Risk and Security of Digital-only banks: perspective from Digital natives in South Africa

Akani Machimana

Supervisor: Dr. Ayanda Magida

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2025

ABSTRACT

The increasing adoption of technology has transformed various industries, including banking, where traditional services are now accessible through digital platforms. In South Africa, digital-only banks operate without physical branches, relying solely on digital infrastructure. While this presents opportunities, it also introduces risks such as cyberattacks, data breaches, and financial losses. Understanding these risks is crucial to fostering adoption, particularly among digitally active individuals.

This study addresses a gap in existing literature, which largely focuses on general adoption factors rather than the security-specific concerns of digital natives in South Africa. Grounded in the Technology Acceptance Model (TAM) and Perceived Risk Theory (PRT), the research explores security and risk as key determinants of adoption. It also investigates measures that consumers and digital-only banks can implement to enhance security.

A qualitative approach was employed, using semi-structured interviews with eleven digital natives selected through purposive sampling. Findings reveal that perceived security risks remain a key barrier to adoption, despite advancements in digital banking security. Threats such as social engineering and phishing persist due to low user awareness, while infrastructure challenges in underserved areas further hinder adoption.

Despite perceptions of convenience and usability, digital-only banks are not widely seen as cost-effective. To enhance trust and adoption, digital-only banks must prioritise security awareness, transparency, and collaboration with stakeholders to address infrastructure gaps and cybersecurity threats. Strengthening consumer education and adopting advanced security technologies are essential for ensuring responsible digital banking adoption in South Africa.

KEYWORDS

Digital banking, Digital-only banks, Digital natives, Perceived Risk, Perceived Security, Technology acceptance model (TAM)

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This qualitative study sought to understand customer experiences with digital-only banks in South Africa amongst digital natives, specifically focusing on their perceived risks and security.

1.2 Background of the study

The Fourth Industrial Revolution has accelerated digitalisation on a global scale, necessitating rapid digital transformation for countries to remain competitive and interconnected (Bajpai & Biberman, 2021). This technological shift has significantly disrupted various sectors, including financial services, reshaping how banking institutions operate. In South Africa, the banking sector underwent a profound transformation, with the introduction of the first fully digital bank in 2019 marking a pivotal moment in the country's financial evolution. This disruption aligns with global trends as digital banking emerges as a mainstream alternative to traditional banking models. Factors such as the COVID-19 pandemic, increasing smartphone penetration, expanded internet access, and the proliferation of fintech companies have further accelerated the adoption of digital banking in recent years (Agur et al., 2020).

The issuance of the first fully digital banking licence to TymeBank in 2019 catalysed a new wave of banking innovation, with subsequent market entrants such as Discovery Bank and Bank Zero reinforcing the sector's digital transformation. The rapid expansion of digital banks is evident in their growing customer bases. By June 2022, TymeBank had surpassed five million customers, achieving profitability by December 2023—making it the first fully digital bank in Africa to reach this milestone within five years of its launch (TymeBank, 2024). Similarly, Discovery Bank, the world's first behavioural bank, recorded an

impressive 42% annual client growth, reaching over 825,000 customers by December 2023 (Discovery, 2024). These figures illustrate a strong and growing appetite for digital banking solutions in South Africa.

However, while digital banks offer convenience and accessibility, they also present heightened security concerns. Research conducted by the Financial Sector Conduct Authority (FSCA) in 2021 found that digital-only customers acknowledged improvements in digital banking security over time. Nonetheless, cybersecurity threats remain a significant concern, with customers expressing ongoing dissatisfaction regarding the safety of online transactions. Key apprehensions include risks associated with personal information breaches, unauthorised access to accounts, and password security vulnerabilities. These concerns directly affect customer trust and adoption rates, as security perceptions strongly influence the overall user experience.

The security risks associated with digital banking are further corroborated by the South African Banking Risk Information Centre (SABRIC), which reported a 24% increase in fraud cases in its 2022 annual report. This escalating trend underscores the pressing need for digital banks to implement advanced security measures to safeguard customer data and reinforce confidence in digital platforms. The ability of digital-only banks to sustain long-term growth and maintain a competitive edge is contingent on their ability to mitigate cybersecurity threats while enhancing user experience. This necessitates a proactive approach, integrating robust authentication methods, artificial intelligence-driven fraud detection, and customer-centric security education to foster digital trust.

Understanding these evolving risks and customer security perceptions is crucial for the sustainability of digital-only banks in South Africa. As digital banking expands, addressing security vulnerabilities and improving user trust will remain paramount in ensuring widespread adoption and long-term viability.

1.3 Research Problem

The rise of digital-only banks, also known as challenger banks, has disrupted the traditional banking sector in South Africa (Nel & Boshoff, 2021). While these banks are known for their rapid innovation (National Treasury, 2023), they face intense competition from well-established traditional banks. To attract and retain customers, digital-only banks must differentiate themselves through seamless customer experiences and robust security measures (Windasari et al., 2022). As fully virtual institutions, digital-only banks are particularly vulnerable to cybersecurity threats, including cyber-attacks, data breaches, and fraud (Zvavandanga, 2024). Security concerns are a major factor influencing consumer trust, with a study by the Boston Consulting Group (2022) revealing that 60% of South African consumers would consider using a digital-only bank only if they were confident in its security. Despite growing adoption, digital banking fraud cases increased by 24% in 2022 (SABRIC, 2022), raising concerns about the adequacy of existing security frameworks. However, the extent to which these risks shape the perceptions and adoption decisions of digital natives remains underexplored.

Existing studies have examined digital banking adoption through factors such as ease of use, usefulness, and trust (Cele, 2024; Almaiah et al., 2023; Slazus & Bick, 2022). While global research has applied theoretical frameworks to identify adoption factors in digital banking (Windasari et al., 2022; Chawla et al., 2023; Hakimi et al., 2023), few studies have specifically explored how digital natives perceive and navigate security risks. In South Africa, prior research has focused on broad consumer adoption trends (Cele & Mlitwa, 2024) and traditional banking customers' attitudes toward digital-only banks (Nel & Boshoff, 2020). However, little is known about how security and perceived risk influence digital natives' trust and adoption of digital-only banking.

Research shows that perceived security risks, including cybercrime and online fraud, are key deterrents to fintech adoption (Almaiah et al., 2023; Baraba & Mahmudi, 2023). Additionally, security, ease of use, and perceived risk significantly shape consumer trust and satisfaction in digital banking (Wilson et al., 2021). Given that digital natives are highly tech-savvy and more open to adopting digital financial services (Assala et al., 2023), it is critical to understand their experiences and attitudes toward security in digital-only banking. With 70% of South Africa's population under 40 (Stats SA, 2023), this demographic represents a significant consumer base. Furthermore, digital natives accounted for 61% of new credit originations in 2023 (TransUnion, 2023), demonstrating their growing economic influence.

This qualitative study seeks to address this gap by exploring digital natives' perceptions of security and risk in digital-only banking. By providing in-depth insights into their lived experiences, concerns, and trust-building factors, this research will inform digital banks on enhancing security frameworks while maintaining usability. The findings will contribute to industry and regulatory discussions, offering strategic recommendations for improving security perceptions and driving digital banking adoption among South African digital natives.

1.4 Research Objectives

1. To explore the factors that digital natives consider risks and security levels in South Africa's digital-only banking.
2. To explore how the perceived risk and security influence Digital natives' intention to adopt Digital-only banking.
3. To understand from digital natives what measures digital-only banks in South Africa can prioritise to reduce risks and improve security.

1.5 Rationale

A study by Accenture (2023) found that 85% of consumers aged 18–24 had purchased a financial product from a new provider—a higher rate than older age groups—making them an attractive market for financial products. Additionally, 48% of digital-only banking adopters use these platforms to supplement traditional banking, often for specific purposes such as small payments or savings. This highlights the need for digital banks to become competitive so that they are perceived as full banks and not supplementary. Without effective marketing and differentiation, digital-only banks risk stagnation or decline. Digital-only banks have existed in South Africa for five years, making them a relatively new phenomenon in the financial sector. However, research on this type of banking in the South African context remains limited. While prior studies have explored factors influencing digital banking adoption, there is a lack of in-depth analysis of individual determinants shaping customer experience, particularly regarding perceived security and risk.

Digital natives are the highest adopters of digital platforms, including digital banking. They prioritise customer experience, trust, and security (Chawla et al., 2023). Previous research has identified key factors affecting customer experience in digital banking, such as perceived quality, ease of use, risk, usability, and security (Windasari et al., 2022). Almaiah et al. (2023) further emphasised that perceived security is crucial in e-banking adoption, fostering trust and confidence in digital transactions. However, as digital banking evolves, so do cybersecurity risks (Oyewole et al., 2024), making robust security measures essential for customer retention and trust. This study seeks to contribute to the existing body of knowledge by providing in-depth insights into the customer experiences of digital natives, with a focus on their perceptions of risk and security in digital-only banking. Academically, it fills a critical gap in South African research by offering a nuanced analysis of security concerns specific to digital natives—an increasingly influential consumer segment. Practically, the findings will help digital-only banks refine their security strategies and user

engagement approaches, enabling them to address key customer concerns more effectively. By strengthening trust in digital banking security, the study's insights may also assist financial institutions in improving adoption rates and ensuring long-term sustainability in an evolving digital landscape.

1.6 Delimitations of the study

This study focused on banking customers who are digital natives, those between the ages of 18 and 43. While many factors impact the adoption of digital-only banks, this study only focused on two factors: perceived risk and security. The study was exclusively for digital-only banks. The study involved participants based in Johannesburg and Cape Town who had a level of understanding when it came to digital-only banking.

1.7 Definition of terms

Digital banking: According to FCSA (2021), Digital banking entails digitising traditional banking services to deliver financial services to customers. This entails digitising marketing, customer onboarding, service channels, processes, products, and features such as savings and deposits, loan management, and bill payments and facilitating digital lifestyle services such as ride-hailing, health, tech, telecoms, media, etc., through ecosystem orchestration, partnerships, and open APIs.

Digital-only banks: Also called virtual banks, rely solely on digital infrastructure to offer banking products and services. Services are provided through smart devices such as mobile phones, tablets, and computers. They do not have brick-and-mortar offices or branches; everything is through virtual platforms (McKinsey, 2021).

Digital Natives: Digital natives have had significant exposure to technology, which has moulded how they interact with digital tools. Early exposure to technology like the Internet, computers, and mobile devices fundamentally

changes how digital natives learn and operate. They are highly literate in ICT (information and communication technology), and they gather information through their gadgets. They include Millennials and all generations after millennials (Sadiku et al.,2017).

Generation Z: Generation Z are those born after the Millennials; they were born between 1997 and 2012. Since the Z generation's higher level of adaptive technology, new technologies appear to be a part of their daily lives (Almaiah et al., 2023; Park et al., 2024).

Millennials/ Generation Y: Millennials are those born between 1981 and 1996. They are highly reliant on technology and interconnected (Almaiah et al.,2023; Baraba & Mahmudi, 2023).

Perceived Risk is an individual's belief in the likelihood of an adverse outcome and consequence when using a fintech (Khedmatgozar & Shahnazi, 2018; Almaiah et al., 2023; Wilson et al., 2021).

Perceived security is the degree to which a user feels a mobile banking application is secure against any risks. Applying security techniques to guarantee the security of user services, transactions, privacy, and data is considered the top priority for the success of mobile banking services among clients (Almaiah et al., 2023; Cele, 2024; Wilson et al., 2021).

1.8 Assumptions

The following assumptions have been made about this study.

- The participants are a good representation of the digitally engaged population.
- Participants must have engaged with digital banking applications and have experience.
- Participants have provided honest, candid, and unbiased responses to the interview questions to the best of their knowledge and ability.

- The findings from participants will apply to all digital-only banks in South Africa.

1.9 Report Outline

1.9.1 *Introduction*

Chapter one highlights the research purpose, background, problem, objectives, rationale, delimitations, definition of terms, assumptions, and report outline.

1.9.2 *Literature Review and Theoretical frameworks*

Chapter two provides definitions of key terms and review of associated literature for Digital natives, Digital-only banks, and Risk and Security of digital-only banks. The chapter also discusses theoretical frameworks underpinning the study; Perceived risk theory (PRT) and Technology acceptance theory (TAM).

1.9.3 *Research Methodology*

Chapter three outlines the research paradigm, approach, design, data collection methods, population, sampling methods, research instrument, data collection procedures, data analysis, quality assurance and ethical considerations.

1.9.4 *Presentation of Findings*

Chapter four provides a view of the data collected from the semi-structured interviews and highlights the key themes identified, as well as linking of themes to the objectives of the study and theoretical frameworks.

1.9.5 *Discussion of Findings*

Chapter five provides a view of the analysis of the data and highlights the results in alignment with the research objectives.

1.9.6 *Conclusion and recommendations*

Chapter Six concludes the research report, highlights the limitations of the study, and offers recommendations and suggestions for future research.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This chapter reviews the literature on digital banking, risk, and security. It begins by defining digital natives, exploring their characteristics and engagement with digital innovations. The second part elaborates on digital-only banking, followed by examining the associated risks and security issues. Finally, the chapter discusses the theoretical frameworks underpinning the study, specifically the Technology Acceptance Model (TAM) and Perceived Risk Theory.

2.2 Digital natives

The term "digital native," introduced by Prensky (2001), refers to individuals born during the age of technology. This group includes Generation Y (Millennials), born between 1981 and 1996; Generation Z, born between 1997 and 2012; and Generation Alpha, born from 2013 onwards (Howe & Strauss, 2000). Generations Y and Z have only known a world where digital technology is the norm (Çoklar & Tatli, 2021). These generations, often called the iGeneration, have grown up with various technologies, including computers, smartphones, and the internet. Their daily routines seamlessly integrate social media, online music, video on demand, instant messaging, and digital gaming (Sadiku et al., 2017). Assala et al. (2023) refer to digital natives as "Generation Google," "Net-Generation," and "smartphone natives" due to their distinctive ways of learning, communicating, and thinking. Digital natives are described as experimental learners, proficient multitaskers, and highly dependent on information and communication technology (ICT) (Liu et al., 2019; Bennett et al., 2008).

Digital natives represent the largest demographic globally (Thangavel et al., 2021). Stats SA states they constitute approximately 75% of the South African

population. This generation exhibits a high level of digital competence and engagement, making them prime targets for digital innovators, including digital banks (Assala et al., 2023). Smith (2017) and Endsley et al. (2020) highlight that digital natives prefer co-creation in product and service offerings, seeking active participation in shaping the services they consume. Daqar et al. (2020) further note that Millennials and Generation Z demonstrate a strong digital appetite for fintech adoption, underscoring the importance of businesses targeting marketing strategies, particularly in the banking sector.

Although digital natives readily accept digital platforms, they apply specific criteria when engaging with them. This generation is not brand-loyal and will readily switch brands based on perceived benefits (Cahete, 2020). Studies on digital banking adoption conducted in Indonesia (Windasari et al., 2022), Portugal (Cahete, 2020), the United States (Jiang et al., 2022), and Indonesia (Islamic banking) (Yussaivia et al., 2021) all confirm that digital natives are willing to engage with digital banks they trust. However, Jiang et al. (2022) found that trust was not the most critical factor; social influence played a significant role. Digital natives are more likely to adopt brands, including digital banks, recommended by their peers, family, or trusted individuals.

Despite their high engagement with digital platforms, digital natives prioritise data security, particularly in digital banking (Assala et al., 2023). This aligns with Hakimi et al. (2023), who assert that while convenience and ease of use are essential, the perceived security of digital banking platforms significantly influences adoption. A study in Portugal found that Millennials preferred digital banking due to its efficiency, speed, and superior service quality compared to traditional banking (Cahete, 2020).

2.3 Digital-only banks

Digital banking, as defined by the Financial Sector Conduct Authority (FSCA, 2021), refers to transforming traditional banking services into digital formats, allowing clients access to financial services at their convenience. These services are delivered through various platforms, including point-of-sale (POS) systems, USSD, online, and mobile banking. Digital banking encompasses electronic, internet, and online banking (Alkhowaiter, 2020; Windasari et al., 2022). Digital-only banks, also known as virtual banks, provide similar services to traditional banks but operate entirely on digital infrastructure without physical branches (Windasari et al., 2022). Nel and Boshoff (2021) describe digital-only banks as "challenger banks" due to their disruptive innovations in banking.

Unlike traditional banking, which requires physical presence and is bound by operating hours, digital-only banking improves financial inclusion, particularly in underserved communities. The South African banking landscape has historically presented access challenges, contributing to financial exclusion. However, introducing digital-only banks, such as TymeBank, founded on financial inclusion principles, has significantly improved accessibility (Jeník, 2022). Digital-only banks allow users to conduct banking transactions anywhere and anytime, eliminating the need for physical branches. Previously, customers had to visit branches, often requiring extensive travel, especially for those in rural areas. However, digital banking is not without challenges in South Africa. Internet connectivity issues, high smartphone costs, and expensive mobile data remain significant barriers (Mdluli, 2022). Power outages, poor ICT infrastructure, low digital literacy, particularly among older generations, and poverty further impede adoption (Mdluli, 2022).

Digital-only banking enhances customer experience, improves security, and lowers operational costs (Saif et al., 2024; Jeník et al., 2020; Shahabi et al., 2020). Ofodile et al. (2024) note that digital banking offers benefits such as affordability, convenience, and financial inclusion, positively impacting Sub-Saharan African economies. South African banks typically offer both traditional

and digital banking services. However, the country's first fully digital-only banks—TymeBank (2019), Discovery Bank (2019), and Bank Zero (2021)—have introduced a new era of banking. These banks leverage partnerships with retailers to facilitate services like cash withdrawals without needing dedicated brick-and-mortar facilities. This approach reduces operational costs, offering these banks competitive pricing (Saif et al., 2022).

A study by Khedmatgozar (2021) highlights the convenience of digital banking, providing 24/7 access through multiple channels. An analysis by PwC (2024) revealed that the number of digitally active customers in South Africa increased from 17.5 million in 2022 to 18.5 million in 2023, an 8.8% growth. This increase presents an opportunity for digital-only banks. Anggraeni et al. (2021) argue that user habits cultivated during the COVID-19 pandemic, when consumers increasingly relied on digital platforms, could further drive digital banking adoption. Other determinants include the ability to meet customer needs, perceived price value, and specific motivations for adoption (Harahap et al., 2023; Nel & Boshoff, 2021). Digital natives are more likely to engage with platforms that provide unique benefits, such as rewards attached to digital banking (Yussaivia et al., 2021).

2.4 Risk and security of digital-only banks in South Africa.

Digital banking is an evolving financial ecosystem that uses advanced technology to facilitate transactions. Digital-only banking requires internet-connected smart devices to access banking applications, offering both convenience and heightened security risks (Saif et al., 2024). These risks may result in security breaches and financial losses, manifesting through vulnerabilities such as weak passwords, social engineering attacks, phishing, and malware infections. The Financial Sector Outlook study (2022) highlighted that the transition to digital banking created new opportunities for fraudsters, with online impersonation fraud increasing by 337% in 2020. This surge in cybercrime, including social

engineering and phishing scams targeting both bank employees and consumers, presents a significant barrier to adoption (Kuraku, 2024 & Kayode-Ajala, 2023).

Cybersecurity breaches lead to financial losses and damage a company's reputation, ultimately affecting consumer trust (Hassan & Ahmed, 2023; Hakimi et al., 2023). In South Africa, cybercriminals frequently employ SIM-swapping fraud, where fraudsters assume control of victims' mobile numbers to bypass security measures and access banking accounts. The South African Banking Risk Information Centre (SABRIC, 2022) reported a 24% increase in digital banking fraud cases compared to the previous year, highlighting the urgent need for enhanced security measures.

The human factor remains a primary vulnerability in cybersecurity. Phishing scams and social engineering attacks have become increasingly prevalent, often distributed via SMS and email with malicious links to steal data. These attacks also target banking employees, and when successful, they can lead to customer data breaches and unauthorised account access. Kuraku (2024) explores the complexity of social engineering threats, emphasising the psychological manipulation of deceiving users into divulging confidential information. The 2021 Experian data breach, in which the personal information of over 24 million South Africans was compromised through social engineering tactics, exemplifies the real-world impact of such threats (SABRIC, 2021). Moinescu et al. (2019) identify human error as a key vulnerability in security breaches, reinforcing the importance of consumer education and awareness initiatives. Studies by Zvavandanga (2024), Chawla et al. (2023), and Hassan & Ahmed (2023) indicate that increasing digital literacy not only strengthens security but also enhances consumer trust and satisfaction. Babikian (2024) also argues that safeguarding data privacy requires a multi-faceted approach that includes regulatory compliance, technological innovation, corporate responsibility, and user empowerment. Robust cybersecurity frameworks are essential for protecting consumer information as digital banking expands.

Countries such as the United Kingdom and Singapore have implemented stringent cybersecurity regulations that serve as benchmarks for South Africa. The UK's Financial Conduct Authority (FCA) mandates strong customer authentication, while Singapore's Cyber Security Agency (CSA) enforces rigorous compliance measures. These best practices highlight the importance of regulatory oversight in mitigating digital banking risks (Smith & Wong, 2023).

Digital-only banks have made significant investments in cybersecurity to strengthen platform security. These initiatives include deploying artificial intelligence (AI) algorithms for fraud detection, introducing multi-factor authentication, and integrating biometric technologies. Technological advancements, such as biometric authentication, have significantly improved banking security and bolstered consumer confidence (Morake et al., 2021; Piotrowska, 2024). However, biometric security measures require active consumer participation, as users must enable these features on their devices. This creates a security gap for users who opt not to activate these safeguards. The adoption of security measures varies across demographics, with younger, tech-savvy individuals more likely to implement security best practices compared to older generations, who may prefer simpler solutions (Morake et al., 2021; Piotrowska, 2024; Mudduluru, 2024). Despite these advancements, hesitancy regarding digital-only banking adoption remains. In South Africa, reluctance is primarily driven by concerns about overexposing sensitive information to cybercriminals (Cele, 2024). This aligns with findings from Almaiah et al. (2023), Slazus and Bick (2022), and Baraba and Mahmudi (2023), who highlight that perceived risk and security concerns significantly negatively influence adoption rates.

Beyond cybersecurity risks, consumer perceptions also play a crucial role in adopting digital-only banking. The absence of a physical branch, which provides reassurance when resolving issues, is a major challenge for digital banks. Users who prefer traditional banking often resist digital-only alternatives and may discourage those in their immediate circles from adopting them. Nel and Boshoff

(2020) examined how traditional bank customers' negative perceptions hinder digital-only banking adoption in South Africa. Their study found that these consumers resisted digital banking and actively spread negative sentiments, further slowing adoption rates. Digital natives, the highest adopters of digital platforms, rely on social influence when making purchasing decisions and selecting financial service providers. Windasari et al. (2022) highlighted that digital natives are more connected to peers, have a strong social conscience, and consider opinions from friends and fellow consumers as a reliable basis for adoption decisions. Not actively managed perceptions could lead to negative sentiments and negatively impact adoption (Yussaivia et al., 2021; Cahete, 2020). Digital-only banks must actively manage the risk around reputation and brand. Similar findings by Anggraeni et al. (2021) suggest that social influence is a key driver of digital banking adoption in Indonesia. However, their study also highlights that positive experiences from existing users can significantly impact prospective users' willingness to embrace digital-only banking services. Digital-only banks must implement targeted education and communication strategies to counteract negative perceptions. In South Africa, digital-only banks like TymeBank have launched financial literacy programmes and transparent security communication initiatives to address consumer concerns (TymeBank Annual Report, 2023).

To foster trust, digital-only banks must proactively communicate their security measures to customers. Chawla et al. (2023) argue that transparency in security protocols enhances consumer confidence and encourages adoption. Similarly, Hakimi et al. (2023) highlight that strategic communication is vital in managing risk perceptions. Jiang et al. (2022) stress that effective communication by financial institutions can create a secure transaction environment, thereby reducing perceived risks and improving consumer trust in digital banking. Despite technological advancements, digital-only banking customers report lower satisfaction levels, largely due to security concerns. Salqaura et al. (2023) found that fears over data breaches and password security contribute significantly to consumer dissatisfaction. Wilson et al. (2021) reinforce these findings,

demonstrating that perceived security is a key determinant in consumers' willingness to adopt mobile payment services. Almaiah et al. (2023) further argue that perceived security, trust, and service quality are fundamental drivers of adoption, while perceived risk negatively influences consumer attitudes towards digital banking. Given these concerns, digital-only banks must deepen their understanding of customer apprehensions and proactively address them to build trust and ensure long-term sustainability.

This review underscores the complex relationship between risk, security, consumer perception, and the adoption of digital-only banking in South Africa.

2.5 Theoretical framework

This section discusses the theoretical frameworks that underpin the study, Perceived risk theory (PRT) and Technology acceptance model (TAM).

2.5.1 *Perceived Risk Theory*

Several studies have been conducted to understand customer behaviour and how they perceive risk when accepting and using new technology (Xie et al.,2021; Almaiah et al., 2023). Multiple definitions have emerged from the studies. Chiu et al. (2012) defined perceived risk as the customer's perception of distrust and potential adverse outcomes of using or buying a product or service. Cox and Rich (1964) define perceived risk as the nature and amount of risk perceived by consumers in purchasing decisions and as the main determinant of a person's behaviour in adopting the technology. Khedmatgozar and Shahnazi (2018) also define perceived risk as the individual's thoughts and belief in the likelihood of having an adverse outcome and consequence in using technology. This is the customer's worry or concern about using a particular product/ platform or service. When customers feel there is a high potential for loss in using digital-only banks, they will have little to no appetite for using digital-only banks. This is supported by Xie et al. (2021).

Bauer (1967), in his perceived risk theory, characterised consumers as either risk-taking or risk-reducing. Further, he explained that perceived risk has multiple dimensions that consumers consider before purchasing. Some of the risk dimensions that are specific to digital banking include performance risk, financial risk, privacy risk, time risk and security risk (Alkhowaiter, 2020; Ali et al.,2021; Khedmatgozar, 2021; Reepu & Arora, 2022). **Performance risk**: The risk that a product or service may not meet the consumer's expectations regarding performance (Tiwari & Tiwari., 2020). In the context of digital-only banking, this would include issues such as application downtime, slow platform performance, or any other platform performance issues. **Financial risk**: the risk of financial loss. In digital banking, this includes the fear that the bank may not incentivise the customer when something goes wrong in the banking application itself (Khedmatgozar, 2021). An example is the application timing out while processing a payment before a transaction is concluded. **Privacy risk**: the risk that customers may not have control of their data; an example would be cyber-attacks that steal customer data (Baraba & Mahmudi, 2023). **Time risk:** the risk of the time that a customer needs to learn and understand how a new technology works (Khedmatgozar, 2021). Moreover, last, **Security risk**: the risk that the digital platform will compromise sensitive information such as security codes and PINs (Aldammagh et al., 2021). This can also be a cyber security concern, such as hacking or online fraud.

Thusi and Maduku (2020) concluded a study on millennials' intentions to adopt mobile retail banking in South Africa. It was found that perceived risk is one of the determinants that significantly impact the intentions of millennials to accept mobile banking. If users perceived the risk as high, they would not accept the mobile banking app. Another study by Ali et al. (2021), investigated determinants of perceived risk and perceived benefits in Fintech. The researchers also assessed the relationship of those determinants to Fintech adoption. It was found that perceived risk was influenced by financial, legal, security and operational risk. This further demonstrates the significance of digital banks in understanding

risks from the customers' perspective and implementing strategies that will minimise the risks.

2.5.2 *Technology Acceptance Model (TAM)*

The Technology Acceptance Model (TAM) is a widely recognised framework for predicting human intention to adopt technology (Hu et al., 2019). Originally developed by Davis (1989) and rooted in the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975), TAM explains user acceptance based on two key factors: Perceived Usefulness (PU)—the belief that using a particular technology enhances performance—and Perceived Ease of Use (PEOU)—the belief that using the technology requires minimal effort. The model seeks to answer why users accept or reject technology and how system design influences acceptance. TAM has been widely applied in technology adoption research, including studies on Fintech, mobile money services, and branchless banking (Slazus & Bick, 2022; Njele & Phiri, 2021; Almaiah et al., 2023). In the context of digital-only banks, TAM has been instrumental in identifying factors that influence adoption, particularly among digital natives, who prioritise trust, ongoing risk management, and security when selecting a financial service provider (Chawla et al., 2023). Research has found that perceived quality, ease of use, risk, usability, and security influence customer experience in digital banking (Windasari et al., 2022). Moreover, Almaiah et al. (2023) highlight that perceived security is crucial in determining mobile banking adoption, as it fosters trust and comfort in digital transactions. This study explores digital natives' perceptions of risk and security in digital-only banking, making TAM a suitable framework for understanding their adoption behaviour. If digital natives perceive digital-only banks as insecure, their Perceived Usefulness (PU) will be low, discouraging adoption. Similarly, if security features are overly complex, their Perceived Ease of Use (PEOU) may be compromised, impacting user engagement. By applying TAM, this study examines how risk and security concerns shape digital natives’ willingness to adopt digital-only banking. The insights gained will strengthen security strategies, ultimately enhancing user confidence and adoption rates.

2.6 Conclusion

This literature review critically examined digital-only banking, risk, and security within the context of digital natives in South Africa. It explored the factors influencing digital banking adoption, the risks perceived by digital natives, and the theoretical frameworks underpinning their engagement with digital banking platforms.

The review highlighted that digital natives, characterised by their high digital literacy and preference for convenience, are key adopters of digital-only banking. However, their adoption is influenced by various factors, including perceived risk and security. Studies indicate that while digital natives are more inclined to embrace digital financial services, their engagement is conditional upon trust, security, and peer influence. Trust plays a critical role in adoption, but social influence often outweighs trust in shaping consumer behaviour. These findings reinforce global trends while providing a nuanced understanding of South Africa's digital banking landscape. The analysis of digital-only banks in South Africa revealed significant advancements in accessibility, financial inclusion, and cost efficiency. Banks such as TymeBank, Discovery Bank, and Bank Zero have disrupted the traditional banking sector by offering innovative digital solutions. Despite these benefits, South Africa's digital banking landscape faces unique challenges, including cybersecurity threats, internet connectivity issues, and socio-economic barriers such as digital literacy and financial exclusion. The literature emphasised the importance of security in digital banking adoption, with studies demonstrating that risks such as phishing, malware attacks, and SIM-swapping fraud hinder consumer confidence. The prevalence of cybercrime in South Africa underscores the critical need for robust security measures and regulatory frameworks to protect consumers.

From a theoretical perspective, the review engaged with the Perceived Risk Theory and the Technology Acceptance Model (TAM) to contextualise digital banking adoption. The Perceived Risk Theory suggests that consumers assess multiple risk dimensions—including financial, security, and privacy risks—before

adopting digital-only banking. Studies indicate that heightened perceived risk negatively impacts adoption, reinforcing the need for banks to prioritise cybersecurity measures and transparent communication. Similarly, TAM underscores the significance of Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) in influencing adoption. If digital-only banks fail to address security concerns, their perceived usefulness diminishes, discouraging adoption. This highlights the necessity for user-friendly yet highly secure banking platforms.

The findings of this study contribute to existing knowledge by confirming global trends while emphasising the unique contextual factors affecting digital banking adoption in South Africa. While studies from countries such as Indonesia, Portugal, and the United States highlight similar concerns around trust and security, South Africa's challenges are compounded by infrastructure limitations and high cybercrime rates. Furthermore, the role of social influence in adoption suggests that digital-only banks must address security concerns and leverage positive consumer experiences to build credibility.

While digital-only banking presents significant opportunities for financial inclusion and innovation in South Africa, the associated risks remain a substantial barrier to adoption. This review underscores the importance of targeted risk mitigation strategies, regulatory interventions, and consumer education initiatives to foster trust in digital banking. Digital-only banks must continuously evolve their security frameworks and communicate transparently to mitigate perceived risks and enhance adoption among digital natives. Addressing these challenges will be pivotal in shaping the future of digital banking in South Africa.

CHAPTER 3. RESEARCH METHODOLOGY

The previous chapter provided a literature review relevant to this study. It first focused on literature around digital-only banks, followed by a description of digital natives, highlighting some of their characteristics based on existing literature, and a discussion of the risks and security associated with digital-only banks. It also discussed the theoretical frameworks relevant to the study: Technology Acceptance Model (TAM) and Perceived Risk Theory (PRT). This chapter outlines how the research was conducted. It begins with a discussion of the research approach, followed by the research design, sample and population, data collection and analysis methods. It further specifies some of the study's limitations and moves on to ethical considerations.

3.1 Research Paradigm

This study adopted the interpretivism paradigm, which seeks to understand human experiences, social realities, and meanings from participants' perspectives. Interpretivism assumes that truth is subjective and varies from person to person (Krauss, 2015; Creswell, 2013). It values individual contributions and aims to generate in-depth, rich insights from the data collected. This paradigm considers participants' feelings, context, experiences, and how they make sense of the world (Husam & Pius, 2020). It is widely used in studies that explore perceptions, beliefs, and cultural meanings.

One of the key strengths of interpretivism is its ability to provide rich, context-specific insights; however, it has been criticised for its lack of generalisability, as findings are often limited to specific settings (Creswell, 2013). Additionally, the approach is highly subjective, as results rely on the researcher’s interpretations rather than measurable facts (Bryman, 2016). Despite these criticisms, interpretivism is well-suited to this study, as it allowed for a deeper exploration of digital natives’ risk and security concerns in digital-only banking. This nuanced

understanding can inform banking strategies and contribute to building customer trust.

3.2 Research approach

This study employed a qualitative research approach to explore digital natives' perceptions of the risks and security of digital-only banks. A qualitative approach is suitable when a complex issue requires an in-depth understanding (Creswell, 2007). This method enriches respondents' beliefs, experiences, and values while allowing researchers to develop theories that capture these experiences. The nature of a qualitative study enables detailed questions to elicit comprehensive responses that fully address the research objectives (Alamri, 2019).

In this study, understanding digital natives' perceptions required in-depth discussions to give the researcher deep insights into their perspectives. This level of exploration cannot be achieved using numerical approaches; instead, it required direct conversations to understand participants' beliefs, experiences, and values. Therefore, a qualitative approach is the most appropriate for this study.

3.3 Research design

The study followed a general qualitative design. According to Caelli et al. (2003), generic qualitative research is characterised by flexibility, adaptability, and practicality, as it is not bound by the specific philosophical assumptions or methodological frameworks of established qualitative traditions; it allows for a more flexible and responsive research process. This approach is useful for understanding perceptions and real-world experiences related to the explored problem. The current study does not fit neatly into specific qualitative methodologies such as phenomenology, grounded theory, or ethnography. Therefore, a general qualitative design was chosen to integrate principles from various methods, ensuring the research objectives are achieved. Flexibility is

essential for capturing the complex and dynamic nature of the participants' experiences and perceptions.

While generic qualitative research has been criticised for lacking a theoretical basis and mixing methodologies, proponents argue that the need for methodological innovation and adaptation outweighs these difficulties (Kahlke, 2014). To address the criticisms of generic qualitative research, such as the lack of a theoretical basis and potential methodological contradictions (Kahlke, 2014), the study implemented the following measures:

- All research processes and decisions are documented to ensure transparency and provide a clear guide for those interested in replicating the study in different contexts.
- The researcher engaged in reflexive practices, critically examining their own biases and influence on the research process to ensure the credibility of findings.
- The research design, data collection methods, and findings were subjected to supervisor review to identify inconsistencies or contradictions.

Ahmed (2024) highlights that following a methodical application of measures to ensure improved trustworthiness, precision, transparency, and reliability addresses criticism around qualitative findings and their subjectivity. To ensure quality and rigor, the researcher applied the quality checks process proposed by Guba and Lincoln (1986).

3.4 Data collection methods

Data was collected through semi-structured interviews conducted on a one-on-one basis. These interviews followed a predefined set of open-ended questions to facilitate conversation and encourage participants to express their views about specific issues in detail. Hennink et al. (2020) highlight that through semi-structured interviews, the interviewer and participant co-create knowledge and

co-construct reality based on the setting and connection. Alamri (2019) highlights this method's advantages and disadvantages.

Advantages

- The data collection method offers the interviewer flexibility in that the interviewer can change the question to gather richer insights from the participant,
- the interviewer can clarify questions during the interview, which helps increase the accuracy of the data.

Disadvantages

- This method is time-consuming, as data collection and analysis are required.
- Participants may be concerned about acceptable norms about the topic instead of expressing their opinions and beliefs which can take away the truthfulness of the data.

There was flexibility in conducting the interviews either in person or online. With the participant's consent, the interviews were recorded. This data collection was appropriate for this study because it allowed the researcher to obtain detailed participant perspectives based on their experiences and motivations (Cresswell, 2007). Additionally, the researcher could modify the questions during the interviews based on participants' responses. This flexibility ensured focus and clarity and enabled the incorporation of new insights during the process, ensuring that the study's objectives were met.

3.5 Population and sample

3.5.1 *Population*

The population of the study was digital natives. Digital natives include everyone born from 1981 to date. However, the focus was on digital natives legally allowed to open a bank account without a guardian. In South Africa, people can have a bank account without guardian consent from 18. Therefore, the population was digital natives who were 18 years old but not over 43 in 2024. Participants were required to have a bank account so that they can be able to engage the topic from lived experiences.

3.5.2 *Sample and sampling method*

Based on the objectives of this study, the participants selected had some level of understanding of what risk and security mean, as well as what digital-only banks are. The concept of digital-only banks is new in South Africa; it cannot be assumed that there is enough awareness of their existence amongst all digital natives. The study employed purposive sampling to ensure that participants offered in-depth, appropriate, and valuable knowledge in their responses, which addressed the research objectives (Campbell et al., 2020). Shaheen et al. (2019) expressed that qualitative research is considered meaningful if the sample selected is information-rich and the analytical capabilities of the researcher are high. The study aimed to interview 12 participants chosen by the researcher based on their understanding of the topics. In qualitative research, sample size is determined by the depth of insight rather than statistical representativity. A sample of 12 participants is justifiable based on the principles of data saturation, methodological considerations, and alignment with qualitative research standards. Data saturation occurs when no new data themes, patterns, or insights emerge, indicating that additional participants would not contribute substantially new information (Guest et al., 2006; Hennink & Kaiser, 2022). In many qualitative studies, particularly those using thematic analysis, saturation is often reached

with 12 to 15 participants, depending on the research question's complexity and the sample's homogeneity (Braun & Clarke, 2006). Since this study explored lived experiences and perceptions, a sample of 12 participants allows for sufficient depth while ensuring a manageable dataset for rigorous analysis. Qualitative research prioritises rich, detailed data over large sample sizes (Creswell & Poth, 2018). Unlike quantitative studies, which rely on statistical power, qualitative research focuses on meaning-making through in-depth participant engagement (Merriam, 2002). A smaller, purposive sample ensures deep exploration of participants' experiences. Lastly, the thematic analysis approach (Braun & Clarke, 2006) does not require a large sample to generate meaningful themes. In studies where interviews are the primary data collection method, a sample of 6 to 12 participants is commonly used. Numerous qualitative studies have utilised small samples to generate rich and meaningful insights. Guest et al. (2006) found that saturation often occurs within 12 interviews, while Braun and Clarke (2013) argue that a sample of 10 to 15 participants is generally sufficient for thematic analysis. For the current study, a saturation point was reached after 11 interviews; the number was revised to 11 participants.

3.6 The research instrument

Primary data was collected through semi-structured, one-on-one interviews with selected participants. A set of open-ended questions was prepared in advance to serve as a guide for the interviews. The interview guide, attached in Appendix C, was developed in alignment with the study’s objectives to ensure a comprehensive exploration of digital natives’ perceptions of risk and security in digital-only banking. The questionnaire was informed by relevant theoretical frameworks, particularly Perceived Risk Theory (PRT) and the Technology Acceptance Model (TAM), to facilitate an understanding of key factors influencing the adoption of digital-only banks, such as risk perceptions, security concerns, and usability.

The interview questionnaire was structured into the following sections:

- **Background Information**—To understand participants' familiarity with and engagement with digital banking and to create a comfortable environment for discussion.
- **Knowledge of Digital-Only Banks** – To assess participants' awareness and perceived significance of digital-only banking.
- **Perceptions of Risk and Security** – To explore participants' security concerns, awareness of digital banking risks, and their impact on adoption.
- **Criteria for Selecting a Digital Bank** – To identify key factors influencing participants' choice of a digital-only bank.
- **Risk Mitigation Strategies** – To gather participants' recommendations on enhancing security and reducing risk in digital banking.

Interviews were scheduled to last between 30 and 45 minutes to allow sufficient time to build rapport with participants. The interview guide was piloted with two participants to assess language clarity, ensure question interpretation consistency, and identify potential misunderstandings. Based on the feedback received, the questionnaire was refined to improve clarity and effectiveness. This iterative approach facilitated a co-constructive process between the researcher and the participants (Creswell et al., 2007).

Semi-structured interviews were selected for this study's data collection method due to their flexibility and ability to provide in-depth insights into participants' lived experiences. This method enabled participants to express their thoughts freely, offering a richer understanding of their perspectives (Qu & Dumay, 2011). The interview guide was also designed to adhere to ethical research principles. Questions were carefully framed to minimise discomfort or bias, and participants were informed that they could decline to answer any sensitive question. By adopting this approach, the study ensured that the research instrument was well-structured, theoretically grounded, and capable of capturing meaningful insights into digital natives' perceptions of digital-only banking security and risk.

3.7 Procedure for data collection

The researcher approached potential participants directly. The purpose and context of the study were explained informally to provide enough information for the participant to make an informed decision. Participation criteria were discussed during this informal conversation to ensure the potential participant understood the topics. Potential participants were verbally asked to participate. Upon verbal consent, an email was sent with a detailed explanation of the study and a formal consent request. The email included a consent letter outlining the study's purpose, process, and confidentiality measures. Participants were requested to sign and return the consent form if they willingly agreed to participate. Once signed consent was returned, the interview was scheduled with the participant. Most interviews were conducted on Microsoft Teams, with one being in person. Before the interview, the researcher reiterated the purpose of the study, informed participants that they were allowed to withdraw at any time, and re-iterated that the interview was recorded. After a second verbal consent to proceed, the recording and interview started. The interviews were recorded, and transcription was enabled, using Otter AI software. Participants were candid with their responses. After the interview, Interviewer listened to the recordings and edited the transcription to ensure accuracy. Transcription was verbatim to capture detailed accounts of participants' experiences and perspectives. Once the transcription process was complete, it was sent to two participants to confirm accuracy; thereafter, the transcripts were used for coding and thematic analysis to identify key themes and patterns relevant to the research objectives.

3.8 Data analysis and interpretation

This study aimed to gain in-depth insights into the perspectives, emotions, and lived experiences of risk and security in digital-only banking. Thematic analysis was used as the primary method of data analysis. Thematic analysis is a widely recognised qualitative approach that focuses on identifying, analysing, and reporting patterns (or ‘themes’) within the data, which provides rich insights into

participants' lived experiences and perceptions (Braun & Clarke, 2006; Guest et al., 2012).

Data was collected through one-on-one interviews, which were recorded and transcribed verbatim. Once the transcription process was complete, the researchers familiarised themselves with the data by reading through the transcripts to gain a comprehensive understanding and identify initial impressions. The transcripts were then uploaded into ATLAS. ti, qualitative data analysis software, to facilitate systematic coding and organisation of the data. Coding was conducted using a combination of manual coding and software-assisted analysis. This dual approach was adopted to ensure analytical rigour and accuracy. Manual coding allowed the researcher to engage deeply with the data, capturing nuances in language and meaning while ATLAS.ti provided a more efficient and structured way of managing, retrieving, and categorising the data.

The coding process was iterative and continued until the researcher was confident that the codes adequately captured the key themes and ideas within the data. Once the initial codes were established, they were grouped into themes representing the key patterns identified in the data. These themes were then reviewed, refined, and revisited to ensure they accurately represented participants' lived experiences. The analysis followed the six-step process outlined by Braun and Clarke (2006) and Guest et al. (2012):

- **Familiarising oneself with the data**: Reading and re-reading the transcripts to thoroughly understand the content.
- **Generating initial codes**: Identifying meaningful features of the data that were relevant to the research questions.
- **Searching for themes**: Grouping the initial codes into broader themes that reflected major patterns.
- **Reviewing themes**: Ensuring the identified themes accurately represented the data and refining them where necessary.

- **Defining and naming themes**: Clearly articulating the essence of each theme, defining its scope, and explaining its significance.
- **Documenting the findings**: Presenting the identified themes coherently and structured, supported by illustrative quotes from the data to provide deeper insight into the analysis.

In qualitative research, it is important to maintain trustworthiness and credibility (Kahlke, 2014). To enhance these aspects, reflexivity was maintained throughout the data analysis process. The researcher reflected on their own potential biases, acknowledging that their personal experiences and perspectives may have influenced the interpretation of the data. This process of self-reflection helped ensure a more transparent and balanced analysis. To further support the trustworthiness of the findings, strategies such as member checking were employed, where participants were asked to review the analysis to ensure the findings accurately reflected their experiences.

3.9 Quality Assurance

3.9.1 *Transferability*

Transferability refers to the extent to which the research findings can be applicable in a different context Ahmed (2024). In this this report, transferability has been achieved through the detailed description of the research context, methodology, processes, and resultant final report. The data collection methodology and experience are detailed to contribute to a better and more comprehensive understanding of the research context. Although this research is focused on digital natives and their risk and perceptions regarding digital-only banks in South Africa, the results can be applied to other contexts, such as outside of South Africa and yield similar findings.

3.9.2 *Credibility*

Enworo (2023) describes credibility in qualitative research as the degree in which the research findings accurately represent the reality of the participants and their experiences. Devault (2019) also highlighted that triangulation and member checks assist in establishing credibility and contribute to the trustworthiness of the research study. Participant checks were conducted with some of the individual participants once the initial data had been transcribed and analysed to check against any biases and misrepresentations that could have occurred during the analysis and interpretation of the results. This validated that the participants' meanings were captured correctly and ensured that the researcher maintained objectivity throughout the process, thus ensuring credibility.

3.9.3 *Dependability*

Dependability is the consistency of results over time (Kakar et al., 2023). It is also described as data consistency over a similar context (Enworo, 2023). Transparency throughout the process has been maintained. Documentation such as transcripts (without participants' identifiers), interview guides, and data collection and analysis processes can be made available. The detailed process and decisions are documented in detail in this report to allow for enough audit trail so that the study can replicated by other researchers.

3.10 Ethical considerations

The Wits Business School ethical guidelines were followed. The process only commenced once the ethics clearance certificate from the ethics committee was issued to the researcher. Prior engagement about the research objectives was communicated, and consent was obtained in writing from all potential participants. Participants were advised of the process to ensure anonymity by removing any reference to the participant's names, to respect their privacy and to maintain confidentiality throughout the study. The participants were notified that

the interviews were recorded, and the purpose was highlighted with them. Participants were also made aware that they were not obligated to respond to all questions; they were also made aware that they could withdraw from the process at any time without any consequences. Participation was voluntary, and no participants were incentivised to participate. All information about the study was stored in a password-protected computer.

CHAPTER 4. PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents the results and findings from the qualitative study conducted through semi-structured interviews with digital natives. The interviews were designed to explore perceptions of risks and security levels associated with digital-only banks. Specifically, the questions aimed to gather insights into how these perceptions influence the intention to adopt digital-only banking and to identify recommendations for reducing risks and improving security. The findings were analysed using thematic analysis to uncover key themes and insights. The chapter is organised into five sections: Introduction, Demographics of participants, Data analysis process, and Presentation of emerging themes and interview results, followed by the conclusion.

4.2 Demographic profile of participants

The data was collected from 11 participants who meet the definition of digital natives who were between the ages of 18 and 43 in 2024. The participants were required to have a bank account in any of the banks in South Africa or be eligible to acquire one. They also had to understand the key concepts of risk, security, and digital banking. The table below represents the profiles of the participants.

Table 1 – Participant demographics

Participant	Age range	Gender	Digital-Only Bank
1	36 - 43	Male	User
2	30 - 35	Male	User
3	36 -43	Female	Non-User

4	36 -43	Male	User
5	30 - 35	Female	Non-User
6	26 - 29	Female	User
7	18 - 25	Male	User
8	26 - 29	Male	Non-User
9	26 - 29	Male	User
10	36 -43	Male	User
11	26 - 29	Female	Non-User

4.3 Data analysis process

The data collected from the semi-structured interviews were analysed using a thematic analysis approach, following the six steps outlined by Braun and Clarke (2006). The data collected from the interviews was recorded and transcribed using software. The researcher listened to the recording and validated the transcript to ensure accuracy. The transcripts were captured verbatim. Once that process was completed, the transcripts were uploaded into the qualitative analysis software ATLAS.ti for coding purposes. The researchers familiarised themselves with the data, and once they were comfortable, the analysis and coding process started. A combination of manual coding and the ATLAS. ti software was used to analyse the data. This approach was employed to ensure accuracy and maintain rigour in the analysis. The manual process allowed the researcher to engage deeply with the data and interpret nuanced meanings using ATLAS. ti provided a systematic and efficient way to identify patterns and organise codes. Cross-checking between the two methods further enhanced the reliability of the findings and minimised the risk of overlooking important patterns or themes. Analysing the transcribed document involved listening and reading the interview, picking out the most important participant input, and then classifying

the feedback based on comparable meanings. The coding process aims to highlight similarities between the data, group the data into categories, and identify common themes across the data. The process was iterative until the researcher addressed the research questions sufficiently and narrowed the themes into themes that sufficiently addressed the research questions.

4.4 Theme development

The is study aims to understand customer experiences with digital-only banks in South Africa amongst digital natives, specifically focusing on their perceived risks and security. The research objectives of the study are:

- To explore what digital natives consider risks and security levels in South Africa's digital-only banking.
- To explore how the perceived risk and security influence Digital natives' intention to adopt Digital-only banking.
- To understand from digital natives what measures digital-only banks in South Africa can prioritise to reduce risks and improve security.

As such, the following themes emerged from the data:

- Security and Risk levels of Digital only banks
- Digital-only bank's adoption factors
- Measures to enhance security and reduce risks
- Strategic Role and Opportunities of Digital-Only Banking

Theme 1: Security and Risk Levels of Digital banks

This theme explores multiple aspects of security and risk in Digital-only banking. It highlights existing sentiments from participants and what they consider to be the levels of security and risks; it further highlights the vulnerabilities and measures that are currently in place. Sub-themes under this theme include:

- **Institution and platform security measures** – This highlights existing security measures employed by digital- only banks to protect users, as well as internal risks applicable to banks.
- **Device security measures and vulnerabilities**– These are device security features that consumers can enable to increase security of their devices, as well as gaps from the device.
- **Digital-Only bank sentiments** – This sub-theme captures perceptions about the safety of this form of banking.
- **Online threats** – This sub-theme captures cyber-attacks that can threated digital-only banks, including social engineering.
- **Service availability threats** – This sub-theme highlights risks to the availability on the actual bank platform.

Theme 2: Digital-only banks adoption factors

The theme explores various factors that participants highlighted as critical for digital-only banking adoption. These include motivations for adoption, challenges, and criteria that consumers used to select the digital-only bank.

- **Adoption challenges**—This sub-theme groups all challenges that hinder adoption. The challenges rank from infrastructure to technology to demographics to technical abilities.
- **Adoption drivers** – This sub-theme groups all motivating factors for users adopting digital-only banking. These range from convenience of the platforms, advanced technology access, as well as ease of use.
- **Bank selection criteria**—This sub-theme highlights different decision factors that inform consumer choice when selecting a digital-only bank.

Theme 3: Measures to enhance security and reduce risks

This theme explores strategies and recommendations to strengthen the security of digital only banking. It highlights consumer-facing measures, digital-only banks specific measures, as well as the role of education and digital awareness.

- **User based enhancements** – This sub-theme highlights safe engagement practices that users can adopt to ensure protection for their accounts.
- **Digital banks enhancements** – This sub-theme focuses on some strategies that banks can implement to enhance security further and reduce risks on their platforms.
- **Education and awareness** – This sub-theme focus on the importance of educations, channels to educate for efficiency and overall awareness.

Theme 4: Strategic Role and Opportunities of Digital-Only Banking

This theme explores the significance of digital-only banking, highlighting their contribution and them being the future of banking. The category further brings in some opportunities for the banks to investigate strategically to cement their place further. This theme includes the following sub-themes:

- **Target Market** – This sub-theme explores who digital-only banking is targeted at.
- **Significance of digital-only banking** - This sub-theme explores the overall contribution of digital-only banking, highlighting its transformative nature to the banking landscape in South Africa.
- **Opportunities for Digital-only banks** – This sub-theme highlights strategic avenues and initiatives banks can pursue to maximise their market share.

4.5 Emerging Themes

This section highlights the themes and sub-themes identified from the data. The themes and sub-themes emerged from the coding process, and similarities have been identified and grouped into sub-themes aligned to the study objectives. Below is a list of themes and descriptions of what they represent.

4.5.1 *Theme 1: Security and Risk levels of Digital-only banks*

This theme explores multiple aspects of security and risk in Digital-only banking. It highlights existing sentiments from participants and what they consider to be the levels of security and risks; it further highlights the vulnerabilities, as well as measures that are currently in place.

a. *Sentiments on Risk and security*

Digital platforms do bring in risks associated with cyber-attacks, as well as attacks through physical devices. Even with that, participants strongly believed that the banking apps are safe, however, the most prominent vulnerability was the human factor. Some participants considered them safe "*when you are aware and cautious of the dangers of digital banking*".

> "*Absolutely, I would say that they are sufficiently secured. And the reason why I'm saying that, like I said earlier, right, there's multiple levels of verification that can be done before the application can be accessed*." - participant 1

> "*I would consider it to be safe, I think from my personal experience so far, I would consider them to be safe*." – Participant 2

> *"I believe it's safe. Because, okay, so let me put it this way, I believe it's safe when you are aware and cautious of the dangers that come with banking digitally*." – Participant 3

Other participants strongly believe that online banking is a safer option than traditional banking due to the absence of physical branches in digital-only banking, which is perceived as taking away a channel to cause security harm.

> *“I consider them safer than traditional banks. I can't say they're absolutely safe. Yes, as an absolute response. But if I had to pick between safe and not safe, I would pick safe.”* – Participant 10

Some participants had different views regarding the safety of the platform. Their view was that should the physical device land in the wrong hands, this would cause a risk to your banking app; when probed if there were more than the banks could do to mitigate that, participant was unclear on the necessary mitigation.

> “*No, like, I don't know what I want them to do, but I feel like, they could do more, yeah, because certain times you'll find that you have you're being debited by someone who's scamming you, you didn't approve that debit order, but it's still going through.”* - Participant 11

Digital-only banks are seen to be proactively prioritising security of their platform and introducing new security features more frequently. There are also new roles in cybersecurity that have emerged which also gives participants comfort that a lot is being done to mitigate adverse outcomes.

> “*Because I think technology has evolved in such a way that security as we know it's now, compared to back in the day, I think it's, it's a very advanced level in terms of data security. And if you look at how banks and pretty much look at Bank budgets, for example, there's much investment going into security of systems on their side, so I think there's an active approach to maintain that. P*articipant 10:

“Every now and then they try to introduce something new and that you sort of enhance the security.” – Participant 9

Technology advancement is seen to bring advancement in cyber threats as well, and digital-only banks have no option but to make sure their platforms are highly secured and stay ahead of the game. It was highlighted that the attackers are highly skilled and well-informed, which puts banking security personnel under pressure.

“I think it also puts them on their toes to say, you must always keep things up to date. So, I do believe they are making an effort.” - Participant 7

Some participants raised the importance of digital-only banks changing some of the perceptions around risk when it comes to online banking. It was mentioned that it is not easy for everyone to understand the technicalities of online banking, but banks needed to reflect and find out how they can educate consumers about platform safety and try to keep it simple and transparent.

“*How do we make sure our customers are understanding how safe our platforms are? And what are we doing to educate the customers on the safety of our platform.”* - Participant 1

No additional risks were identified that are specific only to Digital-only banking. Participants mentioned that the same risks exist across digital-only banking and digital platforms for traditional banks, as highlighted in the extract below.

“So, the same risks that it is how only bank could have a traditional bank would also have, if you ask yes, but a digital bank, the difference would be that it has less risk because it doesn't really have a physical infrastructure that can be, penetrated or something stolen from it. So, it's all it's all virtual. So, I think on that side, it would have less risk.” - Participant 5.

b. ***Risks in digital-only banking***

Cybercrimes are a concern for digital-only banking. Participants highlighted that a lot of activity and verification is happening online, which increases the probability of cybercrimes, including social engineering. Email and SMS Phishing scams are a massive concern for some participants; however, the participants were also in agreement that user education and precaution can eliminate some of them.

> "*Unless you are educated in terms of, like, the different ways, and people are trying to Phish and scam like, I wouldn't consider it safe, okay, you just need to get it on how to use it properly."* – Participant 8

All participants agreed that cybercriminals are getting even more creative in how they run scams; it is important for consumers to consumers need to be responsible and diligent when engaging in banking platforms. Data breaches opened users to cyber-attacks. Participants agree that data protection is a shared responsibility between banks and consumers, as this type of risk can manifest itself from the bank or the consumer or other third parties, such as credit bureaus.

> "*Too often that people are just clicking on everything that they like, clicking on links that you know they would never recognise but why not let me just click on it to see what it is, and you know it's understanding their responsibility when it comes to their information security. I think all too often, people just step away from the responsibility and put it on the third party. But you know, it might, it's, it's your data. You are just as accountable as anybody else."* – Participant 10

> "*Security is something that also it requires the user of that digital bank, or whatever it is that you're using. It requires effort from them. They're not consuming a service, but they must be cautious. So, it requires effort from them. So, how the question should be, how do you get the people to be willing to put in that effort?"* – Participant 7

Digital-only banks are banks on hand due to them being accessed through a mobile phone. With that, participants raised issues around losing the device their banking app is linked to. Participants raised the concern that South Africa has a high crime rate, which further causes concerns about this type of risk. Participant 6 described the loss of the phone as the "*biggest fear*" because you will need another device to contact your bank to alert them to block your account. The longer it takes to secure a device, the more time criminals will have to attempt to penetrate your phone and banking app to access your funds. Some participants shared similar views that due to all activities happening online, should you lose your physical device, the turnaround to securing your account is long because you will need access to either a PC or a secondary phone to contact and notify your bank.

> "*Let's just say you lose your device you somewhere far where you don't even have access to a computer, depending on the level of security you have on your phone as well. I mean, there are chances that whoever takes your phone can access your digital accounts, right, and they can do whatever transactions.*" – Participant 1

> "*I know people who have had their phones stolen from them, and people that stole those phones are able to access everything from their phone like in even banks, that's also a little concern for me, because knowing that someone could be able to just have access to your banks easier without your, yeah, it makes it look like now the bank apps are not as safe."* – Participant 11

Some participants associated losing a device with "losing access to your bank", which can be inconvenient because there are no alternative avenues to access your bank account. With the loss of your device, if criminals can penetrate your phone and get to your banking app, a participant who has previously lost their device highlighted that.

> "*It's not super hard to reset the credentials to my digital bank. I noticed this recently is they need someone who needs some basic information about me, which, considering you know the things that we do from day to day, they are not that hard to find."* – Participant 6

This highlights the significance of a secure device. Another participant highlighted the risks of the actual digital-only bank being attacked through employees or hacker activities, highlighting the significance of educating employees about responsible clicking and emphasising shared responsibility.

> *"Do not trust anyone. Because I think, if anything, the reason why we are susceptible to all these risks is because we trust the banks like we are still trusting someone else so much. Yes, we're supposed to trust them. We put our money in there, and it makes sense, but at the end of the day, there is still a risk that they come with."* – Participant 7

Some participants saw bank employees as the biggest target for cyberattacks because "criminals stand to gain more from attacking the actual bank than a single individual". Consumer-specific risks were raised as the biggest issues that make the platforms risky. It was highlighted that users should treat "sensitive" information as sensitive information. However, current behaviour shows that consumers like "instant gratification", which opens them up to the risks of passing information to scammers. To quote the participant.

> *"I think they use these, these scenarios that they know people will fall easily, like into the trap with, I guess in terms of money, you put a financial factor to it and say you've won a Million rand, click on the link. Even I would click on the link."* – Participant 8

It was mentioned that there is a lack of seriousness when dealing with platforms from the user side, and that is how scammers succeed. The extract below highlights that users are "enablers" when it comes to scammer activities:

> *“I think people don't necessarily think things through. They you get excited. I won a competition, but now they're asking me for my card number and CVV, that doesn't make sense, because if I won the competition, you cannot ask for my account number as well. But certain things cannot be done without my approval.”*– Participant 6

Other user behaviours that bring risk were raised, such as saving passwords and card details online and the complexity of password creation and maintenance. Participant 7 admitted that these practices are convenient for users; however, they compromise security.

> *“People make passwords like some things that they should be sentimental, and I don't think passwords are supposed to be sentimental; they are a security feature.”* – Participant 7

Due to digital-only banks running online and being fully virtual, they also incur a risk of service disruptions. This is not limited to the actual bank, but because banking apps are reliant on telecom networks, any disruption to that infrastructure will cause loss of access to its users.

> *“I was also a customer to a bank that had an issue with accounts were reflecting zero balances*.”- Participant 3

> *“The banks themselves may have stayed up because they've got mechanisms and backups to maintain uptime, but, but you have to access it, mostly through telecoms networks, and those were affected quite massively in some areas, especially for banks that perhaps don't have apps that are zero rated.* – Participant 10

Even with all the risks highlighted, participants highlighted that they have peace of mind due to the level of security provided by the banks and the security features available on the device. Participants highlighted that the availability of multiple layers of authentication or two-factor authentication is an effective measure of security. Other internal bank processes, such as real-time fraud activity

monitoring on the bank side, gave participants additional comfort. Participant 1 provided an example of real-time monitoring by sharing their lived experience.

> "*And I've also seen, I mean, sometime when I tried to get transactions, and then I couldn't do it at that point, and immediately I had a service consultant call me like to say we can see that there's a certain transaction of this amount that's going on in your account. Is it actually you? And this is after doing all the verifications, right. So, once you confirm all of them, they're like, Okay, no, it's fine. Then you can just go back to the application and do the transaction."* – Participant 1

> *"I think there's also two factor authentication. I don't know exactly how it really works in the bank, but I think there's some AI machine that learns how you spend your money and picks up inconsistency and block the account."* - Participant 4

Other features that increased security included one-time pins, dynamic CVV when using virtual cards, quick session expiry, and in-app approvals when transacting.

> *"I even log into my app making any online purchase, regardless of what the value is, there is always that, you know that thing where I get that I have to approve it, because I think it's just that authentication piece that's really key."* – Participant 5

Another view on security was that the highest level of security should be on the actual device.

> *"It should be harder for criminals to get into your device*". – Participant 6

On the actual device security, all participants found biometric authentication to be highly effective and much harder for criminals to bypass. The most popular biometrics are fingerprint and facial recognition. Some participants confirmed that they have never seen anything that tops biometrics due to their uniqueness for

every user. Other participants highlighted that the fingerprint capability gave them a level of confidence when it comes to accessing the device.

> "*We already have biometric authentication, we already have voice identification, we already have all these kind of different things in place that makes it safer*." - Participant 2

> "*I'm always thinking that we are going to reach a point where the apps are going to require for all devices to have, like a minimum-security feature, like maybe fingerprints or eye recognition or something*." - Participant 4

Participants also encouraged the enrolment and enablement of existing device-specific security features that users can enable to add an extra layer of security, such as Find My iPhone for iPhone users or installing software that can block spam calls and suspicious emails/ SMS.

> "*My phone also detects a suspicious email and literally blocks it, so maybe having that type of security on phone making it almost a standard". –* Participants 4

4.5.2 *Theme 2: Digital-only banks adoption factors*

The theme explores various factors that participants highlighted as critical for digital-only banking adoption. These include motivations for adoption, challenges faced, as well as criteria that consumers used to select the digital-only bank.

a. *Adoption challenges*

Regarding the adoption of digital-only banking in South Africa, participants were asked what some of the enablers for the success of digital-only banking, as well as some of the challenges that may derail this form of banking. This was to

explore the overall readiness of this kind of banking. Highlighting infrastructure as the biggest challenge for South Africa as rural areas do not necessarily have internet infrastructure in place; this is also coupled with areas that do not have electricity.

> *"I think it will take us time, I don't think we have the infrastructure now for the whole country to benefit with digital only banks, I think, it will take us time yeah, for us to benefit from that, and to just have the infrastructure, and then for everything, for everyone to be able to use them".* – Participant 9

Some participants, as existing consumers of Digital-only banking, highlighted some of their personal experiences with internet connection in remote and rural areas. They are based in Gauteng and can transact without any challenges; however, when they are outside of outside the city, they express challenges due to poor internet connection. Their sentiment is that for people based in those areas, this form of banking may not yet be feasible. In terms of infrastructure, raised similar sentiments

> "I *think the metropolitan areas 100% I think it's both metropolitan setting urban areas, I think the infrastructure is there, but the maturity, in the in the in the outline areas, I think it's, it's a bit like spread, and to a large extent, not, not quite optimized. So, I think those areas will probably struggle*." - Participant 10

Some participants mentioned the challenges around access to smartphones and good connectivity. The cost in South Africa is still high for most people. With the high rate of unemployment, the cost factor is a challenge.

> "*Our rural communities, network is always an issue. They don't always have good network. They don't have the right devices. So, they will, until South Africa changes, and we don't have, you know, like people in areas where you can't provide them connectivity and where their smartphones are not affordable, Digital-only banks will be a challenge."* - Participant 5

Some participants raise affordability issues when it comes to the internet and smartphones furthers Participant 4 raises affordability issues regarding the internet and smartphones, further highlighting the accessibility challenges for disadvantaged communities. Some participants highlighted that due to this banking happening on digital channels, it requires some level of technological savvy to ensure responsible and seamless engagement. Lack of the tech-savviness may lead to resistance to adoption.

> "*If you are a client that's using a digital bank, to a certain extent, one would expect you to be, you know, somewhat technical, technically savvy as well*." – Participant 2

> *"I don't think I'm going to be a fan, because sometimes some people are not ready, they don't have experience with digital apps and smartphones, they need to talk to someone to be able to understand some of the policies or things about their banking. So, I just people that don't have that much knowledge about their apps and machines and AI. So, I'm not really a fan of being having digital only banks*." - Participant 11

While some participants highlighted that digital-only banks would be highly beneficial for everyone, there was an agreement on the required tech savviness. However, the level required is not as high according to participants, as per insert

> *"So, it's more on how technically savvy you are. It doesn't require a lot of technical savviness, but at the same time, it does require some form of technical savvy."* - Participant 6

Another challenge raised was change management for older generations. According to some participants, older generations are perceived as "people of habit" and have lower tolerance for changing their ways, including switching from branch banking to fully digital banking. Some participants attributed this older generation challenge to them not being tech savvy enough.

"*I think especially for the elderly, elderly, and certain age ranges. They so used to go to the traditional bank to sort out their finances, going to a branch, sitting down with a private banker. So, some people would ideally prefer to still have that".* -Participant 2

"It cannot become like 100% because, you know, there is the older generation that also prefers to go into the branches when handling their banking matters, but not quite tech savvy." – Participant 8

Other participants raised concerns about cyber security challenges, more specifically phishing scams. It was highlighted that less tech-savvy people and older generations who are not high internet consumers are likely to fall victims. This was expressed in the following insertion.

"*But I think for someone who's more vulnerable, who's not aware, for example, my mother does bank, she's a bit cautious as possible, but I think she's more likely to fall victim than myself because of my, Im more aware of the usage of technology and internet abilities"*. – Participant 3

"It's very convenient, but I'm also conscious of the safety side of it and how it could also be unsafe, because I could get a link and would be disguised as a link for my bank, only to find out if it was someone that is not for my bank, and I click the link and they have access to like my account, but it's very convenient for me." – Participant 11

b. ***Adoption drivers***

While there are adoption challenges to digital-only banking, participants also raised several benefits to this form of banking. Most participants raised benefits such as banking anywhere, anytime as a game changer. Some participants described banking apps as seamless and efficient. Almost all participants agreed that digital banking apps have brought much convenience into their daily lives. Participant 10 described the platforms:

"*Very smooth, hustle free, yeah, I do enjoy it. I think I was probably one of the first cohort of people to jump up to Discovery bank before the launch, I think they did a pilot with the select number to people. So, this is that I think it's, yeah, it's very smooth, very, very smooth, hassle free, I barely need to call with the bank."* – Participant 10

"My experience has been amazing, because I prefer to not leave the comfort of my house, so the fact that I can bank at the palm of my hands, I find that I'm happy with the convenience." – Participant 3

"It is much more efficient than going to the branch for sure. And I guess the whole self-service element is probably like the best thing, the fact that I don't have to wait in a queue, and I can service and do things myself." – Participant 5

Participants were clear on the critical requirement of efficient online customer service. As a digital-only customer, a participant mentioned that having the challenges of digital-only banks resolved digitally is part of the convenience of this form of banking. They also mentioned that face-to-face human interaction is important in banking, especially when someone has a problem to address. However, participants mentioned that they would be willing to adopt digital-only banking if there was a "*trustworthy online customer service to replace the human interaction."* Participants agreed that reliable customer service is important and in their experience as a digital-only customer:

"*If you have like the number to call, it's easy, because you can just call them and say, listen, I have this issue of this issue and this issue. I've never had an issue to where I felt, you know, I cannot resolve this issue on the phone." – Participant 6*

"For digital banks, all their issues and problems are solved digitally. So, if I have a problem, I can still say, I can stay at home and they will make sure to solve it digitally, I'm not going to be requested to come to the office or to the branch or something. There's that convenient." – Participant 7

According to most participants, digital banking platforms have advanced technology and features that users would not ordinarily have without the apps. Some participants highlighted the innovation and evolution of these banking apps.

> "*Technology has evolved quite a bit since implementation of banking apps, right? So, I mean, back then, if I think about it, the functionality was quite limited, right? So there when quite a lot of things where you could verify yourself, and I don't even think security was that great as well, but I mean, it has evolved quite a bit."* – Participant 1

The advancement in the South African banking landscape also involves a shift into a mostly cashless society, which is raised as another driver for the adoption of digital banking. Some participants highlighted the issues around crime. The crime rates in South Africa also force people to use digital money, which drives adoption. This was also confirmed by a participant who is a digital-only customer.

> "*I hardly even withdraw money to make purchases, or physical cash, like an ATM to withdraw, withdraw physical cash from an ATM to make purchases. I can't even remember when last I withdrew money to make a purchase."* – Participant 2

c. ***Bank selection criteria***

To further understand some of the adoption drivers, participants who have a digital-only bank account highlighted some of the criteria that they applied to select their digital-only banks, and those who did not have digital-only bank accounts were asked what benefits would convince them to adopt. Participant 10 highlighted that the ease of opening the account, the user experience of the apps, as well as functionality were the biggest driver for adoption. While participants 1, 2 and 7 highlighted the importance of brand strength and reputation and safety of platform when selecting a digital-only banks. Participant 2 highlighted that:

"Discovery has a brand of trust. Discovery as the brand of delivering. So you go with the brand that you've trusted. You won't go for a brand that you're not familiar with, but you go with the brand that you've trusted, right? And that's why it just made sense for me to stay within that same ecosystem as well." – Participant 2.

Rewards and benefits offered by the banks also became an important driver for adoption for some participants, along with integration with other products by the financial provider. According to participant 10:

"So those were the top two items that I was looking for. And then the third was pretty much in terms of complementors based on other financial services products that I had and how they integrated into my bank. It just made it just made it easier. And obviously, then, you know, items such as the benefits that come with the rewards portion of what that bank offers as well." – Participant 10

For participants who did not have a digital-only bank account, the cost factor was mentioned as a driver. They mentioned that due to digital-only banks not having physical presence /branches, the running costs are kept low, and that should be factored into the pricing of their products. The second driver mentioned was the actual costs of credit. Another participant alluded to not being concerned about a bank being a digital-only bank or not, but if their price were competitive, they would be willing to adopt:

"So, you know, like, I have a home loan, I have a car loan, and the better the interest rates, you know, I don't mind moving. I mean, I was previously with the bank, I moved because the bank I was moving to give me a much, much better interest rate." – Participant 5

"But if maybe the way to give me, because I think the charges for the banking that actually has run both, physical and digital platforms for banking, the charges are now kind of the same, whether you no option like

they are maybe it should be cheaper if you opt to online banking only. So maybe there were, if there was a financial benefit". – Participant 3

4.5.3 *Theme 3: Measures to Enhance security and reduce risks*

This theme explores strategies and recommendations to strengthen the security of digital only banking. It highlights consumer-facing measures, digital-only banks-specific measures, as well as the role of educations and digital awareness.

a. *User based enhancements*

Participants noted that most security breaches or risks manifest due to users not taking the necessary precautions and doing their due diligence before clicking. It was mentioned that even with access to certain device functionality, users still do not enable those features to safeguard themselves. Most participants agree that banks are doing enough to make sure that there is education available, however, consumers have the responsibility to understand the education further and apply it to their everyday engagements.

"*I think, educating yourself on what you need to do right to keep your information safe as well. Because, I mean, banks and technology can only do so much right at the end of the day, it's on you as an individual to keep your information secure as well, so the level of security that you also implement on your devices."* – Participant 1

"*I think I get emails from my bank around once a month, sometimes once every two months, and then, like we'll never ask you for your password via email. And if there's updated scams, and then there will list like examples and what to do if, in that situation, if you are a victim of a scam or cyber-attack."* – Participant 8

"I mean, awareness doesn't always have to come from the bank itself. People must read up on their own as well because it is your investments that you're protecting at the end of the day. So, I think people could also

read more, and then also just ensuring that the devices are secured as much as possible." – Participant 10

Some participants discussed how a basic password maintenance strategy could reduce risks. They highlighted that users need to normalise changing their passwords regularly. They further recommended that users apply different passcodes to access the device and the banking application. This will ensure that your banking app is still secured even if your phone passcode is compromised.

It's about making sure that your passwords, they're protected, and they like you protect yourself by having two different sets of authentications for I get if I can break into the phone, it doesn't necessarily mean I'll break into your banking app." – Participant 9

Other participants further supported this, and it was also suggested that passwords should not be basic because that would make the application "hackable." Participants also touched on users performing reasonable due diligence to validate suspicious activities. These range from banks contacting you and asking for information to competition messages from scammers. Banks do communicate what they will never ask from you, and it is suggested that users pay attention to the communications from the bank. Below is an extract from some of the participants on reasonable due diligence.

"I've seen things like, you get a SMS that you won something that you didn't even enter competition for. I mean, the first thing that should come to your head is, how, how did I win something if I didn't enter anything like people shouldn't be that gullible, right? I mean anything that you get. So again, you as an individual, it's your responsibility to make sure that you don't fall for most of these things, because that's how your information gets accessed at the end of the day." – Participant 1

"*You see, too often that people are just clicking on every single thing that they like, clicking on, on links that you know they would never recognize but why not let me just click on it to see what it is, and you know it's actually*

understanding their responsibility when it comes to their information security." – Participant 5

"*There are ways to verify if things are true or not. Find the contact number online and confirm with the organization, saying, listen, did you guys send me this type of communication, because it's requiring some sensitive information from me, and I do not feel safe handing out that information without actually being sure that that is indeed you guys who are contacting me, most people will also most organizations will also say we will never contact you and ask for this, this and that."* – Participant 6

There were suggestions around consumers' understanding the impact of other specific practices that users take for granted but can be harmful. Some of these include connecting to public Wi-Fi.

"*So I think those are some of the things that that people can, can do as well, you know, perhaps, yeah, and maybe also just assessing and understanding the risk that comes with certain Wi Fi connectivity, you know, especially public WIFI's in certain areas, even when you travel on holiday, those type of things, where we all look for a house with free Wi Fi. But how free is free really? It could cost you."* – Participant 10

Not opting to enable other device-specific security features, such as remote wiping, is supported by the following quote.

"*But also, you know, things like, remote wiping, people don't realize how important it is, so nobody does it. Like you trying to set up your device google tells you, like, set this up, and you just like, oh, I will do it later. But you don't realize how important it is to have a remote wipe set up on your device.*" – Participant 5

Measures include installing software that can detect and block spam calls, emails, and SMS, installing anti-virus on your device, and hiding your banking application from the home screen on your device.

b. *Digital bank enhancements*

Current security levels have been described as sufficiently secured for digital-only banking; this was the sentiment of most participants. Even with this, participants were clear that there are always new threats coming up, and banks needed to stay ahead of the game by looking for more opportunities to secure platforms. When asked about the safety of platforms, a participant shared the following views.

> *"I think they try but unfortunately, the criminals are working just as hard as the banks, they are also very much aware whenever there's an upgrade of sorts, because these people are also intelligent people that you know. So, they try and keep up with security as well, but they do try. I mean, when we started with Internet Banking, you used to maybe just a PIN code, but now they've added, as I said, like the two, two security system stuff, where they not just want you to put in your password, for example, they also want you to verify on their banking app as well, which is the second layer of security*." – Participant 3

It was acknowledged that the bank is taking a lot of initiative to mitigate some of the risks; however, there is a gap in communication about what the bank is doing to mitigate risks. Some participants shared that as consumers with advanced technical understanding, the investments in platform security are evident; however, to a regular consumer, it looks simple.

> *"Security is a priority. So obviously on user end it looks simply, but in the background, there's a lot happening to have everybody secure.."* – Participant 4

The same observation was shared by another participant, who is an IT professional:

> "*Banks also don't share enough to customers, about what they're doing to protect customers from security, and I think that's what the biggest thing*

is, is, you know, like when you, when you come from an IT space, it's easy for you to understand the controls. Tell customers what you're doing. Explain to them why it's secure to use your platform. And yes, there'll be risks, and there'll always be risks, but tell them what you're doing to mitigate the risks." – Participant 5

A further improvement to security, other participants recommended that banks need to be more transparent on communication channels to their clients, as well as the questions they will ask you to authenticate so that scams can be easily detectable for users. Participants agree that there's enough warning about what banks will not ask you. However, it is not always obvious what they will ask you, and this should be obvious, at least between the consumer and the bank.

Some participants recommended leveraging AI technology to enhance security. The first recommendation is that digital-only banks can monitor and learn users' banking behaviour, such as times when a customer banks, and amounts on a transaction level, and from this regular behaviour, AI would be able to pick up suspicious behaviour and trigger additional verification processes, such as contacting a client or triggering additional authentication such has three-factor authentication.

"*I don't know if there can be a way to be able to, I don't know to be able to say in the system. I only bank at whatever, whatever times so that if they see me banking outside of time, maybe they will know that something is wrong."* - Participant 3

"*Maybe then you can make a three-factor authentication, I have only heard two factor authentication, I don't know about three, so they can initiate a third one if there's suspicious activity."* – Participant 4

Ensuring that the correct person is accessing the banking application is also the biggest challenge since everything happens online. These sentiments were shared by most of the participants, and multiple additional verification steps have been recommended. Other participants recommended a real-time, live

verification process using pictures. They also recommended the introduction of security questions for account recovery, as they deem this to be easier but more secure, as well as an introduction on enabling location before transacting to detect and mitigate scams where users are transacting in various locations at the same time.

> "*So, if you can invest in security questions, or verify by sending a picture. Say, okay, send us a picture so that we know it's you, right, right? That would help. That's a better measure, rather than what I know, especially with my bank. And I think their recovery account recovery, for me is not satisfactory. I think they can do much better there. That's simplistic."* – Participant 6

> *"I think this selfie thing is good because, yeah, like, if it's not me, and then you're trying to process a payment with my banking app, and then hopefully it will pick up that this is the wrong person. I'm just hoping, like, that is the end goal, like, if it's not me, then it won't match with my picture and stuff, and then the payment won't go through."* – Participant 9

Digital-only banks are also encouraged to prioritise following best practice frameworks when it comes to security. These frameworks include ISO security standards, IT policies, POPI, and all other processes and procedures, such as well-trained employees and regulatory requirements. Participants acknowledge that some of these are not "must" haves; however, they are useful when it comes to protecting information and security.

> *"I guess it's always making sure that their security, their IT security is always, you know, like, kept up to date, and you know, they are following best practice and things like that, because, you know, like, they're holding all our data, and if that data gets into the wrong hands, we kind of screwed, in a nutshell*." – Participant 5

> "*Those are things that, yes, all they are, are guidelines but you know, you follow those guidelines, and it does help you from like a security*

perspective. So, I think it's using guidelines, practices, certifications that are out there to strengthen the security in the banks." – Participant 2

c. ***Education and awareness***

All participants share a sentiment about the challenges posed by consumers and their lack of awareness regarding digital engagements. On this subject, most participants agree that there is sufficient education and information available; however, it is not reaching consumers in the best possible way, bringing into question the effectiveness of channels being used by banks to communicate.

"I think finding the best way to get the information to the people but also making the I don't know how people will do that, like getting the people to believe the information, because I think the biggest thing is that they don't believe it so that's why I mentioned that, yes, I'm watching something. Someone is hacking. It's fun to me. It's a movie. It's entertaining. But it actually happens. – Participant 7

A different view raises gaps around the use of language and makes sure that banks stay clear of technical language when delivering the education. This are expressed in the following comments:

"Tell me why I should use your internet banking, but in English, you know, like it, you know, don't tell me, like, don't click on this link because it's going to give you malware." - Participant 5

"*Speak their language. I think that's what I've realized. I don't think most things that are communicated to the people speaks the people's language. Yes, in terms of like, marketing, and stuff, you see those people speak the people's language. That's why they can get to the people. But I don't think we have the same exercise in terms of, like, security practices and whatnot."* – Participant 7

It is recommended that these digital-only banks find a way to simplify their communication language for effectiveness. As an extension to effective communication, it is recommended that banks use targeted communications that are personalised while also considering channels that are effective for the different target groups. It was raised that the older generation is more likely to read SMS's, however, it will be different for the younger generation, which highlights the need for targeted communication.

> "*One thing I know is that people don't read. So, sending, sending SMSs, and sending email, like people don't read, probably get awareness to be done more on segments, you know, like a youngster will read WhatsApp messages, while people in their 60ties will read SMSs. I guess its tailoring communication based on personas.*"- Participant 5

Social media was highly recommended as an effective channel by most of the participants, especially for the younger generation. Another participant also raised the advantage of channels that offer a more personalised experience such as WhatsApp. They expressed their view as follows:

> "*Definitely social media, the biggest obviously being WhatsApp. I think it's, it's, I don't know what the stats say, but almost, I'm pretty sure nine out of 10 people are on WhatsApp. So, I think WhatsApp is one tool that they can utilize, because usually banking accounts are linked to either your email address or your phone number. Usually there is a phone number. So, it's, I think it's, it's an easy you know item to utilize that you know to capture, you know, the audience of your market. So, WhatsApp is, number one. And then on WhatsApp, it can be personalised as well, which, which helps, because people now tend to more generalised communication."*- Participant 10

Other participants also echoed the same sentiments about the effectiveness of social media as a learning and awareness tool.

> "*Social media, once again, a beautiful thing. There is a channel on YouTube. The name has slipped my mind now, but it's a man who engages with all these scammers all over the world about different things and different types of scams, and he releases these documentaries like just to bring about awareness about these things with live action events, just to show everyone who's watching what can happen and how big it can happen."* – Participant 8

Other participants were also in support on social media as an effective channel for educating and creating awareness. They were in favour of distributing visual representation of the educational material.

> *" So imagine, you know you are on TikTok and find this interesting video about cyber security, and from that time, you will barely forget you know about it, because it's something which was a visual, something that is you've seen, so it will always ring a bell in your mind, like, you know, actually, I need to do this."* – Participant 9

It was also highlighted that sometimes users learn when there is an instant and direct benefit. It was suggested that banks can find a way to deliver education, track some set of activities to see if consumers are improving on their behaviours, and, for those who are showing improved behaviour, issue them with an incentive to drive engagement.

> *"They must use some incentive like, let the public do those videos, or do those exercises, and then give them a reward. Maybe that will increase their awareness of cyber security."* – Participant 4

4.5.4 *Theme 4: Strategic Role and Opportunities of Digital-Only Banking*

This theme explores the significance of digital-only banking, highlighting their contribution and them being the future of banking. The category further brings in

some opportunities that the banks can investigate strategically to further cement their place.

a. *Target market*

Participants were asked to share their opinions on who they believe is the target market for digital-only banking. The majority of the participants highlighted that this form of banking is mostly suitable and targeted at the younger generation. Some of the reasoning was that this requires users to be technically savvy, which might not be true for most elderly people.

> "*I guess it might not be suitable for the older generation who are not that familiar with technology, but definitely for the younger generation.*" – Participants 6

> "*Definitely your millennials and Gen Z. Because I guess, like the older you get, you also need a smartphone. And not all the older generations want to use a smartphone.*" – Participant 5

> "*Definitely young people. In terms of age, I think between the age of 18 and 55. Because I feel like, you know 55 they're not really that old. So yeah, they can still learn about digital banking. And then once they start knowing about it, and then they will realize how it makes their life easier.* – Participant 9

A different view highlighted that the banks most likely started with a specific target market; however, that has evolved over time due to advancements in technology adoption.

> "*I think probably they've started with the target market, but the nature of the evolution of digital banking now is just opening it to everyone. I think that's the direction that they'll just call it strategically, where it's no longer a fit purpose for, let's say maybe they were targeting the middle class, or the upper middle class, at the beginning, people who had access to*

communication resources. But I think with the democratization of comms and infrastructure and devices, I think it's now opening it pretty much to everyone, and I think that's the strategy that would probably go with." – Participant 10

b. ***Opportunities for digital-only banks***

Participants reiterated that for Digital-only banking to penetrate as much as traditional banks, they needed to recognise the importance of taking the initiative to educate users and potential users about this form of banking. The education should cover a range of things, including the benefits of this form of banking, the convenience factor, perceptions around digital banking, and the safety of platforms.

"*There's a lot of education that still needs to be done, right? And I mean more than anything, if you want, you know your digital banking to be as big as traditional banks are, and for security to be enhanced, there's a lot of education that need to be done there*." – Participant 1

"*Banks don't do things to change people's perception about online banking, or even digital-only bank, you know things that it's never going to work. I mean, the fact that people who don't know half the features that exist in the bank app and how secure those features are, like, it's crazy*." – Participant 5

"*Just spend the time to actually educate customers and change perception if you tell somebody you can do this online, instead of standing in the queue for two hours, it's safer because I am in control of it with, you know*." – Participant 2

"*Make people aware. The education, because, as much as, for example, people are using a digital bank, but they may not even be acknowledging that they're using a digital only bank. So, we also must acknowledge that*

we are migrating from traditional banking to digital banking. So, affording people information and making people learn is critical." – Participant 7

Some of the participants that currently do not have digital-only banks highlighted that they would be willing to take up an account with one of the banks if the banks offered competitive pricing. It was further highlighted that due to digital-only banks being fully virtual, that is a saving on the physical infrastructure that traditional banking has. Therefore, this should be reflective in the pricing. Other participants mentioned that their deciding factor is purely on cost, it is not a material factor whether a bank is digital-only or traditional with digital presence.

"I like the idea of digital only if, if the I can benefit from their rates. I mean, for example, if a bank must run a physical facility, there's a cost impact of it. So, if the if the digital banks can maybe filter the benefit of not having the expense of running a facility to the customers, I would, lean towards that if I can, yeah, if I can experience the discounted rate of not having to run a physical facility."– Participant 3

"I have a home loan, I have a car loan, and the better the interest rates, you know, I don't mind moving. I mean, I was previously with the bank, I moved because the bank I was moving to gave me a much, much better interest rate. So, I guess things that can help me save money, like interest rates, is something that would appeal me to move." – Participant 5

Digital-only banks can also look at options to increase trust by publishing and benchmarking security using defined metrics. It was suggested that the metrics include variables such as how well they are tracking, incidents encountered, impact, threats successfully mitigated, etc. While participants agree that this might also cause challenges for the banks by creating fears for users, it was highlighted that it will also attract and retain loyal customers, which is beneficial in the long term.

"Having this information as public information and consumable by users perhaps could help digital banks just get that level of confidence, you

know, with regards to users, because anybody can sell your dream to say we are the most secure but based on what. So, in terms of positioning, I think that is one thing that they could utilize for transparency. If you do that, then your users become loyal users, because them knowing that, then they're loyal, you know, because we talk about customer centricity at the end of the day." Participant 10

c. ***Significance of Digital-only banks***

All participants described Digital-only banks as "banks of the future." This is driven by the fact that the world is naturally becoming technologically advanced. It was also mentioned that the rate of innovation is a big driver for this. Participants highlighted that whether we are ready for it, this is where the world is going. Some participants highlighted that this will soon be the dominant way of banking.

"*I think that's really, I think that's, that's where the future is going to be honest, in terms of that digital bank*."- Participant 2

"*So, there will be a time where we at least have enough technological knowledge to do the basics, and actually, you know, only have digital only banks*." - Participant 6

"*I think that's where we're going. And I think that's probably like the goal for most innovators, like people who are creating, they're creating in that direction to say, okay, we're moving into this age where things might be this way. So, I think that's where we're going. It might even be sooner than we think.*" – Participant 7

This was further substantiated by comments that traditional banks have also downsized their physical presence and generally drive users to their banking apps and use their branches as a last resort.

“you'll notice that even with the traditional commercial banks, a lot of them, a lot of them have moved to close a lot of their branches, right? for economic and operational purposes. But what that is also doing is pushing people more into the digital bank side, because then they they're not inconvenienced at all.” – Participant 10

“*I feel like at some point, because even the banks that have branches, my experience when I go to FNB or ABSA they always ask where your app is, things are always getting approved in the app, they are moving towards that direction.*”- Participant 4

The introduction of digital-only banks is perceived as a growth move for South Africa, as it gives SA global relevance in technology.

“*I think they (digital-only bank) are important, I think we are growing as the world at large.*”- Participant 7

“*And the yes part is, obviously, it's keeping up with technology. It's keeping up with the trends. That's the part where I say it's relevant to have a digital bank.”* – Participant 4

“*I think the world is growing, and the world is adapting and it's advancing, right? Even the people in disadvantaged communities, there are outreaches that go into those communities to sort of try and give them a better exposure.”* – Participant 6

This relevance is significant because it improves the country’s profile, which can attract investors.

“*They add value to the country's brand as well. I think if we need to look at it from the point of view, from a from an investor perspective as well, those investing in the country as we have, right, they see, okay, this is a country that actually keeping up with the times from the technology perspective,*

they are growing, there's potentially this country to invest in this potential for the country to grow something that." – Participant 2

It was highlighted that South Africa has an advanced banking system compared to other countries, and the introduction of digital-only banks is further advancing the banking landscape. Due to digital-only banks running on technology platforms, participants highlighted that this creates opportunities for IT roles that did not previously exist before. It was highlighted that young people gravitate towards technology roles, which creates opportunities for more options.

"Particularly people around my age, you would find that the conversations that most people have, especially if we're going to talk about growing up and becoming a professional and what type of employment or what other skills you want to you know, what's the what's I'm trying to find the word like whatever skill, skills you want to have for yourself people are normally like more gravitating towards the IT side of things." – Participant 7.

4.6 Linking themes to Objectives

4.6.1 *RO1: To explore what digital natives consider risks and security level in South Africa's digital-only banking.*

Most participants believed that while threats are a concern for digital-only banking, this risk was not limited to digital-only banks. Therefore, it was not perceived as digital-only bank specific, but rather a general risk in banking. Participants highlighted that while there's an increase in cybercrimes such as phishing attacks, there were measures that banks have put in place to protect consumers from such. However, there was a shared responsibility between banks and users to protect the banks, some of the measures that increased trust and mitigated these risks include biometric authentication, real-time fraud detection and monitoring, in app approvals and two-factor authentication. Participants agreed that no attack can happen without user participation. The

primary threat highlighted relates to users and their engagement behaviour. Social engineering and phishing came up as a prominent risk and persistent risk.

4.6.2 *RO2: To explore how the perceived risk and security influence Digital natives' intention to adopt Digital-only banking.*

The majority of the participants think that digital-only banking platforms are sufficiently secure. The participant, who was not in agreement, believed the lack of education about responsible engagement made the platform not sufficiently secure. Seven out of the eleven respondent participants are digital-only banking users; they confirmed that their criteria for taking up banking were due to factors such as brand reputation and trust, convenience, app user experience, rewards and benefits, integration of products, as well as platform safety. Three out of the four participants who were not digital-only bank users would be willing to take up digital-only banking on condition that there could be a specific benefit, such as reduced costs and favourable interest rates. Regarding risk and security, users highlighted that there are enough measures in place, and digital-only banks continuously improve their security. While risk and security levels are big drivers for adoption, participants highlighted that digital-only banks have the same level of online risk as any other digital platform, and it is mostly about responsible digital engagement. They also highlighted that even traditional banks have adopted a digital-only approach due to advancements in banking, and the subject of risk users felt that they were accepting the same level of risk when it comes to digital platforms between digital-only banks and traditional banks. Participants also raised that they believed digital-only banks are safer because they do not have the physical infrastructure that would create another opportunity for attacks. Participants went on to highlight some of the opportunities for digital-only banks, such as educating users about digital-only banking, their ESG contribution the benefits of using digital-only banking, their ESG contribution, etc., to investigate to advance their penetration in the market. Most participants are in favour of this banking and agreed that this form of banking is important for South Africa as a

global brand. It also created new employment opportunities in the IT sector, which aligns with roles that young people are not interested in.

4.6.3 *RO3: To understand from digital natives what measures digital-only banks in South Africa can prioritise to reduce risks and improve security*

Most participants agreed that while security is currently sufficient, there is a need for continuous improvements since cyber attackers are getting more creative in their attacks. It was mentioned that digital-only banks needed to "stay ahead of the game" when it comes to security measures. Participants provided recommendations of measures that can be introduced, such as additional biometrics, leveraging AI, introducing security questions etc. Participants also highlighted some recommendations that users can implement to increase security, such as enabling device-specific security features, installing software that can detect suspicious activities, performing reasonable due diligence, etc. All participants believed there is a gap regarding digital platform safe engagement when it comes to the users. It was mentioned that even though banks were pushing out enough information about responsible engagement, they needed to leverage channels that users are engaging in, such as social media, they needed to speak the language of users and move away from technical jargon, as well as personalise the education to ensure that there is targeted communication for effectiveness. There was also agreement that users needed to take the initiative to apply what they learned and further expand their education on online safety. Participants highlighted the significance of continuous enhancements for the bank's reputation and building of trust.

4.7 Linking themes to the research objectives and theoretical framework

This study was shaped by three core research objectives that collectively aimed to explore how digital natives in South Africa perceive the risks and security aspects of digital-only banking. The analysis was guided by two established theoretical frameworks—Perceived Risk Theory (PRT) and the Technology Acceptance Model (TAM)—which provided a strong foundation for both data collection and the interpretation of findings.

The first objective focused on understanding how digital natives view the risks and levels of security in digital-only banking. This was explored using Perceived Risk Theory, which highlights how individuals' perceptions of risk can influence their decisions and behaviour. The theme that emerged from this objective, "Security and Risk Levels of Digital-Only Banks", highlights a range of concerns raised by participants, from technical vulnerabilities in the banking platforms to their personal views on how safe they feel using these services. The second objective examined how these perceived risks and concerns about security affect digital natives' willingness to adopt digital-only banking. This was analysed through the lens of the Technology Acceptance Model, which suggests that if people find a new technology useful and easy to use, they are more likely to adopt it. Two key themes emerged. The first; "Digital-Only Bank Adoption Factors", covers what encourages or discourages digital natives from taking on digital-only banks. The second theme that emerged, "Strategic Role and Opportunities of Digital-Only Banking", looks more broadly at the potential and future relevance of these banks in the South African financial sector.

The third objective aimed to identify what measures digital-only banks can take to reduce risks and improve their security. This objective was informed by both

PRT and TAM, reflecting the importance of addressing both how digital natives feel about risk and what practical steps can be taken to support technology use. The resulting theme, “Measures to Enhance Security and Reduce Risks”, includes suggestions from participants on what users can do to protect themselves, what banks should be doing to secure their platforms, and the importance of raising awareness and digital literacy among consumers.

The identified themes provide a well-rounded understanding of the digital-only banking space in South Africa, from the perspective of tech-savvy young users. They also show how perceptions of risk and security affect whether or not people choose to adopt these banks, and highlight the strategic steps banks can take to ensure sustainability and growth, while keeping customers safe. Table 2 below presents a summary of how the research objectives, theories, themes and sub-themes link together. These are further discussed in detail in chapter 5.

Table 2 – Summary of Research objectives, theoretical framework, and themes

Research Objective	Theoretical Framework	Emergent Theme	Sub-Themes
RO1: To explore what digital natives consider risks and security levels in South Africa's digital-only banking.	Perceived Risk Theory (PRT)	Theme 1: Security and Risk Levels of Digital-Only Banks	- Institution and platform security measures - Device security measures and vulnerabilities - Digital-only bank sentiments - Online threats - Service availability threats
RO2: To explore how perceived risk and security influence digital natives’ intention to adopt digital-only banking.	Technology Acceptance Model (TAM)	Theme 2: Digital-Only Banks Adoption Factors	- Adoption challenges - Adoption drivers - Bank selection criteria

		Theme 4: Strategic Role and Opportunities of Digital-Only Banking	- Target market - Significance of digital-only banking - Opportunities for digital-only banks
RO3: To understand what measures digital-only banks in South Africa can prioritise to reduce risks and improve security.	Perceived Risk Theory (PRT) and Technology Acceptance Model (TAM)	Theme 3: Measures to Enhance Security and Reduce Risks	- User-based enhancements - Digital banks enhancements - Education and awareness

4.8 Summary of the findings

This chapter presents the findings from interviews conducted as part of the research. Using a thematic analysis approach, four key themes emerged from the data. The themes have been discussed in detail, and below are some of the key points that emerged from the data.

Participants emphasised that security and risk management are high priorities for digital-only banking. They found the platforms to be secure, with robust security features. Notably, participants did not perceive digital-only banking as riskier than traditional banking. Participants identified several factors that drive the adoption of digital-only banking, including platform safety and security features, benefits offered (e.g., rewards, lower fees), convenience and ease of use and positive user experience. However, participants also highlighted barriers to adoption, such as cybersecurity risks (e.g., phishing, and social engineering attacks), poor internet infrastructure, high internet costs, and limited tech-savviness among certain demographics.

While participants acknowledged that digital-only banks proactively mitigate risks and educate users, they emphasised the shared responsibility between banks and users in maintaining security. Users were encouraged to engage responsibly online, enable device security features, and self-educate on cybersecurity risks and safe practices. Participants also noted that while banks communicate security advice via SMS and email, expanding education through platforms like social media and using simple and personalised messaging could improve awareness and engagement. Participants highlighted the broader significance of digital-only banking for South Africa, including advancing technology adoption and digital innovation, creating opportunities for skill development, particularly in IT and enhancing South Africa’s global competitiveness in digital banking.

However, participants noted challenges reaching rural areas and regions with poor internet infrastructure, suggesting that digital-only banking is more suitable for urban, tech-savvy populations. Participants identified opportunities for digital-only banks to expand their market share by increasing education and awareness initiatives tailored to diverse user groups, simplifying messaging to ensure accessibility for less tech-savvy individuals and addressing infrastructure challenges to broaden accessibility in rural areas.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter presents and discusses the results of the research findings outlined in Chapter 4, linking them to the research objectives and existing literature. The research objectives are as follows:

1. To explore what digital natives consider risks and security levels in South Africa's digital-only banking.
2. To explore how the perceived risk and security influence digital natives' intention to adopt digital-only banking.
3. To understand from digital natives what measures digital-only banks in South Africa can prioritize to reduce risks and improve security.

The discussion delves into the main findings, examining their implications in light of the research objectives and situating them within the broader context of existing literature. These findings draw conclusions, providing a comprehensive understanding of the themes emerging from the data.

5.2 Discussion pertaining to Objective 1: Perceived Risk and Security levels in digital-only Banking

While digital banking security has advanced significantly, risks remain a persistent concern for digital-only banking users. Participants in this study highlighted that their perceptions of risk were shaped by their lived experiences with online banking, past exposure to cyber threats, and their broader trust in digital financial services. The absence of physical branches was frequently

mentioned as a factor that heightened perceptions of vulnerability, as participants expressed concerns about limited recourse in cases of security breaches or service disruptions.

Interestingly, participants did not perceive digital-only banks as significantly riskier than traditional banks offering digital services. Instead, they acknowledged that security risks were inherent to all forms of online banking, with mobile banking applications emerging as a focal point of concern. Given the entirely virtual nature of digital-only banking, the security of personal devices was considered paramount. Participants recognised that even robust banking security measures could be undermined if a mobile device were compromised.

Biometric Technology: Enhancing Perceived Security

Participants strongly supported biometric authentication as a security measure that enhances trust in digital-only banking. Fingerprint scanning and facial recognition were viewed as effective safeguards due to their uniqueness and difficulty in replicating. These technologies were particularly valued for their ease of use and perceived reliability in preventing unauthorised access.

These findings align with existing literature. Morake et al. (2021) emphasise the need for authentication mechanisms that are both secure and user-friendly, identifying biometrics as an effective solution. Similarly, Patra et al. (2022) and Piotrowska (2024) highlight the role of biometrics in reducing fraud risks while improving digital banking functionality. However, there are concerns about the permanence of biometric data—unlike passwords, biometric identifiers cannot be changed once compromised. This aligns with Piotrowska's (2024) argument that financial institutions must prioritise the ethical management and protection of biometric information.

Multi-factor authentication and Layered Security

Multi-factor authentication (MFA) emerged as another critical security measure influencing participants' perceptions of risk. Participants noted that requiring

multiple authentication steps, such as one-time PINs (OTPs) and in-app approvals, instilled greater control over account access. While some found MFA slightly inconvenient, they acknowledged its necessity in mitigating unauthorised access risks.

The literature corroborates these findings. Putra et al. (2023) advocate for the use of layered security mechanisms to foster trust in digital financial services. Similarly, Faisal et al. (2024) highlight MFA's role in enhancing user confidence by ensuring access requires multiple verification steps. The study suggests that digital-only banks should continue refining MFA strategies to balance security with user convenience.

Fraud Detection and the Role of AI

Participants appreciated the increasing use of artificial intelligence (AI) in fraud detection, particularly in identifying suspicious transactions in real-time. They viewed AI-driven security measures as reassuring, particularly when combined with immediate alerts and the ability to block fraudulent transactions. However, some participants expressed concerns about the reliability of AI in distinguishing between fraudulent and legitimate transactions, occasionally leading to unnecessary transaction blocks.

Research supports these insights. Patra et al. (2022) highlight the role of AI in enhancing fraud detection accuracy, while Singh et al. (2024) caution that AI-based security systems are not infallible and can be manipulated by sophisticated cybercriminals. Additionally, ethical concerns surrounding algorithmic bias and data privacy require further consideration in AI-driven security applications (Ghandour, 2021).

Phishing and Social Engineering: A Persistent Concern

Despite advancements in banking security, participants remained overly concerned about phishing and social engineering attacks. Many shared personal or anecdotal experiences of receiving fraudulent emails and SMS messages

designed to extract sensitive banking details. Participants indicated that while they were generally aware of phishing risks, some still found distinguishing between legitimate and fraudulent communications challenging.

Kuraku (2024) and Kayode-Ajala (2023) identify phishing as a major cybersecurity threat, while Washo (2021) notes that social engineering exploits human psychology rather than technological vulnerabilities. Participants suggested that digital-only banks should be more proactive in educating users about these threats. Kuraku et al. (2023) recommend continuous cybersecurity awareness campaigns to strengthen user resilience. However, White (2021) argues that even digital natives often underestimate cyber risks, highlighting the need for more engaging and interactive educational approaches.

Notably, participants expressed a strong expectation that banks should compensate victims of phishing attacks, suggesting a perception that responsibility for security should be shared between banks and users. This finding underscores the need for clearer communication about user accountability in digital banking security.

Cybersecurity Awareness and Education

Participants were generally critical of existing cybersecurity awareness initiatives, particularly those relying on emails, SMS notifications, and app alerts. Many reported that such messages were often ignored or lost among spam and promotional content. Instead, they recommended banks leverage social media platforms for broader and more effective engagement. Social media penetration in South Africa is significant—26 million users, including 22.75 million aged 18 and above (Kemp, 2023)—banks could enhance outreach by adopting innovative educational strategies tailored to these platforms. Additionally, participants suggested that banks explore more interactive communication channels, such as WhatsApp, to provide real-time security updates and user-friendly educational content. These recommendations align with research suggesting that targeted,

platform-specific cybersecurity education can improve digital financial literacy and risk awareness (Kemp, 2023).

The findings effectively address the first research objective by offering insights into digital natives' perceptions of risk and security in digital-only banking. Participants identified biometric authentication, MFA, and AI-driven fraud detection as critical security features that enhance trust. However, persistent risks such as phishing and social engineering highlight the need for ongoing collaboration between banks and users. The study further underscores the importance of cybersecurity education, with participants advocating for more engaging, platform-specific awareness initiatives.

5.3 Discussion Pertaining to Objective 2: The Influence of Perceived Risk and Security on Digital Natives' Adoption of Digital-Only Banking

Digital natives increasingly embrace digital-only banking, perceiving it as a natural progression in financial services. These banks are not regarded as fundamentally distinct from traditional banks, as both are evolving towards digital-first strategies. Furthermore, digital banking has become an essential tool for accessing financial services. In South Africa, digital-only banking enhances the country's global relevance, particularly as the world transitions towards a cashless economy.

Perceived Safety and Security of Digital-Only Banks

All participants in the study reported engaging with their digital banking applications frequently, either daily or weekly. The platforms are widely perceived as safe and secure, presenting a viable alternative to physical branches in a country with high crime rates. Eliminating in-person banking mitigates risks such as muggings, making digital banking an attractive option. These findings align with previous research by Almaiah et al. (2023), Slazus and Bick (2022), and

Baraba and Mahmudi (2023), which highlight safety as a key driver of digital banking adoption.

Convenience and Efficiency

A primary enabler of digital-only banking adoption is its convenience and efficiency. Users can perform banking transactions at any time and from any location, integrating financial management seamlessly into their daily routines without being constrained by branch visits or banking hours. Additionally, digital-only banking applications leverage advanced technology to provide innovative features relevant to South Africa's evolving technological landscape.

Users benefit from 24/7 assistance through AI-powered chatbots accessible via mobile devices. Previously, customers were required to visit a branch during operational hours and queue to speak to a service agent. Alternatively, access to a personal banker often required a premium payment, which was not a viable option for many. Furthermore, digital banking has introduced personalised real-time analysis of spending behaviours, enabling users to improve their financial management practices. Previously, adding new accounts required certified documentation, necessitating multiple visits to different institutions for verification. In contrast, the digital banking era has enabled online authentication and verification, significantly enhancing user convenience.

These findings align with the Technology Acceptance Model (TAM), particularly the concept of Perceived Ease of Use (PEOU) (Davis, 1986). According to TAM, users are more likely to adopt technology that enhances efficiency and integrates seamlessly into their lives. Chawla et al. (2023) further emphasise that ease of use, trustworthiness, security, perceived risk, and customer satisfaction are critical determinants of FinTech adoption. Similarly, Windasari et al. (2022) found that even tech-savvy digital natives prefer simple, intuitive, and cost-effective banking platforms.

Brand Trust and Transparency

Brand reputation plays a crucial role in digital-only banking adoption. Digital natives prefer banking with well-established institutions, particularly those with existing financial relationships. Transparency regarding security incidents and rapid response to cyberattacks contribute to customer loyalty, as supported by Windasari et al. (2022). Hassan and Ahmed (2023) also suggest that consumers hesitate to fully engage with financial brands without a strong foundation of trust.

Seven participants in this study had digital-only bank accounts, all with Discovery Bank. They cited their prior engagement with Discovery Bank through other financial products, which fostered trust and familiarity. This foundation of trust has provided Discovery Bank with a competitive advantage. New market entrants, such as Bank Zero, must carefully consider their brand positioning strategies. While TymeBank has already penetrated the market, its offerings are primarily targeted at lower-income segments, whereas participants in this study belonged to the middle-class demographic.

However, transparency has its limitations. While users appreciate openness regarding security breaches, excessive disclosure may expose vulnerabilities, as highlighted by Firoozi and Mohsni (2023). Similarly, George and George (2023) argue that banks must balance transparency and robust security measures.

Cost Considerations and Banking Preferences

Contrary to expectations, participants did not perceive digital-only banks as significantly cheaper than traditional banks. While cost advantages, such as lower transaction fees and competitive loan interest rates, could drive adoption, users apply the same selection criteria to digital-only and traditional banks. Factors such as convenience, cost-effectiveness, security, brand reputation, and rewards programmes influence decision-making. Although approximately 75% of South Africans are internet users, data affordability remains a significant barrier (Stats SA, 2024). The country has some of the highest data prices in Africa, exacerbating challenges in digital banking accessibility. Additionally, South

Africa's high youth unemployment rate (45.5%) makes digital banking unattainable for many (Stats SA, 2024).

Participants with digital-only bank accounts did not perceive them as cost-effective. However, all were clients of Discovery Bank, which prioritises rewarding good financial behaviour over cost reduction. Its value proposition integrates various financial products into a comprehensive ecosystem that enhances user benefits. In contrast, TymeBank focuses on providing affordable banking solutions for lower-income markets. These findings suggest that perceptions of digital-only banking costs may vary based on the specific institution and its targeted demographic. Digital banks in South Africa do not yet offer a comprehensive range of banking solutions comparable to traditional banks. For instance, none of the existing digital banks provide vehicle financing, and Discovery Bank only introduced its home loan product in 2024, while TymeBank does not offer long-term financing options. As a result, customers are often required to maintain accounts with traditional banks to access essential financial products unavailable through digital-only banks. This is an additional cost for the user. To remain competitive and establish themselves as primary banking providers, digital banks must expand their product offerings to match those of traditional banks. Failing to do so will likely result in their continued use as secondary or supplementary banking options rather than primary financial service providers.

Infrastructure Challenges and Digital Exclusion

A significant barrier to digital-only banking adoption in South Africa is infrastructural readiness. Digital banking requires stable internet access, reliable electricity, and smartphones. In rural areas, inadequate infrastructure, frequent power outages, and high mobile data costs hinder access. South Africa's high unemployment rate exacerbates these issues, as financial constraints limit smartphone ownership and internet accessibility.

Participants in this study were based in urban areas with reliable internet infrastructure. However, they acknowledged experiencing challenges with connectivity when travelling to other parts of the country. According to Kemp (2023), 31.4% of South Africans reside in rural areas, with 27.7% lacking internet access. Digital-only banks must explore solutions to mitigate these constraints, potentially through strategic partnerships. Mzekandaba (2024) highlights various interventions by private, public, and non-profit organisations aimed at improving public Wi-Fi access in key areas such as schools, hospitals, shopping centres, public buildings, and transport hubs.

These findings align with Cele (2023), who identifies infrastructure challenges, smartphone costs, and mobile data expenses as major barriers to digital banking adoption. However, studies by Ofodile et al. (2024) and Jeník (2022) suggest that digital-only banks can enhance financial inclusion and affordability. While some research associates digital banking with increased accessibility, this study highlights the persistent infrastructural challenges that disproportionately impact rural communities.

Generational Differences in Adoption

Digital-only banking is not universally appealing across age groups. Older generations tend to prefer traditional banking because they rely on physical interactions, stability, and established relationships with financial institutions. Their reluctance to adopt multi-layered security features and security-enhancing applications further complicates digital banking adoption. Many older adults in South Africa lack essential internet skills, potentially limiting their access to digital financial services.

Gwala and Mawela (2024) and Erasmus (2024) emphasise the importance of inclusive technology-driven services to prevent excluding marginalised groups, such as the elderly and rural communities. Faisal et al. (2024) and Chaimaa et al. (2020) further highlight generational disparities in digital banking adoption,

with digital natives demonstrating higher technological proficiency and security awareness than older consumers.

Security and Cyber Risk Awareness

Limited digital literacy increases exposure to cybersecurity risks. Users unfamiliar with digital banking may inadvertently compromise their security, making them more susceptible to fraud. These findings align with Tiwari (2019), who identifies education, infrastructure limitations, and weak internet access as primary barriers to adoption. Aldboush and Ferdous (2023) further emphasise that trust in digital banking is shaped by convenience, user experience, transparency, reliability, and security factors.

This study confirms that perceived risk and security play a critical role in digital-only banking adoption among digital natives in South Africa. While digital natives value security, convenience, and innovation, factors such as brand trust, cost considerations, infrastructural limitations, and generational differences significantly influence adoption rates.

5.4 Discussion pertaining to Objective 3: Measures that Digital-only banks can undertake to improve security

The study revealed that while digital-only banks maintain adequate security measures, continuous improvements are essential to mitigate emerging cyber threats. As cybercriminals refine their tactics, financial institutions must remain proactive in safeguarding customer assets and data. This aligns with findings by Cele and Mlitwa (2024), who reported that consumer apprehension regarding cyberattacks and online fraud inhibits fintech adoption in South Africa. Consequently, digital-only banks must employ robust cybersecurity frameworks, fraud prevention mechanisms, and digital literacy initiatives to ensure sustained consumer trust and security. Key areas for improvement include optimising security technologies, enhancing internal processes, promoting digital awareness, and encouraging responsible user behaviour.

Human Error and Employee Training

Despite the implementation of sophisticated security measures, human error remains a critical vulnerability in banking systems. Therefore, Employee training is fundamental to mitigating cyber threats' risks. Cybersecurity training should extend beyond basic awareness of phishing scams and password security to instilling a culture of cyber vigilance among employees (Hassan & Ahmed, 2023). Given the rapid evolution of cyberattacks, continuous upskilling is essential to counter emerging threats effectively.

Investing in cybersecurity education protects financial institutions and secures customer data (Kuraku et al., 2023). Employees must be equipped to recognise social engineering tactics (Moinescu et al., 2019), but traditional training approaches may be ineffective. Cybersecurity training programmes should be dynamic, addressing challenges such as training fatigue, resource limitations, and diverse learning preferences (Moinescu et al., 2019; Kävrestad & Nohlberg, 2021; Ugbebor et al., 2024; Sarker et al., 2023; Jayatilaka et al., 2021). Customised, engaging training methods are required, albeit at an increased cost.

Leveraging Technology for Enhanced Security

Digital-only banks must harness advanced technologies to fortify their security infrastructure. Artificial intelligence (AI) enhances fraud detection by analysing transactional patterns and flagging irregularities in real-time (Patra et al., 2022). However, AI-based security is not without challenges; adversarial attacks can manipulate machine learning models, and algorithmic biases may pose ethical concerns (Ghandour, 2021; Singh et al., 2024).

Integrated into smartphones, location-based security can further prevent unauthorised access by verifying the geographic consistency of transactions. However, while this feature strengthens security, it raises privacy concerns and may generate false positives that inconvenience users (Prasad & Aithal, 2017; AlShalaan et al., 2022). Digital-only banks must, therefore, strike a balance between technological security enhancements and user convenience.

User-Centric Security Measures

The usability of security features is crucial to adoption. While strong authentication measures are essential, excessive security requirements may frustrate users and deter engagement (Hassan & Ahmed, 2023). Effective security solutions should be robust yet intuitive. Multifactor authentication (MFA), for instance, enhances security when implemented user-friendly (Ejekwu et al., 2024). Security questions, real-time online picture verifications, and biometric authentication provide additional layers of protection but must be carefully designed to prevent exploitation through social engineering.

Transparency and Communication

Digital-only banks must improve communication regarding their security measures to build trust. Effective communication can alleviate user concerns about cyber risks and enhance confidence in digital banking (Chawla et al., 2023). Transparent security disclosures strengthen consumer trust, but excessive technical detail may induce anxiety or confusion (Firoozi & Mohsni, 2023; Aldboush & Ferdous, 2023). Banks should prioritise clear, practical messaging highlighting the direct benefits of security measures to users' financial safety.

Best Practices and Compliance

Adhering to best practices in cybersecurity is critical. Implementing role-based access controls minimises internal data breaches, while compliance with South Africa’s Protection of Personal Information Act (POPIA) ensures regulatory alignment and strengthens consumer protection. Establishing a robust cybersecurity framework aligned with international best practices enhances institutional security (Babikian, 2024).

Nonetheless, cybersecurity compliance presents challenges. Excessive regulatory constraints may stifle innovation, necessitating a risk-based approach (Alshaikh, 2020). Additionally, organisational culture, employee attitudes, and regulatory complexities influence the successful implementation of security

policies (Alotaibi et al., 2016). A holistic, adaptive strategy is required to integrate cybersecurity best practices effectively.

User-Driven Security Enhancements

Users play a pivotal role in securing their digital banking accounts. While financial institutions implement sophisticated security protocols, user negligence remains a major risk factor. Cyberattacks can occur when personal devices are lost or compromised due to weak security measures. Users must recognise that their devices serve as gateways to their financial accounts and should enable security features such as biometric authentication and remote-wiping capabilities.

Security-conscious behaviour, including antivirus software and spam filters, enhances online safety. However, many users prioritise convenience over security, making password hygiene a concern. Educating consumers on strong password management and cyber hygiene is essential. Studies by Hassan and Ahmed (2023), Cele and Kwenda (2024), and Kuraku (2024) confirm that user behaviour significantly influences cybersecurity outcomes. Nevertheless, reliance on user awareness alone is insufficient; banks must reinforce security through digital safeguards (Firoozi & Mohsni, 2023; Ali & Hassan, 2020).

Awareness and Education

The study revealed a significant gap in cybersecurity awareness, resulting in risky online behaviour. Users are often unaware of cyber threats, making them vulnerable to fraud (Hassan & Ahmed, 2023). Raising digital literacy levels can mitigate security risks. White (2021) found that cybersecurity awareness training improved Generation Z's ability to identify phishing attacks, malware, and fraudulent transactions.

Current user education efforts, such as emails and SMS notifications, are largely ineffective due to information overload. Alternative approaches, including social media engagement, should be explored. Platforms like WhatsApp provide personalised education, while high-traffic sites like YouTube and TikTok facilitate

visual learning. Twitter (now X) enables real-time security discussions, and Facebook and LinkedIn offer broader educational reach.

Language accessibility is another key factor. Complex technical jargon discourages user engagement; therefore, security messaging should be simple and user-friendly. Gamification and incentive-based learning can enhance participation. Banks can track engagement through quizzes and reward users who demonstrate cybersecurity proficiency. Given the evolving nature of cyber threats, continuous education is essential (Kuraku, 2024; Kuraku et al., 2023). Strengthening digital literacy will enhance security and build long-term customer confidence and satisfaction (Zvavandanga, 2024; Chawla et al., 2023; Kuraku et al., 2023; Hassan & Ahmed, 2023).

This study confirms that while digital-only banks have established sufficient security measures, continuous vigilance is essential. As cyber threats evolve, financial institutions must remain proactive in implementing technological advancements, employee training programmes, user-friendly security solutions, and transparent communication strategies. AI-driven fraud detection and location-based security provide valuable enhancements, yet privacy and ethical concerns must be considered. Effective regulatory compliance strengthens cybersecurity frameworks, though overregulation may pose challenges.

The role of users in cybersecurity cannot be overlooked. Digital literacy and awareness campaigns are crucial in mitigating risks, and banks must leverage innovative communication channels to educate consumers. A multifaceted approach—incorporating institutional security measures, regulatory compliance, and user education—will be critical in sustaining the long-term security and viability of digital-only banking in South Africa.

5.5 Discussion of Findings in Relation to the Technology Acceptance Model (TAM) and Perceived Risk Theory

a. *Perceived Risk Theory (PRT)*

Bauer (1967) introduced the Perceived Risk Theory (PRT), which categorises consumers as either risk-taking or risk-averse, with multiple dimensions of perceived risk influencing their purchasing decisions. In the context of digital banking, key risk dimensions include performance, financial, privacy, time, and security risks, as discussed in Chapter 2. This study found that digital natives expressed concerns regarding adopting digital-only banking in areas with poor internet infrastructure, as these banks are entirely virtual and reliant on stable internet connections. This highlights performance risk, where consumers anticipate service disruptions or inaccessibility.

Financial risk was also a prominent concern, with digital natives fearing potential financial losses due to cyber threats such as hacking and unauthorised access, particularly if a mobile device falls into the wrong hands. In South Africa, where crime rates are high, the likelihood of such risks was seen as significant. Participants noted that losing a mobile device would necessitate access to another device to notify the bank and secure their accounts. However, the time lag between losing a device and reporting the incident was seen as a vulnerability, as cybercriminals could exploit this window to gain unauthorised access, especially if security measures like remote device wiping were not enabled.

Privacy risks were also a major concern, with digital natives expressing anxiety over increasing cyberattacks, particularly phishing attempts targeting banking employees and consumers. They emphasised the necessity of cybersecurity awareness and training to mitigate such risks. Without adequate consumer education and security precautions, successful attacks could compromise sensitive customer data, reinforcing the need for robust privacy protection measures. Furthermore, the study found that digital-only banking may be

challenging for older generations and less tech-savvy individuals who struggle with digital platforms. Younger consumers, who are more engaged with technology, were perceived to be better equipped to manage these risks.

Overall, the findings of this study align with Perceived Risk Theory, as digital natives recognise the risks associated with digital-only banking. However, these risks can be mitigated through proactive security measures, including biometric authentication and AI-enabled fraud detection. The study further highlights the importance of consumer education and transparency in fostering trust in digital banking. Banks must implement comprehensive risk management strategies that address performance, financial, privacy, and security risks. Additionally, digital banks should develop targeted educational campaigns to empower consumers with the knowledge to protect themselves from cyber threats.

b. *Technology Acceptance Model (TAM)*

The findings of this study also align with the Technology Acceptance Model (TAM), which posits that technology adoption is influenced by Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). Digital natives in this study cited convenience, ease of use, efficiency, and rewards as key factors in adopting digital-only banking. Many participants found that digital banking platforms provided all necessary banking functionalities without physical branch visits. Accessing banking services 24/7 without restrictions on operating hours was a particularly valued feature. Additionally, participants reported that customer service in digital-only banking was efficient, with most issues being resolved timeously via telephone or digital support channels. This reflects the perceived usefulness of digital banking platforms.

The study was conducted among digital natives residing in urban areas with stable internet connectivity. However, it was noted that less technologically savvy individuals, particularly older generations, and consumers in underserved areas with limited internet infrastructure, face greater challenges in adopting digital banking. These consumers may struggle navigating digital platforms and are

more vulnerable to online fraud, including phishing attacks. This supports prior research by Venkatesh et al. (2003), which found that PEOU is not uniform across all user groups. To increase adoption rates, digital-only banks must focus on creating intuitive and inclusive banking platforms that cater to diverse users. This includes incorporating multiple language options, simplifying onboarding processes, and offering proactive customer support.

Another critical challenge highlighted in this study is South Africa's high levels of unemployment and the cost of internet access. Many South Africans may find digital banking inaccessible due to the smartphone requirement and the financial burden of purchasing mobile data. The cost of internet access was identified as a significant barrier to adoption, particularly for low-income consumers. To address this, digital-only banks should collaborate with internet service providers to develop cost-effective solutions, such as zero-rated banking apps that allow users to access banking services without incurring data costs. Additionally, banks should engage with government stakeholders to advocate for accelerated internet infrastructure development, particularly in underserved areas.

Security perceptions also play a crucial role in determining the perceived usefulness of digital banking. While digital natives acknowledged the convenience and efficiency of digital banking, concerns about cybercrime and fraud remained prevalent. Trust in digital banking was found to be contingent on the strength of security measures implemented by banks. This finding aligns with Alalwan et al. (2018), who suggest trust enhances PU. However, participants expressed a need for greater transparency regarding security measures, as certain protections—such as AI-driven fraud detection and multifactor authentication (MFA)—are not always visible to users, leading to uncertainty about their effectiveness. Digital-only banks must, therefore, clearly communicate the security features they employ to enhance consumer confidence.

5.6 Conclusion

This study underscores the critical role of perceived risk and security in shaping digital natives' adoption of digital-only banking in South Africa. While digital banking is generally perceived as safe and secure, continuous advancements in cybersecurity are necessary to mitigate evolving cyber threats. Digital-only banks have implemented robust security measures, yet maintaining consumer trust requires proactive investment in technology, employee training, and user education.

The findings align with the Technology Acceptance Model (TAM), particularly the constructs of Perceived Ease of Use (PEOU) and Perceived Usefulness (PU), which influence digital banking adoption. Users are more likely to adopt platforms that integrate seamlessly into their financial routines while ensuring high security. However, security concerns remain a double-edged sword: stringent security protocols enhance protection but can also create usability challenges. This highlights the need for a balanced approach where security does not compromise accessibility.

Furthermore, institutional trust is pivotal in adoption, as digital natives prefer established financial brands with proven security standards. The study also highlights infrastructure constraints, such as high mobile data costs and unreliable internet access, which create a digital divide, particularly affecting lower-income and rural populations. While digital banking enhances financial inclusion, infrastructural limitations may inadvertently exclude vulnerable groups, aligning with previous studies on digital disparities.

Addressing these challenges requires a multi-pronged strategy. Banks must leverage AI-driven fraud detection, biometric authentication, and location-based security while ensuring transparency in risk communication. Equally, consumers must adopt responsible digital behaviours, reinforcing the shared responsibility of cybersecurity. Public and private sector collaboration in digital literacy initiatives and improved internet accessibility will further bridge the digital gap.

As South Africa moves toward an increasingly digital financial ecosystem, this study highlights the importance of user-centric, risk-mitigating, and technology-driven security enhancements. Future research could explore cross-generational perspectives on digital banking adoption, further assessing how evolving fintech solutions address digital inclusion and trust concerns. Ultimately, digital-only banks must balance security, efficiency, and accessibility to foster long-term adoption and sustainability in South Africa's digital economy.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This study sought to understand customer experiences with digital-only banks in South Africa amongst digital natives, specifically focusing on their perceived risks and security. The findings were discussed in the previous chapter. This chapter concludes alignment with the research objectives. The chapter also specify limitations to the study, recommends that digital-only banks can implement to improve customer trust and adoption, as well as suggestion for further research.

6.2 Conclusions regarding research objective 1

The study confirms that perceived risk and security are pivotal in the adoption of digital-only banking, aligning with Technology Acceptance Model (TAM), which posits that security concerns influence Perceived Ease of Use (PEOU) and Perceived Usefulness (PU). While digital banks have implemented robust security measures, continuous adaptation remains necessary to counter the evolving nature of cyber threats. Digital natives generally perceive banking applications as secure; however, the rapid pace of technological advancement necessitates a proactive approach to maintaining security. This study found that users recognise the significant investments digital-only banks make in security, contributing to increased confidence. Prior research also supports this finding.

Implementing biometric authentication, multifactor authentication (MFA), and AI-enabled fraud detection has been highlighted as a positive step in enhancing security. However, the study also revealed that security enhancements implemented by banks are not always visible to users, necessitating improved communication strategies to foster transparency and trust. Nevertheless, a

delicate balance must be maintained between disclosing security efforts and ensuring that such disclosures do not inadvertently provide cybercriminals with exploitable information.

The findings further underscore the critical role of users in maintaining digital banking security. While banks implement security measures, user behaviour remains a significant risk factor, particularly given the rise in phishing and social engineering attacks. This study highlights that cybersecurity requires a collaborative approach, integrating technological safeguards and informed user engagement. Users must be aware of responsible digital practices to minimise their vulnerability to cyber threats.

The research effectively addresses the first objective by exploring digital natives' perceptions of risk and security in digital-only banking. Key security features like biometrics, MFA, and fraud detection align with existing literature and enhance user confidence. However, persistent risks—particularly social engineering and phishing—necessitate ongoing cooperation between banks and users to ensure a secure banking environment.

6.3 Conclusions regarding research objective 2

The introduction of digital-only banks is perceived as economically beneficial for South Africa, as it enhances the country’s global competitiveness and contributes to technological advancements. The emergence of new roles within the cybersecurity sector, necessitated by increasing cyber threats, is also viewed as an economic advantage due to job creation. The study found that digital natives interact frequently with digital banking platforms and require minimal assistance in navigating them. Moreover, digital-only banking is perceived as a safer alternative to traditional banking, particularly given South Africa’s high crime rates. Digital natives describe this form of banking as convenient, efficient, and user-friendly, though a certain level of technological proficiency is required for a seamless experience.

Trust and brand reputation emerged as key factors influencing adoption, highlighting that digital natives are willing to associate with brands that they can trust. Digital natives do not perceive digital-only banks as fundamentally different from traditional banks, aside from the absence of physical infrastructure. This lack of infrastructure presents a cost advantage for digital-only banks, as they do not incur the operational expenses of maintaining physical branches. Participants expect these cost savings to translate into competitive pricing and financial benefits, serving as an incentive for adoption. However, this study found that digital-only banks in South Africa have not demonstrated cost-effectiveness, which contrasts with findings from previous studies that assert that digital-only banks generally offer lower costs.

Nonetheless, several barriers to adoption persist, particularly in underserved communities where internet access is limited or unreliable. Additional challenges include the high cost of mobile data, widespread unemployment, and varying levels of digital literacy. Digital-only banking requires a degree of technological competence, which may be lacking in some rural communities and older demographics, thereby hindering adoption.

The study further found that digital banking adoption necessitates both digital literacy and cybersecurity awareness. Users must actively secure their devices and remain informed about safe online practices. This study confirms that perceived risk and security play a crucial role in adoption among South African digital natives. While security, convenience, and innovation are valued, factors such as brand trust, cost considerations, infrastructural limitations, and generational differences significantly influence adoption rates.

6.4 Conclusions regarding research objective 3

Digital banking has been widely embraced in South Africa, with digital natives perceiving it as essential rather than an alternative to traditional banking. This study found that digital banking is regarded as the future of banking, representing

a natural progression in the financial sector. However, due to the prevalence of cybercrime, security and risk considerations remain central to adoption decisions. While digital banks are actively enhancing security, digital natives identified key areas for further improvement. One such concern is the vulnerability of bank employees, who may be targeted by cybercriminals, leading to potential financial losses. Employee training is critical in ensuring that bank personnel can effectively identify and respond to cybersecurity threats. However, too much training can create fatigue and become redundant. To prevent training fatigue and maintain engagement, banks should diversify training methods and integrate cybersecurity awareness into their organisational culture.

Although banks are leveraging technology to improve security, they are encouraged to implement user-friendly and personalised security measures that do not compromise ease of use. Examples include location-based security settings, real-time picture verification, and personalised security questions. However, challenges such as location inaccuracy, device dependency, and biases in AI-driven security solutions must be carefully managed. Digital-only banks must ensure that security mechanisms do not create barriers to engagement but rather enhance user experience while maintaining strong security frameworks.

Users play a critical role in digital banking security. The study highlights the importance of consumer education in promoting responsible digital practices, such as strong password management and recognising phishing attempts. Banks are encouraged to enhance cybersecurity awareness initiatives through accessible communication strategies, including social media campaigns, gamification, and simplified language.

The findings sufficiently address the research objective, demonstrating that a collaborative approach—encompassing banks, employees, and users—is essential in strengthening digital banking security. By fostering a culture of cybersecurity awareness, digital-only banks can enhance consumer trust and ensure long-term sustainability in the South African digital banking landscape.

6.5 Limitations

This study focused on understanding the perceived risks and security of digital-only banks, traditional banks with a digital presence were not considered explicitly, the aim was to understand the sentiments around fully virtual way of banking. The population that was targeted for this study is digital natives because it is assumed that they are highly digitally engaged, however, banking services are accessible to everyone outside of the “digital natives’ age range. Another limitation is that the study was conducted from participants based in Gauteng and Cape Town which are urban areas, due to this, inconsistent results may be found if the same study is performed in a rural area, where there are infrastructure challenges. The last limitation of this study is the use of purposive sampling, which, while effective in ensuring that participants meet specific criteria relevant to the research, is inherently susceptible to selection bias and error due to the absence of random sampling. This may limit the generalisability of the findings, as the perspectives captured are influenced by the researcher's selection process rather than a randomly representative sample of the broader population. However, as this study aims to provide in-depth insights rather than statistical generalisation, purposive sampling remains an appropriate methodological choice.

6.6 Recommendations

Based on the findings of this study, digital-only banks must acknowledge that cybersecurity extends beyond technology; it necessitates a holistic approach that integrates the human element. Users often perceive security as the sole responsibility of the banking institution, yet fostering a collaborative security culture is essential. Digital-only banks must implement educational initiatives that reshape user perceptions, encouraging shared responsibility in safeguarding digital transactions.

To ensure effective education and awareness, banks must engage users on accessible platforms and in language that resonates with diverse audiences. Security awareness campaigns should be multilingual, visually engaging, and contextually relevant, particularly for users with varying levels of digital literacy. Employee training is equally critical, as internal vulnerabilities pose a significant security risk. Banks should explore incentive-driven training programmes that reward staff for demonstrating improved cybersecurity behaviours, enhancing engagement and retention of security protocols. Given that learning preferences differ, personalised training approaches must be implemented, leveraging artificial intelligence (AI) to tailor learning experiences. However, banks must mitigate risks associated with AI, such as algorithmic biases, ensuring that security mechanisms are inclusive, transparent, and ethically sound.

Expanding Digital Inclusion and Accessibility

Digital-only banks must collaborate with telecommunications providers and public sector entities to improve digital infrastructure, particularly in rural and underserved areas. One effective approach is the investment in zero-rated banking applications, allowing users in areas with connectivity constraints to access financial services without incurring mobile data costs. At present, digital-only banks are predominantly designed to cater to urban populations, inadvertently exacerbating financial exclusion. Even when banks position themselves as accessible to lower-income groups, users still require smartphones and stable internet access, presenting an additional barrier to adoption. To address South Africa's diverse socio-economic and digital landscape, banks must develop context-specific strategies that account for differences in technological proficiency, generational preferences, and linguistic diversity. This includes:

- User-friendly application interfaces that offer multilingual support and intuitive navigation.
- Simplified onboarding processes with direct support mechanisms, such as proactive client outreach and step-by-step digital literacy guidance.

- Customised engagement channels that allow users to provide continuous feedback, ensuring that digital banking platforms evolve in alignment with consumer needs.

Enhancing Competitive Value Beyond Security

While security remains a primary determinant of digital banking adoption, users consider multiple factors before transitioning. To increase market penetration, digital-only banks must optimise their pricing models and ensure that their offerings provide tangible financial benefits to consumers. Competitive pricing, lower transaction costs, and enhanced incentives will be key motivators for adoption. The current digital-only banks do not offer a full banking offering. For example, none of them have car finance available. These banks need to look into bringing all products that users can get from traditional banking because the gaps will require users to have multiple bank accounts to ensure that they have a full banking suite.

Furthermore, given that cybersecurity threats are a global concern, South Africa's digital banking sector must collaborate with international institutions to adopt global best practices in security standards. Engagement in cross-border partnerships will facilitate knowledge exchange, capacity building, and proactive threat detection strategies, ensuring that South Africa remains at the forefront of digital financial security innovation.

6.7 Suggestions for further research

This study focused on risk and security perspectives from digital natives based in urban areas. Based on findings from this study, future studies can explore:

- Financial inclusion strategies, emerging security technologies, and the effectiveness of digital literacy initiatives in fostering safer digital banking environments.

- Challenges in implementing advanced security measures in the South African context.
- The same study can be carried over to rural communities with infrastructure challenges to understand how digital-only banks can develop strategies, such as zero-rated applications, to attract and cater to that market.

REFERENCES

Accenture. (2023). Global Banking Consumer Study. In Accenture. Retrieved March 3, 2024, from https://www.accenture.com

Ahmed, S. K. (2024). The pillars of trustworthiness in Qualitative research. Journal of Medicine, Surgery, and Public Health, 100051. https://doi.org/10.1016/j.glmedi.2024.100051

Agárdi, I., & Alt, M. A. (2022). Do digital natives use mobile payment differently than digital immigrants? A comparative study between generation X and Z. Electronic Commerce Research, 24(3), 1463–1490. https://doi.org/10.1007/s10660-022-09537-9

Agur, I., Peria, S. M., & Rochon, C. (2020). Digital financial services and the pandemic: Opportunities and risks for emerging and developing economies. International Monetary Fund Special Series on COVID-19, Transactions, 1, 2-1.

Alamri, W. A. (2019). Effectiveness of qualitative research methods: interviews and diaries. International Journal of English and Cultural Studies, 2(1), 65. https://doi.org/10.11114/ijecs.v2i1.4302

Aldammagh, Z., Abdeljawad, R., & Obaid, T. (2021). Predicting Mobile Banking Adoption: An Integration of TAM and TPB with Trust and Perceived Risk. *Financial Internet Quarterly*, *17*(3), 35–46. https://doi.org/10.2478/fiqf-2021-0017

Albort-Morant, G., Sanchís-Pedregosa, C., & Paredes, J. R. P. (2021). Online banking adoption in Spanish cities and towns. Finding differences through TAM application. Economic Research-Ekonomska Istraživanja, 35(1), 854–872. https://doi.org/10.1080/1331677x.2021.1945477

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies, 11(3), 90. https://doi.org/10.3390/ijfs11030090

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 352–358. https://doi.org/10.1109/icitst.2016.7856729

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. Computers & Security, 98, 102003.

AlShalaan, M., AlSubaie, R., & Latif, R. (2022). Location Privacy Issues in Location-Based Services. 2022 Fifth International Conference of Women in Data Science at Prince Sultan University, 129–132. https://doi.org/10.1109/wids-psu54548.2022.00037

Ali, M., Raza, S. A., Khamis, B., Puah, C. H., & Amin, H. (2021). How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. Foresight, 23(4), 403–420. https://doi.org/10.1108/fs-09-2020-0095

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. International Journal of Information Management, 53, 102102. https://doi.org/10.1016/j.ijinfomgt.2020.102102

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on Smart M-Banking Application using SEM. Sustainability, 15(13), 9908. https://doi.org/10.3390/su15139908

Anders, T. (2024, March 24). Discovery set to exceed target of 1-million banking clients by 2026. Business LIVE. Retrieved May 2, 2024, from https://www.businesslive.co.za/bt/business-and-economy/2024-03-24-discovery-set-to-exceed-target-of-1-million-banking-clients-by-2026/

Anggraeni, R., Hapsari, R., & Muslim, N. A. (2021). Examining Factors Influencing Consumers Intention and Usage of Digital Banking: Evidence from Indonesian Digital Banking Customers. Asia Pacific Management and Business Application, 009(03), 193–210. https://doi.org/10.21776/ub.apmba.2021.009.03.1

Assala, K., Bylykbashi, S., Lee, J., & Hikkerova, L. (2023). Assessing perceptions of open banking: The case of digital natives in France. *Gestion 2000*, *Volume 39*(4), 45–65. https://doi.org/10.3917/g2000.394.0045

Babikian, J. (2024). Navigating legal frontiers: Exploring emerging issues in cyber law. Revista Española De Documentación Científica, 17(02), 0210–0614. https://www.researchgate.net/profile/John-Babikian/publication/377964834_Navigating_Legal_Frontiers_Exploring_Emerging_Issues_in_Cyber_Law/links/65bfc3921bed776ae32caa15/Navigating-Legal-Frontiers-Exploring-Emerging-Issues-in-Cyber-Law.pdf

Bajpai, N., & Biberman, J. (2021). Digital Transformation and the 2030 Sustainable Development Agenda. ICT India Working Paper, 44. https://doi.org/10.7916/d8-ybcz-3d35

Baraba, R. a. A., & Mahmudi, M. (2023). Understanding the millennial generation behaviour in using digital banking. Asean International Journal of Business, 2(1), 1–13. https://doi.org/10.54099/aijb.v2i1.394

Bauer, R. A. (1967). Consumer behaviour as risk taking. Marketing: Critical perspectives on business and management, 593, 13-21.

Bennett, S., Maton, K., & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. *British Journal of Educational Technology*, *39*(5), 775–786. https://doi.org/10.1111/j.1467-8535.2007.00793.x

Birkel, H. S., Veile, J. W., Müller, J. M., Hartmann, E., & Voigt, K. (2019). Development of a risk framework for industry 4.0 in the context of sustainability for established manufacturers. Sustainability, 11(2), 384. https://doi.org/10.3390/su11020384

Boston Consulting Group. (2022). The future of retail banking in South Africa. Boston Consulting Group 2022. Retrieved February 7, 2024, from https://web-assets.bcg.com/e0/b5/faf9583a45439c9ae8a8f6b60ed3/bcg-future-of-retail-banking-south-africa-aug-2022.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Braun, V., & Clarke, V. (2013). Successful qualitative research: A practical guide for beginners. SAGE Publications.

Bryman, A. (2016). Social research methods (5TH ed.). Oxford University Press.
Business Tech Africa. (2023, January 13). South Africa's digital banking conflict. Retrieved April 2, 2024, from https://www.businesstechafrica.co.za/business/banking-and-finance/2023/01/13/south-africas-digital-banking-conflict/

Caelli, K., Ray, L., & Mill, J. (2003). 'Clear as mud': toward greater clarity in generic qualitative research. International Journal of Qualitative Methods, 2(2), 1–13. https://doi.org/10.1177/160940690300200201

Cahete, J. (2020). Traditional Banking at Digital Age Are they keeping up with changes in consumer behaviour? Millennials' perception in the Portuguese Market [MA Thesis, ISCTE-Instituto Universitario de Lisboa (Portugal).]. https://www.proquest.com/docview/3122643733/previewPDF/CE181380FFD14A16PQ/1?accountid=15083

Caldas, M. P. (2003). Research design: qualitative, quantitative, and mixed methods approaches. RAC. Revista De Administração Contemporânea, 7(1), 223. https://doi.org/10.1590/s1415-65552003000100015

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. Journal of Research in Nursing, 25(8), 652–661. https://doi.org/10.1177/1744987120927206

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime. https://doi.org/10.1108/jfc-10-2023-0263

Cele, S. (2023). Determining customer acceptance of digital-only banks in South Africa: UTUAT extension. South African Journal of Information Management, 25(1). https://doi.org/10.4102/sajim.v25i1.1628

Cele, S. K., & Mlitwa, N. B. (2024). Determining customer acceptance of digital-only banks in South Africa: Unified Theory of Acceptance and Use of Technology extension. South African Journal of Information Management, 26(1). https://doi.org/10.4102/sajim.v26i1.1628

Chaimaa, B., Najib, E., & Rachid, H. (2020). E-banking Overview: Concepts, challenges and solutions. Wireless Personal Communications, 117(2), 1059–1078. https://doi.org/10.1007/s11277-020-07911-0

Chawla, U., Mohnot, R., Singh, H. V., & Banerjee, A. (2023). The Mediating Effect of Perceived Trust in the Adoption of Cutting-Edge Financial Technology among Digital Natives in the Post-COVID-19 Era. Economies, 11(12), 286. https://doi.org/10.3390/economies11120286

Chiu, C., Wang, E. T. G., Fang, Y., & Huang, H. (2012). Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. Information Systems Journal, 24(1), 85–114. https://doi.org/10.1111/j.1365-2575.2012.00407.x

Cho, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. Journal of Retailing, 82(1), 25–35. https://doi.org/10.1016/j.jretai.2005.11.002

Choung, Y., Pak, T., & Chatterjee, S. (2025). Digital Financial Literacy and Life Satisfaction: Evidence from South Korea. Behavioural Sciences, 15(1), 94. https://doi.org/10.3390/bs15010094

Çoklar, A. N., & Tatli, A. (2021). Examining the digital nativity levels of digital generations: From Generation X to Generation Z. Shanlax International Journal of Education (Online), 9(4), 433–434. https://doi.org/10.34293/education.v9i4.4224

Cox, D. F., & Rich, S. U. (1964). Perceived risk and consumer Decision-Making—The case of telephone shopping. Journal of Marketing Research, 1(4), 32–39. https://doi.org/10.1177/002224376400100405

Creswell, J. W. (1994). Research Design: Qualitative, quantitative, and mixed methods approaches. http://www.revistacomunicacion.org/pdf/n3/resenas/research_design_qualitative_quantitative_and_mixed_methods_approaches.pdf

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and Implementation. The Counseling Psychologist, 35(2), 236-264. https://doi.org/10.1177/0011000006287390

Cresswell, J. (2013). Qualitative inquiry & research design: Choosing among five approaches.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Davis, F. D. (1989). Technology acceptance model: TAM. Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behaviour and Technology Adoption, 205, 219.

Daqar, M. a. M. A., Arqawi, S., & Karsh, S. A. (2020). Fintech in the eyes of Millennials and Generation Z (the financial behaviour and Fintech perception). Banks and Bank Systems, 15(3), 20–28. https://doi.org/10.21511/bbs.15(3).2020.03

Devault, M. L. (2019). Triangulation and member checks in qualitative research. In P. Leavy (Ed.), The Oxford handbook of qualitative research (2nd ed., pp. 211–224). Oxford University Press.

Dowling, G. R. (1986). Perceived risk: The concept and its measurement. Psychology & Marketing, 3(3), 193–210. https://doi.org/10.1002/mar.4220030307

Ejekwu, G. U., Ajodo, S., Lawal, O. M., & Balogun, O. S. (2024). Multi-Factor Authentication web security system based on facial recognition, one time password, and hashed secure question. In Advances in web technologies and engineering book series (pp. 66–85). https://doi.org/10.4018/979-8-3693-1487-6.ch004

Endsley, F., Matthews, L., & Ward, C. (2020). An Analysis of Millennials and their Interactions with Financial Institutions. Atlantic Marketing Journal, 9(2), 1. https://paperity.org/p/260514930/an-analysis-of-millennials-and-their-interactions-with-financial-institutions

Enworo, O. C. (2023). Application of Guba and Lincoln's parallel criteria to assess trustworthiness of qualitative research on indigenous social protection systems. Qualitative Research Journal, 23(4), 372–384. https://doi.org/10.1108/qrj-08-2022-0116

Erasmus, D. (2024, October 20). e-Services in South Africa exacerbate inequality through digital barriers. The Mail & Guardian. https://mg.co.za/thought-leader/2024-10-20-e-services-in-south-africa-exacerbate-inequality-through-digital-barriers/

European Banking Authority. (2019). EBA guidelines on ICT and security risk management. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

Faisal, N. A., Nahar, J., Waliullah, M., & Borna, R. S. (2024). The Role of Digital Banking Features in Bank Selection an Analysis of Customer Preferences for Online and Mobile Banking. Frontiers in Applied Engineering and Technology, 1(01), 41–58. https://doi.org/10.70937/faet.v1i01.10

Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: a comparative study. International Journal of Disclosure and Governance, 20(4), 451–477. https://doi.org/10.1057/s41310-023-00190-8

Fishbein and Ajzen (1975): Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behaviour: An introduction to theory and research. Addison-Wesley.

FSCA. (2022). Financial Sector Outlook Study. In Financial Sector Conduct Authority. Retrieved April 5, 2024, from https://www.fsca.co.za

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. New Directions for Program Evaluation (Online)/New Directions for Program Evaluation, 1986(30), 73–84. https://doi.org/10.1002/ev.1427

Ghandour, A. (2021). Opportunities and Challenges of Artificial Intelligence in Banking: Systematic Literature review. TEM Journal, 1581–1587. https://doi.org/10.18421/tem104-12

Ghani, E. K., Ali, M. M., Musa, M. N. R., & Omonov, A. A. (2022). The Effect of perceived usefulness, Reliability, and COVID-19 Pandemic on digital banking effectiveness: Analysis using Technology Acceptance Model. Sustainability, 14(18), 11248. https://doi.org/10.3390/su141811248

Guest, G., MMacQueen, K., & ENamey, E. (2012). Introduction to Applied Thematic analysis. In SAGE Publications, Inc. eBooks (pp. 3–20). https://doi.org/10.4135/9781483384436.n1

Gwala, N., & Mawela, T. (2024). Investigating the internet skills of older adults in South Africa. Artha Journal of Social Sciences, 23(3). https://journals.christuniversity.in/index.php/artha/article/view/5513/2669

Hakimi, T., Jaafar, J., & Aziz, N. (2023). What factors influence the usage of mobile banking among digital natives? Journal of Financial Services Marketing, 28, pages 763–778, (2023). https://doi.org/10.1057/s41264-023-00212-0

Harahap, D., Afandi, A., & Siregar, T. M. (2023). THE ISLAMIC BANKING CUSTOMERS' INTENTION TO USE DIGITAL BANKING SERVICES: AN INDONESIAN STUDY. Journal of Islamic Monetary Economics and Finance, 9(3), 533–558. https://doi.org/10.21098/jimf.v9i3.1673

Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion. Orient review International. https://orientreview.com/index.php/etmibd-journal/article/download/17/15

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine, 292, 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Hennink, M., Hutter, I., & Bailey, A. (2020). Qualitative research methods. SAGE.

Henry, P. (2015). Rigor in Qualitative research: Promoting quality in Social Science Research. Research Journal of Recent Sciences, 4(IVC–2015), 25–28. http://isca.in/rjrs/archive/v4/iIVC-2015/6.ISCA-IVC-2015-20SHS-11.pdf

Howe, N., & Strauss, W. (2000). Millennials rising: The next great generation. Vintage.

Hu, Z., Ding, S., Li, S., Chen, L., & Yang, S. (2019). Adoption Intention of Fintech Services for Bank Users: An Empirical Examination with an Extended Technology Acceptance Model. Symmetry, 11(3), 340. https://doi.org/10.3390/sym11030340

Hublikar, S., Pattanashetty, V. B., Mane, V., Pillai, P. S., Lakkannavar, M., & Shet, N. S. V. (2022). Biometric-Based authentication in online banking. In Lecture notes in networks and systems (pp. 249–259). https://doi.org/10.1007/978-981-19-0095-2_26

Husam, H., & Pius, A. (2020). A Review of key paradigms: positivism VS interpretivism. Global Academic Journal of Humanities and Social Sciences, 2020; 2(3) 39-43, 2(2), 2706-901X (P). https://doi.org/10.36348/gajhss.2020.v02i03.001

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021). Evaluation of security training and awareness Programs: Review of current practices and guideline. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2112.06356

Jeník, I. (2022). The customer impact of inclusive digital banking. In https://www.cgap.org/. Retrieved May 7, 2024, from https://www.cgap.org/research/publication/tymebank-case-study-customer-impact-of-inclusive-digital-banking

Jeník, I., Flaming, M., & Salman, A. (2020). INCLUSIVE DIGITAL BANKING: EMERGING MARKETS CASE STUDIES. In https://www.cgap.org/. Retrieved May 7, 2024, from https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Inclusive_Digital_Banking.pdf

Jiang, M., Rifon, N. J., Cotten, S. R., Alhabash, S., Tsai, H. S., Shillair, R., & LaRose, R. (2022). Bringing older consumers onboard to online banking: a generational cohort comparison. Educational Gerontology, 48(3), 114–131. https://doi.org/10.1080/03601277.2021.2021730

Join Discovery Bank | Share-Value Banking. (n.d.). Discovery. Retrieved May 2, 2024, from https://www.discovery.co.za/bank/join-discovery-bank/

Kahlke, R. M. (2014). Generic Qualitative Approaches: Pitfalls and benefits of methodological mixology. International Journal of Qualitative Methods, 13(1), 37–52. https://doi.org/10.1177/160940691401300119

Kakar, Z. U. H., Rasheed, R., Rashid, A., & Akhter, S. (2023). CRITERIA FOR ASSESSING AND ENSURING THE TRUSTWORTHINESS IN QUALITATIVE RESEARCH. International Journal of Business Reflections, 4(2), 150–173. https://doi.org/10.56249/ijbr.03.01.44

Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. Journal of Financial Services Marketing, 26(2), 107–121. https://doi.org/10.1057/s41264-020-00082-w

Kävrestad, J., & Nohlberg, M. (2021). Evaluation Strategies for Cybersecurity Training Methods: A Literature review. IFIP Advances in Information and Communication Technology, 102–112. https://doi.org/10.1007/978-3-030-81111-2_9

Kayode-Ajala, O. (2023). Application of Cyber Threat intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing. Retrieved January 7, 2025, from https://researchberg.com/index.php/araic/article/view/159/152

Kemp, S. (2023, February 13). Digital 2023: South Africa — DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-south-africa?rq=digital%202023%20%3A%20south%20africa

Khedmatgozar, H. R. (2021). The impact of perceived risks on internet banking adoption in Iran: a longitudinal survey. Electronic Commerce Research, 21(1), 147–167. https://doi.org/10.1007/s10660-021-09475-y

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.

Krauss, S. (2015). Research Paradigms and Meaning Making: A primer. The Qualitative Report. https://doi.org/10.46743/2160-3715/2005.1831

Kuraku, D. S. (2024). Curiosity clicks: the need for security awareness. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4666865

Liu, Z., Wang, X., & Liu, J. (2019). How digital natives make their self-disclosure decisions: a cross-cultural comparison. Information Technology & People, 32(3), 538–558. https://doi.org/10.1108/itp-10-2017-0339

Louw, C., & Nieuwenhuizen, C. (2020). Digitalisation strategies in a South African banking context: A consumer services analysis. South African Journal of Information Management, 22(1). https://doi.org/10.4102/sajim.v22i1.1153

Mane, J. S., & Bhosale, S. (2023). Advancements in Biometric Authentication Systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. Revue D Intelligence Artificielle, 37(3), 709–718. https://doi.org/10.18280/ria.370319

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

McKinsey & Company. (2021, October 1). Lessons from the rapidly evolving regulation of digital banking. https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-the-rapidly-evolving-regulation-of-digital-banking

Mdluli, N. (2022). Digital banking penetration in underserved communities in South Africa [MA thesis]. University of the Witwatersrand.

Merriam S. B. (2002). Basic interpretive qualitative research. In Merriam S. B. (Es.), Qualitative research in practice (pp. 37–39). San Francisco, CA: Jossey-Bass.

Mmari, P., Horne, R., Appiah, E. K., & Gobind, J. (2024). The role of digital financial literacy for inclusive banking in Tanzania. The International Journal of Organizational Diversity, 24(2), 17–40. https://doi.org/10.18848/2328-6261/cgp/v24i02/17-40

Moinescu, B., Stanciu, D., & Petrescu, L. (2019). Human error and cybersecurity risks: The role of awareness programs. Journal of Security & Risk Management, 7(3), 90-108.

Morake, M., Dube, T., & Masango, P. (2021). The effectiveness of biometric authentication in digital banking security. South African Journal of Financial Technology,

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12. https://doi.org/10.3389/fpsyg.2021.561011

Mudduluru, R. V. (2024). EXPLORING FACTORS INFLUENCING ADOPTION AND USAGE OF PRIVACY-ENHANCING TOOLS AMONG SMARTPHONE USERS [Master of Science, Purdue University]. https://doi.org/10.25394/PGS.26072809.v1

Mzekandaba, S. (2024, May 20). South Africa sets Africa's pace on Wi-Fi connectivity. ITWeb. https://www.itweb.co.za/article/south-africa-sets-africas-pace-on-wifi-connectivity/dgp45qaBx8wvX9l8

Nangin, M. A., Barus, I. R. G., & Wahyoedi, S. (2020). The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption. Journal of Consumer Sciences, 5(2), 124–138. https://doi.org/10.29244/jcs.5.2.124-138

National Treasury. (2023). A financial sector for all. In National Treasury. Department of National Treasury. Retrieved March 7, 2024, from https://www.treasury.gov.za

Ncube, J. (2020). The impact of mobile banking customer experience on loyalty among millennials in South Africa. https://open.uct.ac.za/handle/11427/32933

Nel, J., & Boshoff, C. (2020). "I just don't like digital-only banks, and you should not use them either": Traditional-bank customers' opposition to using digital-only banks. Journal of Retailing and Consumer Services, 59, 102368. https://doi.org/10.1016/j.jretconser.2020.102368

Nel, J., & Boshoff, C. (2021). Traditional-bank customers' digital-only bank resistance: evidence from South Africa. International Journal of Bank Marketing, 39(3), 429–454. https://doi.org/10.1108/ijbm-07-2020-0380

Njele, C. C., & Phiri, J. (2021). Factors affecting usage of mobile money services and their impact on financial inclusion: case of Lusaka province. International Journal of Business and Management, 16(7), 104. https://doi.org/10.5539/ijbm.v16n7p104

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104

Obiora, K., & Ozili, P. K. (2023). Benefits of Digital-Only Financial Inclusion. In Advances in finance, accounting, and economics book series (pp. 261–269). https://doi.org/10.4018/979-8-3693-0082-4.ch015

Ofodile, N. O. C., Odeyemi, N. O., Okoye, N. C. C., Addy, N. W. A., Oyewole, N. a. T., Adeoye, N. O. B., & Ololade, N. Y. J. (2024). DIGITAL BANKING REGULATIONS: A COMPARATIVE REVIEW BETWEEN NIGERIA AND THE USA. Finance & Accounting Research Journal, 6(3), 347–371. https://doi.org/10.51594/farj.v6i3.897

Oyewole, A., Okoye, C., Ofodile, O., & Ugochukwu, C. (2024). Cybersecurity Risks in Online Banking: A Detailed review and Preventative Strategies application. World Journal of Advanced Research and Reviews, 21(03), 625–643. https://doi.org/10.30574/wjarr

Park, J., Yoo, J. W., Cho, Y., & Park, H. (2024). Understanding switching intentions between traditional banks and Internet-only banks among Generation X and Generation Z. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-06-2023-0338

Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing digital payment systems: combining AI, big data, and biometric authentication for enhanced security. International Journal of Engineering and Computer Science, 11(08), 25618–25631. https://doi.org/10.18535/ijecs/v11i08.4698

Payne, E. M., Peltier, J. W., & Barger, V. A. (2018). Mobile banking and AI-enabled mobile banking. Journal of Research in Interactive Marketing, 12(3), 328–346. https://doi.org/10.1108/jrim-07-2018-0087

Piotrowska, N. a. I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. Economics and Business Review/ the Poznań University of Economics Review, 10(1). https://doi.org/10.18559/ebr.2024.1.1019

Prasad, K. P., & Aithal, P. S. (2017). A Study on Enhancing Mobile Banking Services using Location based Authentication. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.583230

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 2: Do they really think differently? On The Horizon, 9(6), 1–6. https://doi.org/10.1108/10748120110424843

Putra, A., Linawaty, D., Halianto, Y., & Calista, N. (2023). Factors Affecting Intention to Use on the Digital Banking Services Offered by Digital Banks in Indonesia. International Journal of Industrial Engineering and Operations Management (IJIEOM), 105–117. https://doi.org/10.46254/ap03.20220021

PwC. (2024). South Africa - Major Banks analysis. South Africa. Retrieved May 9, 2024, from https://www.pwc.co.za/en/publications/major-banks-analysis.html

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. Qualitative Research in Accounting & Management, 8(3), 238–264. https://doi.org/10.1108/11766091111162070

Rajaobelina, L., Brun, I., Line, R., & Cloutier-Bilodeau, C. (2020). Not all elderly are the same: fostering trust through mobile banking service experience. International Journal of Bank Marketing, 39(1), 85–106. https://doi.org/10.1108/ijbm-05-2020-0288

Reepu, R., & Arora, R. (2022). The effect of perceived risk on intention to use online banking. Universal Journal of Accounting and Finance, 10(1), 62–71. https://doi.org/10.13189/ujaf.2022.100107

Rodrigues, L. F., Oliveira, A., & Rodrigues, H. (2023). E-banking usage by Gen X, Y, and Z generations. AHFE International. https://doi.org/10.54941/ahfe1004320

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93-114.

SABRIC. (2022). South African Banking Risk Information Centre: Annual Crime Statistics. In SABRIC. Retrieved August 6, 2023, from https://www.sabric.co.za

Sadiku, M. N. O., Shadare, A. E., & S.M Musa, S. (2017). Digital Natives. International Journals of Advanced Research in Computer Science and Software Engineering. https://doi.org/10.23956/ijarcsse.v7i7.111

Saif, M. a. M., Hussin, N., Husin, M. M., Alwadain, A., & Chakraborty, A. (2022). Determinants of the intention to adopt Digital-Only Banks in Malaysia: the extension of environmental concern. Sustainability, 14(17), 11043. https://doi.org/10.3390/su141711043

Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2023). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. Journal of Systems and Software, 208, 111899. https://doi.org/10.1016/j.jss.2023.111899

Salqaura, S. A., Lestari, I., & Pribadi, T. (2023). Comparative analysis of perceived security level in deciding the use of e-banking in Y and Z generations. Deleted Journal, 11(2), 144. https://doi.org/10.25273/equilibrium.v11i2.17381

Salqaura, F., Mendes, J., & Torres, P. (2023). Consumer satisfaction and security perceptions in digital banking. *Journal of Financial Consumer Behavior, 10*(3), 134-156.

Shahabi, V., Azar, A., Razi, F. F., & Shams, M. F. F. (2020). Simulation of the effect of COVID-19 outbreak on the development of branchless banking in Iran: case study of Resalat Qard–al-Hasan Bank. Review of Behavioural Finance. /Review of Behavioral Finance, 13(1), 85–108. https://doi.org/10.1108/rbf-06-2020-0123

Shaheen, M., Pradhan, S., & Ranajee, N. (2019). Sampling in qualitative research. In Advances in business information systems and analytics book series (pp. 25–51). https://doi.org/10.4018/978-1-5225-5366-3.ch002

Sharma, N. (2023). A digital cohort analysis of consumers' mobile banking app experience. International Journal of Consumer Studies, 48(1). https://doi.org/10.1111/ijcs.12989

Singh, S., Parida, J., & Shekhar, S. (2024). The landscape of AI in Indian banking sector: A theoretical perspective. Journal of Informatics Education and Research. https://doi.org/10.52783/jier.v4i1.688

Slazus, B. J., & Bick, G. (2022). Factors that Influence FinTech Adoption in South Africa: A Study of Consumer Behaviour towards Branchless Mobile Banking. Athens Journal of Business & Economics, 8(1), 429–450. https://doi.org/10.30958/ajbe.8-1-3

Smith, D., & Wong, T. (2023). Global banking security regulations: A comparative study. International Journal of Financial Regulation, 20(2), 78-101.

Stats sa. (2023). Censu 2022. In Stats SA. Retrieved May 6, 2024, from https://census.statssa.gov.za/assets/documents/2022/P03014_Census_2022_Statistical_Release.pdf

Stats sa. (2024, May 17). Unemployment in South Africa: a Youth perspective. Stats SA. Retrieved January 18, 2025, from https://www.statssa.gov.za/?p=17266.

Thangavel, P., Pathak, P., & Chandra, B. (2021). Millennials and Generation Z: a generational cohort analysis of Indian consumers. Benchmarking, 28(7), 2157–2177. https://doi.org/10.1108/bij-01-2020-0050

Thanh, N., & Thanh, T. (2015). The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education. American Journal of Educational Science, 1(2), 24–27. http://www.aiscience.org/journal/ajes

Thusi, P., & Maduku, D. K. (2020). South African millennials' acceptance and use of retail mobile banking apps: An integrated perspective. Computers in Human Behavior, 111, 106405. https://doi.org/10.1016/j.chb.2020.106405

Tiwari, R. (2019). Contribution of Cyber Banking towards Digital India: A way Forward. Khoj an International Peer Reviewed Journal of Geography, 6(1), 46. https://doi.org/10.5958/2455-6963.2019.00005.5

Tiwari, P., & Tiwari, S. K. (2020). Integration of technology acceptance model with perceived risk, perceived trust and perceived cost: Customers' adoption of m-banking. International Journal on Emerging Technologies, 11(2), 447-452.

Transunion. (2023). TransUnion Industry Insights Report: Quarterly overview of consumer credit trends. In Transunion. Retrieved March 5, 2024, from https://www.transunion.co.za/iir/reports/q4-2023.

TymeBank. (2023). Annual report: Financial literacy and security measures in digital banking. https://www.tymebank.co.za

Tymebank. (2024, January 16). TymeBank achieves major financial milestone, reaches profitability in under five years. Retrieved April 15, 2024, from https://www.tymebank.co.za

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS. Journal of Knowledge Learning and Science Technology ISSN 2959-6386 (Online), 3(3), 382–409. https://doi.org/10.60087/jklst.vol3.n3.p382-409

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behaviour Reports, 4, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Wilson, N., Keni, K., & Tan, P. H. P. (2021). The role of perceived usefulness and perceived ease-of-use toward satisfaction and trust which influence computer consumers' loyalty in China. Gadjah Mada International Journal of Business, 23(3), 262-294

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. Journal of Innovation & Knowledge/Journal of Innovation and Knowledge, 7(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

White, D. (2021). Cyber-attack awareness training and its impact on Generation Z's ability to identify phishing attempts. Journal of Cybersecurity Education, Research and Practice, 2021(1), 2.

Xie, J., Ye, L., Huang, W., & Ye, M. (2021). Understanding FinTech Platform adoption: Impacts of perceived value and perceived risk. Journal of Theoretical and Applied Electronic Commerce Research, 16(5), 1893–1911. https://doi.org/10.3390/jtaer16050106

Yussaivi, A. M., Lu, C. Y., Syarief, M. E., & Suhartanto, D. (2021). Millennial Experience with Mobile Banking and Mobile Banking Artificial Intelligence Evidence from Islamic Banking. International Journal of Applied Business Research, 39–53. https://doi.org/10.35313/ijabr.v3i1.121

Zvavandanga, R. (2024). An analysis of the impact of digital banking on consumer protection in the face of increasing cyber-attacks [MA Thesis, University of Johannesburg]. https://ujcontent.uj.ac.za/esploro/outputs/graduate/An-analysis-of-the-impact-of/9938906807691

APPENDIX A: Participant Information Sheet

Dear Participant,

My name is Akani Machimana, and I am a Masters in Management (Digital Business) student at the University of Witwatersrand in Johannesburg. As part of my studies, I am conducting research titled “Risk and Security of Digital-Only Banks: Perspectives from Digital Natives in South Africa.” This study aims to gain an in-depth understanding of the risks and security concerns associated with digital-only banks among digital natives in South Africa. This research is particularly important as digitally native individuals constitute a sizeable portion of the South African population. The insights gained from this study will be valuable for improving digital-only banking services, enhancing customer experience and satisfaction.

You have been identified as a potential participant for this study and are invited to participate. The research will involve a 45–60-minute one-on-one interview conducted either through MS Teams or in person. The interview questions will be aligned with the topic of digital-only banking risks and security concerns. With your permission, interviews will be recorded for reference, and transcription will be enabled. Your participation in this research will not subject you to any physical, emotional, or other harm. All feedback will be kept confidential, and no sensitive information will be collected. Confidentiality will be maintained throughout the collection, storage, and presentation of the findings. Pseudonyms will be used to ensure that information cannot be traced back to individual participants. All data collected will be used solely for this research and will not be shared with anyone else. Participation in this study is voluntary, and there will be no incentives offered. For any reason, you are free to withdraw from the study at any point before, during, or after the interview, without any consequences.

Thank you for considering participating in this study. Your insights will contribute significantly to understanding and improving digital-only banking services in South Africa. For you to participate, I will require the attached consent form to be signed and returned to me.

Please free to reach out to either myself or my supervisor for any questions with regards to this research. If you have any concerns or complaints about the ethical procedures of this research study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27 11 717 1408, email address: hrecnon-medical@wits.ac.za.

Yours Sincerely,

Akani Machimana

Researcher: Akani Machimana

Email: 0313901a@students.wits.ac.za

Cell: + 27 82 260 7007

Supervisor: Dr Ayanda Magida

Email: ayanda.magida@wits.ac.za

Tel: +27 11 717 3953

APPENDIX B: Participant Consent Form

Risk and Security of Digital-only banks: perspective from Digital natives in South Africa

Researcher: Akani Machimana

I, _____ do hereby confirm that I have read the above letter of invitation to participate in the study and that I voluntarily provide my consent to participate in the study. Please select the appropriate option below.

I agree that my participation will remain anonymous	Yes	No
I agree that the researcher will use anonymous quotes in the research	Yes	No
I agree that the interview can be recorded	Yes	No
I agree that information provided may be used anonymously by other researchers following this study for academic purposes, provided they receive ethics clearance from Wits University	Yes	No

Signed _____(Participant): Date_____

Signed _____(Researcher): Date_____

Contact detail for the researcher:

Email: 0313901a@students.wits.ac.za

Cell number: 082 260 7007

APPENDIX C: Research Instrument

	Research Objective	Interview Questions
Introduction		- Reiterate purpose of study - Reiterate voluntary participation and right to withdraw - Clarify any questions and concern - Reiterate consent terms, and confirm consent to continue
Background of Participant		1. Confirm your age (if you are comfortable) if not, please confirm if are between the ages 18 to 43? 2. Do you have a bank account with any of the banks? Do you have an account with a digital-only bank? 3. When was the last time you visited a physical branch, and for what purpose? In the last 6 months, how many times have you visited a physical bank branch? 4. How often do you use digital or online banking? What has been your experience with digital banking?

Digital-only banks		5. Please share your thought on digital-only banks. In your opinion, what is their significance in South Africa? 6. Briefly describe the digital-only banks that you know in South Africa, which one would you consider and why? 7. Would you consider digital-only banks as your primary bank? Please share some of your reasons for the response
	Exploring Perceived Risk and Security levels	8. What do you consider the main risks of digital-only banking? 9. Have you, or someone you know experienced challenges with digital banking? Tell me more about the incident/s. 10. Do you consider digital-only banking safe? Please explain your reasons What is your opinion on the security of digital-only banking? 11. In your opinion, are digital-only banks investing enough in enhancing security of their platforms?
	Impact of Perceived risk and Security levels on adoption	12. What security concerns are likely to prevent you from taking up a with digital-only banks? 13. Which security features do you value when it comes to Digital-only banking? What security features would make you more comfortable with digital-only banking?

	Measures to Improve Security and Reduce risks	14. In your opinions, what should digital-only banks do to strengthen cybersecurity? What is your role is protecting yourself from cyber-attacks? 15. Are you aware of any technologies or other measures that can assist digital-only banks to improve their security?
Conclusion		16. Please share any last thoughts on digital-only banking and how they can become more secure and less risky?

APPENDIX D: Approval of title

UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

Private Bag 3 Wits, 2050
Fax:
Tel:

Reference: Ms Jennifer Mgolodela
E-mail: jennifer.mgolodela@wits.ac.za

16 January 2025
Person No: 0313901A
PAG

Ms AP Machimana
P O Box 3032
Aquapark
0850
South Africa

Dear Ms Akani Machimana

Master of Management: Approval of Title

We have pleasure in advising that your proposal entitled *Risk and security of digital-only banks: perspectives from digital natives in South Africa* has been approved. Please note that any amendments to this title have to be endorsed by the Faculty's higher degrees committee and formally approved.

Yours sincerely

Mrs Marike Bosman
Faculty Registrar
Faculty of Commerce, Law and Management

APPENDIX E: Ethics clearance certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB0313901a/990
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Risk and Security of Digital-only Banks: Perspective from Digital natives in South African
Investigator / Researcher	Miss Akani Machimana
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	02/09/2024
Expiry date	Date of submission of the project / research report
Chairperson	Dr Ayanda Magida ☎ +27 11 717 3953 ✉ ayanda.magida@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

AP Machimana — Signature

25 September 2024 — Date:

APPENDIX F: Turn-it-In report

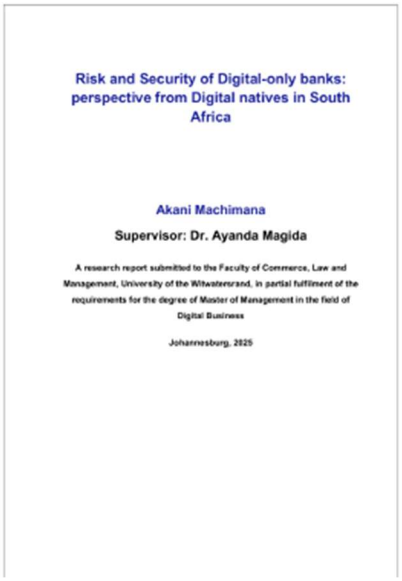
turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Akani Machimana
Assignment title:	Final Research Report
Submission title:	Machimana A MM Research report 1.docx
File name:	Machimana_A_MM_Research_report_1.docx
File size:	709.69K
Page count:	132
Word count:	32,866
Character count:	198,597
Submission date:	28-May-2025 09:10PM (UTC+0200)
Submission ID:	2687017795



Risk and Security of Digital-only banks: perspective from Digital natives in South Africa

Akani Machimana

Supervisor: Dr. Ayanda Magida

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2025

Machimana A MM Research report 1.docx

ORIGINALITY REPORT

2%	2%	1%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	wiredspace.wits.ac.za Internet Source	1%
2	Mistry, Kamal. "Exploring the Inhibitors of Digital Transformation in the South African Mining Industry", University of the Witwatersrand, Johannesburg (South Africa), 2025 Publication	<1%
3	Mashaal A.M. Saif, Nazimah Hussin, Maizaitulaidawati Md Husin, Amgad Muneer, Ayed Alwadain. "Beyond conventions: Unravelling perceived value's role in shaping digital-only banks' adoption", Technological Forecasting and Social Change, 2024 Publication	<1%
4	www.mdpi.com Internet Source	<1%
5	www.fsca.co.za Internet Source	<1%

Exclude quotes	On	Exclude matches	< 50 words
Exclude bibliography	On		

APPENDIX G: Submission Checklist

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

WITS FACULTY OF COMMERCE, LAW & MANAGEMENT

THESIS/DISSERTATION/RESEARCH REPORT – FIRST SUBMISSION CHECKLIST *(for Examination)*

**** This checklist must be completed and included as part of the submission. ****

Name of Candidate:	Akani Machimana	
Person/Student Number:	0313901A	
Qualification:	Master's in Management (Digital Business)	
Title:	Miss	
Supervisor(s):	Dr Ayanda Magida	
Contact Details:	**Cell number(s):** 0822607007	**Email:** 0313901a@students.wits.ac.za

FIRST SUBMISSION CHECKLIST *(for Examination)*

Has this research been submitted with the consent of the supervisor? (Y/N)		Y
Student to submit:	**Electronic copy of research in PDF** *(Hard copy may be required upon request from the examiner)*	✓
	Full Turn-it-in Report *(signed by Supervisor)* *** For WBS – this report does not require the Supervisor's approval ***	✓
	Confirmation of Ethics *(Clearance/Waiver certificate)*	✓
	Overall Supervisor Evaluation form *(MBA candidates ONLY)*	N/A
Supervisor to submit:	**University Clearance Certificate** *(Supervisor to complete and send directly to Faculty)*	
	Supervisor's Report *(Supervisor to complete and send directly to Faculty)*	
Faculty to check on:	Approved title and supervisor(s)	
	Approved examiners	
	Registration status *(students must be registered during the examination period)*	

Please send your research submission to the correct email:

- #Fac-MBAsubmissions@wits.ac.za – for **MBA (ARP)** research submissions
- Veli.Mongwe@wits.ac.za – for PhD and Full Research Masters students **belonging to WBS**
- #Fac-MMsubmissions@wits.ac.za – for MM research submissions **belonging to WBS and WSG**
- Nasreen.Abdulla@wits.ac.za – for PhD and Full Research Masters students **belonging to WSG**
- Tshepo.Mohlakoane@wits.ac.za – for all research types **belonging to Commerce and Law (SEF, SBS, SOA and SOL)**

Please Note:

- *Incomplete submissions will NOT be prioritised.*
- *Outstanding fees must be cleared to enable Awaiting Examiner's registration (upon submission).*
- *WBS submissions may undergo internal academic quality checks before the exam process may begin.*
- *There may be a delay in the examination process – for more information, click:* **Exam Process**
- *For more information on the graduation, click:* **Graduation info.** and **Graduations Office**