Methods, and Practices. *USF Open Access Textbooks Collection. Book 3 University of South Florida* Link https://doi.org/10.1351/pac198961091657

Bojjagani, S., & Sastry, V. N. (2017). A secure end-to-end SMS-based mobile banking protocol. *International Journal of Communication Systems*. 30(15):3302. https://doi.org/10.1002/dac.3302

Bryman, A. (2015). *Social research methods* . Oxford University Press, New Delh

Byrne, B. M. (2013). Structural equation modeling with AMOS: Basic concepts, applications, and programming. Routledge.

Cangur, S., & Ercan, I. (2015). Comparison of Model Fit Indices Used in Structural Equation Modeling Under Multivariate Normality. *Journal of Modern Applied Statistical Methods*. 14(1), 152-166. https://doi.org/10.22237/jmasm/1430453580

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2018). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*. 9(1), 70-104.

https://doi.org/10.1080/10864415.2004.11044320

Chen, C. S. (2013). Perceived risk, usage frequency of mobile banking services. *Managing Service Quality*. 23(5), 410-436. https://doi.org/10.1108/MSQ-10-2012-0137

Chen, L. M., & Cheng, Y. Y. (2017). Perceived severity of cyberbullying behaviour: differences between genders, grades and participant roles. *Educational Psychology*. https://doi.org/10.1080/01443410.2016.1202898

Chen, Y., & Zahedi, F. M. (2017). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*. 37(5), 599-610. https://doi.org/10.25300/misq/2016/40.1.09

Chigada, J. M., & Hirschfelder, B. (2017). Mobile banking in South Africa: A review and directions for future research. *South African Journal of Information Management,* 19(1), 1-9.

Church, A. H., & Waclawski, J. (2017). *Designing and using organizational surveys*. Routledge.

Cudjoe, A. G., Anim, P. A., & Tetteh Nyanyofio, J. G. N. (2015). Determinants of Mobile Banking Adoption in the Ghanaian Banking Industry: A Case of Access Bank Ghana Limited. *Journal of Computer and Communications*. 3(02), 1-19. https://doi.org/10.4236/jcc.2015.32001

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*. 24(1), 116-134. https://doi.org/10.1108/ICS-04-2015-0018

de Almeida, F. C., Lesca, H., & Canton, A. W. P. (2016). Intrinsic motivation for knowledge sharing – competitive intelligence process in a telecom company. *Journal of Knowledge Management*. 20(6), 1282-1301. https://doi.org/10.1108/JKM-02-2016-0083

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*. 34(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Deline, M. B., & Kahlor, L. A. (2019). Planned Risk Information Avoidance: A Proposed Theoretical Model. *Communication Theory*. https://doi.org/10.1093/ct/qty035

Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: a synergy approach. *7th International Conference on Information Warfare and Security*, 1, 98-107. https://doi.org/10.1007/978-3-8349-4134-3_3

Donovan, K. (2014). Mobile Money for Financial Inclusion. In *Information and Communications for Development*. 61(1), 61-73. https://doi.org/10.1596/9780821389911_ch04

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*. 58, 214-220. https://doi.org/10.1016/j.chb.2015.12.050

Falissard, B. (2012). Analysis of Questionnaire Data with R. *International Statistical Review*. https://doi.org/10.1111/j.1751-5823.2012.00196_5.x

Farah, M. F., Hasni, M. J. S., & Abbas, A. K. (2018). Mobile-banking adoption: empirical evidence from the banking sector in Pakistan. *International Journal of Bank Marketing*. 36(7), 1386-1413. https://doi.org/10.1108/IJBM-10-2017-0215

Fornell, C., & Larcker, D. F. (n.d.). Evaluating structural equation models with unob- servable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*. 21(3), 317-334. https://doi.org/10.22434/IFAMR2017.0045

Govender, I., & Sihlali, W. (2014). A Study of Mobile Banking Adoption among University Students Using an Extended TAM. *Mediterranean Journal of Social Sciences*, *5*(7), 451–459. https://doi.org/10.5901/mjss.2014.v5n7p451

Grobler, M., Jansen van Vuuren, J., & Zaaiman, J. (2011). Evaluating Cyber Security Awareness in South Africa. *10th European Conference on Warfare and Security*, 10, 113–121.

Hadlington, L., & Chivers, S. (2019). Segmentation Analysis of Susceptibilityto Cybercrime: Exploring IndividualDifferences in Information SecurityAwareness and Personality Factors. *Policing*. 10, 1-14. https://doi.org/10.1093/zoolinnean/zly093

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *Sage, Thousand Oaks*.

Hair, J. F., Ringle, C. M., Sarstedt, M., Hair, J. F., Ringle, C. M., & Sarstedt, M. (2014). PLS-SEM : Indeed a Silver Bullet PLS-SEM : Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*.

Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review*. 26(2), 106-121. https://doi.org/10.1108/EBR-10-2013-0128

Hajian, S., Shariati, M., Mirzaii Najmabadi, K., Yunesian, M., & Ajami, M. I. (2015). Use of the Extended Parallel Process Model (EPPM) to Predict Iranian Women's Intention for Vaginal Delivery. *Journal of Transcultural Nursing*. 26(3), 234-243. https://doi.org/10.1177/1043659614524247

Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of Internet banking adoption. *Telematics and Informatics*, *31*(3), 492–510. https://doi.org/10.1016/j.tele.2013.04.003

Hayikader, S., Nurafiqah, F., Hadi, A., & Ibrahim, J. (2016). Issues and Security Measures of Mobile Banking Apps, *6*(1), 36–41.

He, W., Tian, X., & Shen, J. (2015). Examining security risks of mobile banking applications through blog mining. 103-108. *In MAICS (pp. 103-108)*.

Heemskerk, D., Caws, M., Marais, B., & Farrar, J. (2015). Prevention. In *Springer Briefs in Public Health*. https://doi.org/10.1007/978-3-319-19132-4_6

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management and Data Systems*. 116(1), 2-20. https://doi.org/10.1108/IMDS-09-2015-0382

Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity

in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*. 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Jansen, J., & van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*. 87, 371-383. https://doi.org/10.1016/j.chb.2018.05.010

Joubert, J., & Van Belle, J. (2013). The role of trust and risk in mobile commerce adoption within South Africa. *International Journal of Business, Humanities and Technology*, 3(2), 27-38.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*. 28(3), 269-282. https://doi.org/10.1080/10919392.2018.1484598

Kader, S., & Minnaar, A. (2015). Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. *Acta Criminologica: Southern African Journal of Criminology*, 5, 67-81.

Ketchen, D. J. (2013). A Primer on Partial Least Squares Structural Equation Modeling. *Long Range Planning*. 46(1-2), 184-185. https://doi.org/10.1016/j.lrp.2013.01.002

Khedmatgozar, H. R., & Shahnazi, A. (2018). The role of dimensions of perceived risk in adoption of corporate internet banking by customers in Iran. *Electronic Commerce Research*. 18(2), 389-412. https://doi.org/10.1007/s10660-017-9253-z

Kim, S. Y., Kim, M. H., & Park, M. G. (2015). A Study on the Information Security Control and Management Process in Mobile Banking Systems. *Journal of Korea Multimedia Society*, 18(2), 218-232.

Koksal, M. H. (2016). The intentions of Lebanese consumers to adopt mobile banking. *International Journal of Bank Marketing*. 34(3), 327-346. https://doi.org/10.1108/IJBM-03-2015-0025

Korpela, K. (2015). Improving Cyber Security Awareness and Training Programs with Data Analytics. *Information Security Journal*. 24(1-3), 72-77. https://doi.org/10.1080/19393555.2015.1051676

Laukkanen, T. (2017). Mobile banking. *International Journal of Bank Marketing*, 35(7), 1042-1043.

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *International Conference on Cyber Conflict, 8, 65-80. CYCON*. https://doi.org/10.1109/CYCON.2016.7529427

Legner, C., Urbach, N., & Nolte, C. (2016). Mobile business application for service and maintenance processes: Using ex post evaluation by end-users as input for iterative design. *Information and Management*. 53(6), 817-831. https://doi.org/10.1016/j.im.2016.03.001

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behavior. In *Lecture Notes in Business Information Processing*. 268, 103-111. https://doi.org/10.1007/978-3-319-49944-4_8

Lin, T. T. C., & Bautista, J. R. (2016). Predicting Intention to Take Protective Measures During Haze: The Roles of Efficacy, Threat, Media Trust, and Affective Attitude. *Journal of Health Communication*. 21(7), 790-799. https://doi.org/10.1080/10810730.2016.1157657

Maduku, D. K., Mpinganjira, M., & Duh, H. (2016). Understanding mobile marketing adoption intention by South African SMEs: A multi-perspective framework. *International Journal of Information Management*. 36(5), 711-723. https://doi.org/10.1016/j.ijinfomgt.2016.04.018

Makanyeza, C. (2017). Determinants of consumers' intention to adopt mobile banking services in Zimbabwe. *International Journal of Bank Marketing*. 35(6), 997-1017. https://doi.org/10.1108/IJBM-07-2016-0099

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in Human Behavior*, *54*, 453–461. https://doi.org/10.1016/j.chb.2015.08.039

Manhas, K. P., & Oberle, K. (2015). The ethics of metaphor as a research tool. *Research Ethics*. 11(1), 42-51. https://doi.org/10.1177/1747016114523421

Marafon, D. L., Basso, K., Espartel, L. B., de Barcellos, M. D., & Rech, E. (2018). Perceived risk and intention to use internet banking: The effects of self-confidence and risk acceptance. *International Journal of Bank Marketing*. 36(2), 277-289. https://doi.org/10.1108/IJBM-11-2016-0166

Martens, M., Roll, O., & Elliott, R. (2017). Testing the technology readiness and acceptance model for mobile payments across Germany and South Africa. *International Journal of Innovation and Technology Management,* 14(06), 1750033.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, *34*(1), 1–13. https://doi.org/10.1016/j.ijinfomgt.2013.06.002

Mbelli, T. M., & Dwolatzky, B. (2016). Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 1-6). IEEE.*. https://doi.org/10.1109/CSCloud.2016.18

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*. 69, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

Mujinga, M., Eloff, MM., & Kroeze JH. (2016). Online banking users' perceptions in South Africa: An exploratory empirical study. *In: Proceedings of the IST-Africa Conference 2016; Durban, South Africa. Durban: IIMC*; 2016. p. 1-7. https://doi.org/10.1109/istafrica.2016.7530617

Nambiro, A. W., Wabwoba, F., & Wasike, J. (2017). Cyber security challenges to mobile banking in SACCOs in Kenya. *International Journal of Computer (IJC)* 27(1),133-140

Nasri, W., & Charfeddine, L. (2012). Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior. *Journal of High Technology Management Research*. 23 (1), 1–14. https://doi.org/10.1016/j.hitech.2012.03.001

Njenga, K., & Ndlovu, S. (2015, November). Mobile banking and information security risks: Demand-side predilections of South African lead-users. In 2015 *Second International Conference on Information Security and Cyber Forensics* (InfoSec) (pp. 86-92). IEEE.

https://doi.org/10.1109/InfoSec.2015.7435511

Ohk, K., & Park, S. (2016). The Effect of Personal Information Security Attitude and Perceived Company Information Security Policy on Mobile Banking Acceptance, *9*(13), 635–640.

Olofsdotter, S., Åslund, C., Furmark, T., Comasco, E., & Nilsson, K. W. (2018). Differential susceptibility effects of oxytocin gene (OXT) polymorphisms and perceived parenting on social anxiety among adolescents. *Development and Psychopathology*. 30(2), 449-459. https://doi.org/10.1017/s0954579417000967

Öȉütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*. 56, 83-93 https://doi.org/10.1016/j.cose.2015.10.002

Park, E., Baek, S., Ohm, J., & Chang, H. J. (2014). Determinants of player acceptance of mobile social network games: An application of extended technology acceptance model. *Telematics and Informatics*, 31(1), 3–15. https://doi.org/10.1016/j.tele.2013.07.001

Paulo, M. M., Rita, P., Oliveira, T., & Moro, S. (2018). Understanding mobile augmented reality adoption in a consumer context. *Journal of Hospitality and Tourism Technology*. 9(2), 142-157. https://doi.org/10.1108/JHTT-01-2017-0006

Payne, G., & Payne, J. (2004). Key concepts in social research. London: Sage.

Pour, P., Des, L. U., & Bancaires, O. (2011). The Analysis of Influencing Factors and Promotion Strategy for the Use of Mobile Banking. *Canadian Journal of Social Science*. 2(7), 60-63.

Roky, H., & Meriouh, Y. Al. (2015). Evaluation by Users of an Industrial Information System (XPPS) Based on the DeLone and McLean Model for IS Success. *Procedia Economics and Finance*. 26, 903-913. https://doi.org/10.1016/S2212-5671(15)00903-X

Rönkkö, M., McIntosh, C. N., Antonakis, J., & Edwards, J. R. (2016). Partial least squares path modeling: Time for some serious second thoughts. *Journal of Operations Management*. 47, 9-27. https://doi.org/10.1016/j.jom.2016.05.002

Rotolo, T., Berg, J. a., Paton, D., Johnston, D., Kitagawa, K., Heagele, T. N., De Mers, G. (2016). Social Science Research: principles, methods, and practices. *Textbooks Collection*. https://doi.org/10.1017/S1049023X16000157

Sanchez, G. (2013.). PLS Path Modeling with R. Berkeley, CA: Trowchez Editions.

Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students (Seventh Edition). In *Research Methods for Business Students (Seventh Edition)*.

Saunders, M. N. K., Thornhill, A., & Lewis, P. (2015). Research Methods for Business Students (5th Edition). In *Research Methods for Business Students*.

Seitz, H. H., Schapira, M. M., Gibson, L. A., Skubisz, C., Mello, S., Armstrong, K., & Cappella, J. N. (2018). Explaining the effects of a decision intervention on mammography intentions: The roles of worry, fear and perceived susceptibility to breast cancer. *Psychology and Health*. 33(5), 682-700. https://doi.org/10.1080/08870446.2017.1387261

Shaikh, A. A., & Karjaluoto, H. (2015). Telematics and Informatics Mobile banking adoption : A

literature review. *Telematics and Informatics*, *32*(1), 129–142. https://doi.org/10.1016/j.tele.2014.05.003

Sharma, S. K., Govindaluri, S. M., Al-Muharrami, S., & Tarhini, A. (2017). A multi-analytical model for mobile banking adoption: a developing country perspective. *Review of International Business and Strategy*, *27*(1), 133–148. https://doi.org/10.1108/RIBS-11-2016-0074

So, J. (2013). A Further Extension of the Extended Parallel Process Model (E-EPPM): Implications of Cognitive Appraisal Theory of Emotion and Dispositional Coping Style. *Health Communication*, *28*(1), 72–83. https://doi.org/10.1080/10410236.2012.708633

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stallings, W., Bauer, M., & Hirsch, E. M. (2013). *Computer Security. Principles and Practice. Computer Security*.

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*. 26(1), 109-128. https://doi.org/10.1108/ICS-06-2017-0039

Sun, B., Sun, C., Liu, C., & Gui, C. (2017). Research on Initial Trust Model of Mobile Banking Users, *7*(1), 13–20.

Talburt, J. R. (2010). Principles of Information Quality. In *Entity Resolution and Information Quality* (pp. 39–62). https://doi.org/10.1016/b978-0-12-381972-7.00002-6

Thakur, R. (2018). The role of self-efficacy and customer satisfaction in driving loyalty to the mobile shopping application. *International Journal of Retail and Distribution Management*. 46(3), 283-303. https://doi.org/10.1108/IJRDM-11-2016-0214

Tran, H. T. T., & Corner, J. (2016). The impact of communication channels on mobile banking adoption. *International Journal of Bank Marketing*. 34(1), 78-109. https://doi.org/10.1108/IJBM-06-2014-0073

Tunay, K. B., Tunay, N., & Akhisar, İ. (2015). Interaction Between Internet Banking and Bank Performance: The Case of Europe. *Procedia - Social and Behavioral Sciences*, *195*, 363–368. https://doi.org/10.1016/j.sbspro.2015.06.335

Van der Waldt, G., Fourie, D., Jordaan, J., & Chitiga-Mabugu, M. (2018). Skills profile of technical staff in the south African local government sector: an empirical survey. *Problems and Perspectives in Management*, 16(1), 173.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*. 75, 547-559. https://doi.org/10.1016/j.chb.2017.05.038

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. *IEEE Consumer Electronics Magazine*. 8(2), 56-60.

https://doi.org/10.1109/MCE.2018.2881291

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security Sixth Edition*. Cengage Learning.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–416.

Yoon, H. S., & Steege, L. M. B. (2013). Computers in Human Behavior Development of a quantitative model of the impact of customers ' personality and perceptions on Internet banking use. *Computers in Human Behavior*, 29(3), 1133–1141. https://doi.org/10.1016/j.chb.2012.10.005

Yu, C.-S. (2014). Consumer Switching Behavior From Online Banking To Mobile Banking. *International Journal of Cyber Society and Education Pages*, 7(1), 1–28. https://doi.org/10.7903/ijcse.1108

Yu, C.-S. (2012). Factors Affecting Individuals to Adopt Mobile Banking: Empirical Evidence from the UTAUT Model. *Journal of Electronic Commerce Research*, *13(2)*, 104–121.

Yu, P. L., Balaji, M. S., & Khong, K. W. (2015). Building trust in internet banking: A trustworthiness perspective. *Industrial Management and Data Systems*. 115(2), 235-252. https://doi.org/10.1108/IMDS-09-2014-0262

Zhou, T. (2018). Examining users' switch from online banking to mobile banking. *International Journal of Networking and Virtual Organisations*. 18(1), 51-66. https://doi.org/10.1504/ijnvo.2017.10011767

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*. 28(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006

APPENDIXES

APPENDIX 1: constructs and research items

Question Number	Construct	Question (construct item)
Q1	Demographic	Are you currently residing in South Africa?
Q2	Demographic	Which province are you located?
Q3	Demographic	What is your gender? - Selected Choice
Q4	Demographic	In which age group do you fall under?
Q5	Demographic	Which category do you fall under?
Q6	Demographic	Do you have a bank account?
Q7	Demographic	Do you use a smart phone?
Q8	Demographic	Do you have a mobile banking application(s) installed on your phone?
Q9	Demographic	Do you use mobile banking application for banking services?
Q10	Demographic	For how many years have you been using a bank?
Q11	Perceived self-efficacy	I believe l will be capable of using mobile banking applications despite security issues.
Q12	Perceived self-efficacy	I am confident that l can use mobile banking applications services on my mobile devices.
Q13	Perceived self-efficacy	I will need fewer security instructions to use mobile banking applications.
Q14	Perceived self-efficacy	I am confident that l can use mobile banking applications if I have the online security instructions for reference.
Q15	Perceived self-efficacy	I am confident that l can use mobile banking applications, even if there is no one around to show me how to do it securely.
Q16	Perceived threat	I don't trust the functionality of banking applications services when using mobile banking applications.
Q17	Perceived threat	Going to the bank to make any transaction make me feel safer as compared to using mobile banking applications.
Q18	Perceived threat	I am scared of losing my money by using mobile banking applications.
Q19	Perceived threat	I am scared of losing my bank details when using mobile banking applications.
Q20	Perceived threat	Security threats can limit my desire to use mobile banking applications.
Q21	Perceived severity	The security of mobile banking applications can result in major consequences to my bank account.
Q22	Perceived severity	I am very scared of losing my money from mobile banking applications attacks.

Q23	Perceived severity	Losing my mobile banking application details will be a serious issue to me and l will not feel safe.
Q24	Perceived severity	Mobile banking applications security will be a serious problem for me.
Q25	Perceived susceptibility	I will feel vulnerable to mobile banking applications security threats.
Q26	Perceived susceptibility	I will not feel safe to process a mobile banking service via mobile banking applications.
Q27	Perceived susceptibility	I am very scared to use mobile banking applications because of security issues.
Q28	Perceived susceptibility	I do care about security issues, l will not use mobile banking applications.
Q30	Perceived data confidentiality	I think that using mobile banking applications is financially insecure for my personal data.
Q31	Perceived data confidentiality	I am concerned if my banking details will be disclosed to unauthorised individuals when using mobile banking applications.
Q32	Perceived data confidentiality	I feel that my personal data can be shared with third parties if l use mobile banking applications.
Q33	Perceived data confidentiality	I feel that a hacker may hack into my private information when using Mobile banking applications services.
Q34	Perceived data confidentiality	I am scared that my personal information can be accessed by third parties if l lose the device with my mobile banking application.
Q35	Cybersecurity Awareness	I follow news and developments about the security-related technologies so l am willing to use mobile banking application.
Q36	Cybersecurity Awareness	I do not care about the security involved in mobile banking since l am aware of them so l am willing to use mobile banking application.
Q37	Intention to use	I read about the problems of malicious threats attacking user's mobile banking devices so l am willing to use mobile banking applications.
Q38	Intention to use	I am aware of the security dangers involved in the usage of mobile banking applications so l am willing to use mobile banking applications.
Q39	Cybersecurity Awareness	Being aware of threats available allows me to use mobile banking applications more wisely.
Q40	Perceived data integrity	I feel that using mobile banking applications is financially insecure for my personal data.
Q41	Perceived data integrity	I don't trust in the ability of mobile banking applications to protect my privacy hence I don't desire to use mobile banking applications.
Q42	Perceived data integrity	I don't desire to use mobile banking applications because l don't trust security features of mobile banking applications technology in protecting my data.

Q43	Perceived data integrity	I believe that a hacker may hack into my private information when using Mobile banking applications hence l am not willing to use mobile banking applications.
Q44	Perceived data integrity	My bank details used in mobile banking applications may be stolen with the mobile banking devices hence l am not willing to use mobile banking applications.

APPENDIX 2: research questionnaire

Masters of Commerce in Information Systems

Start of Block: Introduction

Consent Form Dear Sir/Madam

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town, a research study is required. The researcher, in this case, Ishmael Chikoo has chosen to conduct a study entitled "Perceived influence of mobile banking cyber security on the intention to use mobile banking applications." The main goal of the study is to investigate the perceived influence of cybersecurity on the intention to use mobile banking applications.

This study has been approved by the University of Cape Town Commerce faculty ethics committee. Data collection and compliance of the study comply with UCT data management policy. Your participation in this research is voluntary. All information will be treated confidentially and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring the anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be an online questionnaire. The questionnaire will take approximately 15 minutes to complete. If you are willing to participate in this study, please complete this questionnaire consent and proceed to the next stage. Should you have any questions regarding this research, please feel free to contact me on 0740601410 or email: chkish003@myuct.ac.zaYour participation in this study would be greatly appreciated but is entirely voluntary.

Sincerely,
Ishmael Chikoo

- ○ Yes I consent (1)
- ○ No, I don't consent (2)

Skip To: End of Survey If Dear Sir/Madam In terms of the requirements for completing a Master's Degree in Information Systems... = No I don't consent

End of Block: Introduction

Start of Block: General Research Questions

Section A: General Information (Demographic) Questions

Q1 Are you currently residing in South Africa?

- ○ Yes (1)
- ○ No (2)

Skip To: End of Survey.If you currently residing in South Africa? = No

Q2 Which province are you located?

- ○ Western Cape (1)
- ○ Eastern Cape (2)
- ○ Free State (3)
- ○ Gauteng (4)
- ○ KwaZulu-Natal (5)
- ○ Limpopo (6)
- ○ Mpumalanga (7)
- ○ North West (8)
- ○ Northern Cape (9)

Q3 What is your gender?

- ○ Male (1)
- ○ Female (2)
- ○ Rather not say (3)
- ○ Other (4) _____

Q4 In which age group do you fall under?

- ○ Under 25years (1)
- ○ Between 25 and 30 years (2)
- ○ Between 30 and 40 years (3)
- ○ Above 40 years (4)

Q5 Which category do you fall under?

- ○ Fulltime employed (1)
- ○ Partime employed (2)
- ○ Student (3)
- ○ Not employed (4)

Q6 Do you have a bank account?

- ○ Yes (1)
- ○ No (2)
- ○ No, but l would like to have one (3)
- ○ No, and I don't like to have one (4)

Q7 Do you use a smart phone?

- ○ Yes (1)
- ○ No (2)
- ○ No, but would like to use one (3)
- ○ No, and I don't like to use one (4)

Q8 Do you have a mobile banking application(s) installed in your phone?

- ○ Yes (1)
- ○ No (2)
- ○ No, but would like to have (3)
- ○ No, and I don't like to have one (4)

Q9 Do you use mobile banking application for banking services?

- ○ Yes (1)
- ○ No (2)
- ○ No, but would like to use (3)
- ○ No, and not interested (4)

Q10 For how many years have you been using a bank?

- ◯ less than a year ““
- ◯ Between 1 and 2 years (2)
- ◯ More than 2 years (3)
- ◯ Never used a bank (4)

End of Block: General Research Questions

Section B: Mobile banking Security Questions

Please complete the questionnaire by selecting the most applicable:

Five-point Likert Scale: *5 Strongly agree. – 1 strongly disagree.*

◯ Strongly agree ◯ Agree ◯ Neutral ◯ Disagree ◯ Strongly disagree

Start of Block: Mobile banking Security Questions - Perceived self-efficacy

Q11 I believe l will be capable of using mobile banking applications despite security issues.

- ◯ Strongly Agree
- ◯ Agree
- ◯ Neither agree nor disagree
- ◯ Disagree
- ◯ Strongly disagree

Q12 I am confident that l can use mobile banking applications services on my mobile devices.

- ○ Strongly agree (1)
- ○ Agree
- ○ Neither agree nor disagree
- ○ disagree
- ○ Strongly disagree

Q13 I will need fewer security instructions to use mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q14 I am confident that l can use mobile banking applications if I have the online security instructions for reference.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q15 I am confident that l can use mobile banking applications even if there is no one around to show me how to do it securely.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q16 I don't trust the functionality of banking applications services when using a mobile banking application.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q17 Going to the bank to make any transaction make me feel safer as compared to using mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q18 I am scared of losing my money by using mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q19 I am scared of losing my bank details when using mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q20 Security threats can limit my desire to use mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q21 The security of mobile banking applications can result in major consequences to my bank account.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q22 I am very scared of losing my money from mobile banking applications attacks.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q23 Losing my mobile banking application details will be a serious issue to me and l will not feel safe.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q24 Mobile banking applications security will be a serious problem for me.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q25 I will feel vulnerable to mobile banking applications security threats.

- ○ Strongly agree
- ○ agree
- ○ Neither agree nor disagree
- ○ disagree
- ○ Strongly disagree

Q26 I will not feel safe to process a mobile banking service via mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q27 I am very scared to use mobile banking applications because of security issues.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q28 I do care about security issues, l will not use mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q30 I think that using mobile banking applications is financially insecure for my personal data.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q31 I am concerned if my banking details will be disclosed to unauthorised individuals when using mobile banking applications.

- ○ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q32 I feel that my personal data can be shared to third parties if l use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q33 I feel that a hacker may hack into my private information when using Mobile banking applications services.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q34 I am scared that my personal information can be accessed by third parties if l lose the device with my mobile banking application.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q35 I follow news and developments about the security-related technologies, so l am willing to use mobile banking application.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q36 I do not care about the security involved in mobile banking since l am aware of them, so l am willing to use mobile banking application.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q37 I read about the problems of malicious threats attacking user's mobile banking devices, so l am willing to use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q38 I am aware of security dangers involved in the usage of mobile banking applications, so l am willing to use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q39 Being aware of threats available allows me to use mobile banking applications more wisely.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q40 I feel that using mobile banking applications is financially insecure for my personal data.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q41 I don't trust in the ability of mobile banking applications to protect my privacy hence I don't desire to use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q42 I don't desire to use mobile banking applications because l don't trust security features of mobile banking applications technology in protecting my data.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q43 I believe that a hacker may hack into my private information when using Mobile banking applications; hence l am not willing to use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

Q44 My bank details used in Mobile banking applications may be stolen with mobile banking devices; hence l am not willing to use mobile banking applications.

- ○ Strongly Agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree

APPENDIX 3. Hypothesis testing results

Hypothesis	Relationship	Path Coefficients	Std Beta/ Sample Mean	Std Error	|t-value|^	Decision	5% CI LL	95% CI UL	P values
H1	perceived Self-efficacy -> Intention to Use	0.172	0.165	0.093	1.853**	supported	0.008	0.301	0.064
H2	Perceived severity -> Intention to Use	-0.112	-0.104	0.1	1.126**	Not supported	-0.257	0.076	0.261
H3	Perceived Threat -> Intention to Use	-0.013	-0.03	0.117	0.111**	Not supported	-0.206	0.168	0.912
H4	Perceived Susceptibility -> Intention to Use	-0.136	-0.117	0.114	1.197**	Not supported	-0.289	0.096	0.232
H5	Perceived Data Confidentiality -> Intention to Use	0.228	0.182	0.148	1.54**	supported	-0.072	0.411	0.124
H6	Perceived data Integrity -> Intention to Use	-0.205	-0.174	0.141	1.457**	supported	-0.394	0.066	0.146
H7	Cybersecurity Awareness -> Intention to Use	0.58	0.551	0.079	7.378**	supported	0.411	0.663	0.000

APPENDIX 4: Cross-loadings

	Cybersecurity Awareness	Intention to Use	Perceived Data Confidentiality	Perceived Susceptibility	Perceived Threat	Perceived data Integrity	Perceived severity	perceived Self-efficacy
CyberSecurityAwareness_1	**0.864**	0.593	-0.177	-0.041	-0.138	-0.020	-0.091	0.008
CyberSecurityAwareness_2	**0.896**	0.400	-0.060	0.049	-0.083	-0.025	0.058	0.030
CyberSecurityAwareness_3	**0.781**	0.415	-0.043	-0.094	-0.191	-0.063	0.156	0.093
IntentionToUse_1	0.482	0.827	0.011	-0.052	-0.131	-0.024	-0.101	0.111
IntentionToUse_2	0.520	0.920	-0.138	-0.228	-0.230	-0.275	-0.026	0.203
PerceivedDataConfidentiality_1	-0.157	-0.096	0.881	0.436	0.388	0.519	0.237	-0.047
PerceivedDataConfidentiality_2	-0.101	-0.086	0.872	0.441	0.338	0.375	0.342	-0.138
PerceivedDataConfidentiality_3	-0.059	-0.052	0.902	0.510	0.461	0.571	0.217	-0.089
PerceivedDataConfidentiality_4	-0.051	-0.028	0.824	0.458	0.436	0.467	0.334	-0.205
PerceivedDataIntegrity_1	-0.055	-0.188	0.456	0.432	0.415	0.861	0.034	-0.039
PerceivedDataIntegrity_2	-0.092	-0.192	0.397	0.369	0.354	0.881	0.031	0.002
PerceivedDataIntegrity_3	0.021	-0.102	0.432	0.374	0.456	0.827	-0.066	0.006
PerceivedDataIntegrity_4	-0.007	-0.175	0.516	0.435	0.432	0.845	0.076	-0.099
PerceivedDataIntegrity_5	-0.005	-0.150	0.545	0.517	0.464	0.877	0.146	-0.130
PerceivedSelfEfficacy_1	0.054	0.180	-0.099	-0.039	-0.160	-0.011	-0.087	0.817
PerceivedSelfEfficacy_2	0.056	0.144	-0.208	-0.061	-0.037	-0.182	0.074	0.807
PerceivedSelfEfficacy_3	0.016	0.152	-0.082	0.001	-0.123	-0.055	0.029	0.910
PerceivedSelfEfficacy_4	-0.024	0.166	-0.108	-0.041	-0.031	-0.065	0.058	0.914
PerceivedSelfEfficacy_5	0.099	0.153	-0.007	0.064	-0.083	0.032	0.012	0.820
PerceivedSeverity_1	0.008	-0.046	0.165	0.041	0.031	-0.100	0.810	0.093
PerceivedSeverity_2	-0.023	-0.072	0.258	0.157	0.032	0.071	0.935	-0.002
PerceivedSeverity_3	0.038	-0.052	0.305	0.226	0.136	0.070	0.881	-0.007
PerceivedSeverity_4	0.102	-0.045	0.374	0.362	0.308	0.150	0.772	-0.020
PerceivedSusceptibility_1	0.017	-0.068	0.332	0.784	0.424	0.258	0.170	-0.019

PerceivedSusceptibility_2	-0.074	-0.128	0.463	0.834	0.476	0.486	0.259	0.060
PerceivedSusceptibility_3	-0.002	-0.194	0.471	0.891	0.501	0.420	0.206	-0.064
PerceivedSusceptibility_4	-0.056	-0.166	0.488	0.941	0.544	0.488	0.146	-0.019
PerceivedThreat_1	-0.126	-0.073	0.335	0.506	0.824	0.436	0.112	0.013
PerceivedThreat_2	-0.117	-0.161	0.431	0.512	0.853	0.413	0.183	-0.106
PerceivedThreat_3	-0.177	-0.253	0.416	0.534	0.932	0.422	0.191	-0.164
PerceivedThreat_4	-0.100	-0.170	0.394	0.468	0.890	0.415	0.054	-0.080
PerceivedThreat_5	-0.176	-0.209	0.397	0.519	0.940	0.497	0.042	-0.049

APPENDIX 5: Outer- loadings

	Cybersecurity Awareness	Intention to Use	Perceived Data Confidentiality	Perceived Susceptibility	Perceived Threat	Perceived data Integrity	Perceived severity	perceived Self-efficacy
CyberSecurityAwareness_1	0.864							
CyberSecurityAwareness_2	0.896							
CyberSecurityAwareness_3	0.781							
IntentionToUse_1		0.827						
IntentionToUse_2		0.920						
PerceivedDataConfidentiality_1			0.881					
PerceivedDataConfidentiality_2			0.872					
PerceivedDataConfidentiality_3			0.902					
PerceivedDataConfidentiality_4			0.824					
PerceivedDataIntegrity_1						0.861		
PerceivedDataIntegrity_2						0.881		
PerceivedDataIntegrity_3						0.827		
PerceivedDataIntegrity_4						0.845		
PerceivedDataIntegrity_5						0.877		
PerceivedSelfEfficacy_1								0.817
PerceivedSelfEfficacy_2								0.807
PerceivedSelfEfficacy_3								0.910
PerceivedSelfEfficacy_4								0.914
PerceivedSelfEfficacy_5								0.820
PerceivedSeverity_1							0.810	
PerceivedSeverity_2							0.935	
PerceivedSeverity_3							0.881	
PerceivedSeverity_4							0.772	
PerceivedSusceptibility_1				0.784				
PerceivedSusceptibility_2				0.834				

PerceivedSusceptibility_3				0.891				
PerceivedSusceptibility_4				0.941				
PerceivedThreat_1					0.824			
PerceivedThreat_2					0.853			
PerceivedThreat_3					0.932			
PerceivedThreat_4					0.890			
PerceivedThreat_5					0.940			