



**Mobile banking applications security factors model for aged users
in South Africa**

by

Rumbidzai P Goronga

Submitted in accordance with the requirements
for the degree of

MASTER of SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Prof Adéle Da Veiga

Co-supervisor: Prof Hugo Lotriet

January 2024

DECLARATION

Name: Rumbidzai Petronela Goronga

Student number: 48286885

Degree: MSc Computing

Title of the dissertation:

Mobile banking applications security factors model for aged users in South Africa

I declare that the above dissertation/thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

R.P. Goronga

SIGNATURE

20 February 2024

DATE

ABSTRACT

Technology continues to evolve at a rapid rate, resulting in financial institutions adopting technological developments across multiple products and services, including mobile banking applications. The design of these banking technology products and services is such that services previously offered through physical media or channels can be offered via mobile banking applications that are made available to users for 24 hours per day. While convenient, this also requires a secure experience.

Financial institutions need to adapt and incorporate security into the mobile banking application design for the aged. While it is true that the physical difficulties and limitations brought on by ageing may affect how the aged utilize mobile banking applications, these are not the only factors that may have an impact. There are also security factors that need to be considered.

The literature review conducted as part of this research identified that minimal research has been conducted on the factors that influence the security of mobile banking applications for aged users in South Africa. This quantitative study sought to investigate the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa.

The study proposes an Aged Users' Mobile Banking Application Security Factors Model of the factors that influence the perception of security of mobile banking applications for aged users, based on a review of existing literature and informed by the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2). A questionnaire with 53 statements was developed from the conceptual model, and a quantitative approach was applied using a survey to collect data from (n=286) aged users in South Africa from different social and economic backgrounds. Statistical analysis of the respondents' data was performed using descriptive and inferential statistical analysis. Exploratory Factor Analysis was applied to validate the questionnaire, and Cronbach's Alpha coefficients were used to assess reliability.

The Exploratory Factor Analysis that was conducted on the study questionnaire yielded eight factors. The reliability of the questionnaire was assessed as good,

based on Cronbach's Alpha. Structured Equation Modelling (SEM) and multiple regression analysis conducted on the dataset suggested that privacy and risk are the strongest predictors of technological security perception, which in turn influences the intention to use and the actual use of mobile banking applications by aged users in South Africa.

The Aged Users' Mobile Banking Application Security Factors Model could inform the design of secure mobile banking applications for aged users.

KEY TERMS

elderly, seniors, older adults, mobile banking, on-line security, security, design, user-centred design, security perception

ACKNOWLEDGEMENTS

I would like to extend my gratitude to Professor Da Veiga for her unwavering support and supervision. To Professor Lotriet for starting this journey with me, and the patience as I navigated my way in attempting to commence this study. The unwavering motivation, support, and constant feedback got me through this, and I am truly honored and humbled to have been on this journey with both of you. I would not have come this far without both of you, and I will forever be grateful. Thank you.

To my husband and my daughter, for being with me through the sleepless nights and the difficult days. You remain the reason I never gave up.

To my family – my beautiful mother, for supporting me and encouraging me, I cannot begin to find words to express my gratitude. My sisters, my Shumie – I am grateful.

To a great mentor, H.B., who told me I would do great things and made sure I never doubted it. Thank you for encouraging me to go on this journey and for your constant support.

To everyone who spared their time to contribute to this study, all the conversations, and enduring my endless questions. I truly appreciate your support and patience.

And last, but not least, to my late father - D.A. Goronga, who taught me the value of education, and that I could do anything I set my mind to. I dedicate this work to him.

TABLE OF CONTENTS

DECLARATION	II
ACKNOWLEDGEMENTS	V
LIST OF TABLES	X
LIST OF FIGURES	X
LIST OF APPENDICES	XIII
LIST OF ABBREVIATIONS	XIV
CHAPTER 1	1
INTRODUCTION AND PROJECT OVERVIEW	2
1.1 Introduction	2
1.2 Context and background	2
1.3 Problem statement	4
1.4 Research question(s)	7
1.4.1 Research sub-questions	7
1.5 Research objective(s)	7
1.5.1 Research aim	7
1.5.2 Research objectives	7
1.6 Significance of the study	10
1.7 Research methodology	11
1.7.1 Research philosophy	11
1.7.2 Research approach	11
1.7.3 Research strategy	12
1.7.4 Research methodology choice	12
1.7.5 Research time horizon	12
1.7.6 Research data collection	12
1.7.6.1 Sampling frame	12
1.7.6.2 Sampling technique	12
1.7.6.3 Sample size	12
1.7.7 Research data analysis	13
1.7.8 Data validation	13
1.7.9 Data reliability	13
1.7.10 Ethical considerations	13
1.8 Outline of the study	14
1.9 Conclusion	15
CHAPTER 2	16
MOBILE BANKING APPLICATION SECURITY AND AGED USERS AS MOBILE BANKING APPLICATION USERS	17
2.1 Introduction	17
2.2 User perception	17
2.2.1 Definition of perception	17
2.3 Mobile banking applications	19
2.3.1 Use and availability	20
2.3.2 Design concepts and guidelines	21
2.3.3 Security by design	24
2.3.3.1 No default passwords	26

2.3.3.2 Biometric login.....	26
2.3.3.3 Multi-factor authentication.....	27
2.3.3.4 Push notifications.....	27
2.3.3.5 Automatic logout.....	27
2.3.3.6 Older mobile banking application version blacklisting.....	28
2.3.3.7 Sensitive data encryption.....	28
2.3.3.8 Secure transfer protocols.....	28
2.3.3.9 Security logging.....	28
2.3.3.10 Rooted or jailbreak device check.....	29
2.4 Aged users in South Africa.....	29
2.4.1 Aged users as mobile banking application users.....	30
2.4.2 Aged users as a growing banking customer segment.....	31
2.4.3 Mobile banking application security for the aged.....	31
2.5 Conclusion.....	33
CHAPTER 3.....	34
AGED USERS' MOBILE BANKING APPLICATION SECURITY FACTORS	
CONCEPTUAL MODEL.....	35
3.1 Introduction.....	35
3.2 Literature Overview.....	36
3.2.1 Keywords.....	36
3.2.2 Inclusion and exclusion criteria.....	37
3.2.3 Databases.....	37
3.2.4 Literature search and analysis.....	38
3.2.5 Factors on the security of mobile banking applications for the aged.....	39
3.2.5.1 Moderators.....	49
3.3 Theoretical Framework.....	51
3.3.1 Theories.....	51
3.3.1.1 Unified Theory of Acceptance and Use of Technology (UTAUT).....	51
3.3.1.2 Extended Unified Theory of Acceptance of Technology (UTAUT2).....	53
3.3.2 Constructs.....	57
3.3.3 Hypotheses.....	58
3.3.3.1 Performance Expectancy (PE).....	59
3.3.3.2 Effort Expectancy (EE).....	60
3.3.3.3 Social Influence (SI).....	63
3.3.3.4 Facilitating Conditions (FC).....	64
3.3.3.5 Hedonic Motivation (HM).....	66
3.3.3.6 Price Value (PV).....	67
3.3.3.7 Habit (HB).....	68
3.3.3.8 Perceived Privacy (PP).....	69
3.3.3.9 Technological Trust (TT).....	71
3.3.3.10 Perceived Risk (PR).....	72
3.3.3.11 Perceived Security (PS).....	73
3.3.3.12 Behavioural Intention (BI).....	75
3.3.3.13 Use Behaviour (UB).....	76
3.3.4 Conceptual Model – Aged users' mobile banking application security factors model.....	77
3.4 Conclusion.....	78
CHAPTER 4.....	79
RESEARCH METHODOLOGY.....	80
4.1 Introduction.....	80
4.2 The research onion.....	80
4.3 Research design.....	82
4.4 Research philosophy.....	83

4.4.1 Research paradigm	85
4.5 Research approach.....	86
4.6 Research strategy	87
4.7 Methodological choices.....	90
4.7.1 Quantitative research	90
4.8 Time horizon	92
4.8.1 Longitudinal.....	93
4.8.2 Cross-sectional	93
4.9 Research procedures and techniques	93
4.9.1 Sampling technique.....	93
4.9.2 Sample	95
4.9.2.1 Unit of analysis.....	95
4.9.2.2 Sample size.....	95
4.9.2.3 Target Population.....	96
4.9.3 Data collection.....	97
4.9.3.1 Data collection instrument.....	98
4.9.3.1.1 Questionnaire design.....	100
4.9.3.1.2 Questionnaire refinement	102
4.9.3.1.3 Questionnaire administration	111
4.9.4 Data analysis.....	112
4.9.4.1 Factor analysis	113
4.9.4.2 Descriptive statistics.....	114
4.9.4.3 Inferential statistics.....	114
4.9.4.3.1 Structural equation modelling	114
4.9.4.3.2 Multiple regression analysis.....	115
4.9.5 Data quality	116
4.9.5.1 Validity.....	116
4.9.5.1.1 Face validity	116
4.9.5.1.2 Content validity	117
4.9.5.1.3 Construct validity	117
4.9.5.2 Reliability	118
4.10 Research ethics	119
4.10.1 Study conduct	120
4.10.2 Study inclusivity.....	120
4.10.3 Data integrity	120
4.10.4 Respondent consent	120
4.10.5 Respondent sensitive data.....	120
4.10.6 Respondent confidentiality	120
4.10.7 Respondent participation	120
4.10.8 Research study approval and ethical clearance	121
4.11 Conclusion	121
CHAPTER 5.....	122
RESEARCH FINDINGS	123
5.1 Introduction	123
5.2 Demographic profile	123
5.2.1 Age distribution	124
5.2.2 Education distribution.....	124
5.2.3 Mobile banking application experience distribution	125
5.2.4 Proxy or assistance distribution	126
5.2.5 Demographic profile summary	126
5.3 Instrument validation	126
5.3.1 Determining the number of factors.....	128
5.4 Reliability.....	134
5.5 Revised hypotheses and model	136

5.5.1 Final factors: revised hypotheses	136
5.5.2 Final factors: Revised conceptual model – Aged users’ mobile banking application security factors model.....	136
5.6 Tests of normality.....	137
5.7 Descriptive statistics.....	139
5.7.1 Means and standard deviation	139
5.8 Inferential statistics.....	140
5.8.1 Structural Equation Modelling (SEM).....	140
5.8.2 Multiple regression analysis	143
5.8.4.1 Technological security perception dependent variable	143
5.8.4.2 Risk behaviour dependent variable.....	146
5.8.4.3 Intent and Use Behaviour dependent variable.....	148
5.9 Research hypotheses conclusion	149
5.10 Conclusion	150
CHAPTER 6.....	152
CONCLUSIONS, LIMITATIONS, AND FUTURE RECOMMENDATIONS	153
6.1 Introduction	153
6.2 Reflection of the research study objectives	153
6.2.1 Research questions	154
6.2.1.1 a) What are the factors that influence aged users’ perception of the security of mobile banking applications?.....	154
6.2.1.1.1 To analyse literature for factors that influence the aged users’ perception of the security of mobile banking applications	154
6.2.1.1.2 To develop the Aged Users’ Mobile Banking Application Security Factors Model of the factors that influence aged users’ perception of the security of mobile banking applications	155
6.2.1.1.3 To develop a questionnaire based on the Aged Users’ Mobile Banking Application Security Factors Model.....	156
6.2.1.2 b) What is the relationship between the factors influencing aged users’ perception of the security of mobile banking applications?	156
6.2.1.2.1 To determine the reliability and validity of the questionnaire.....	157
6.2.1.2.2 To investigate the relationship between the factors that influence aged users’ perception of the security of mobile banking applications	157
6.2.1.3 c) What are the factors that must be considered when designing secure mobile banking applications that are used by aged users in South Africa?	158
6.2.1.3.1 To validate the Aged Users’ Mobile Banking Application Security Factors Model	159
6.2.1.3.2 To suggest recommendations for secure mobile banking applications for aged users, based on the Aged Users’ Mobile Banking Application Security Factors Model	160
6.3 Limitations	161
6.4 Future recommendations	162
6.4.1 Recommendations for financial institutions.....	162
6.4.2 Recommendations for future research.....	164
6.5 Conclusion	165
LIST OF REFERENCES	166
INDEX OF APPENDICES	190

LIST OF TABLES

Table 1 – 1: Research questions, objectives, chapters, and deliverables	8
Table 1 – 2: Research methodology, philosophy, and approach: summary selection (Saunders et al., 2019).....	11
Table 2 – 1: The User Engagement Scale with the six user perception aspects (O'Brien & Toms, 2009).....	18
Table 2 – 2: Locally controlled South African banks and mobile banking application status.....	21
Table 2 – 3: South Africa legislature for mobile banking applications	22
Table 2 – 4: Barriers and enablers of adoption of mobile banking applications by aged users in South Africa (Msweli & Mawela, 2021)	30
Table 3 – 1: Literature review inclusion and exclusion criteria	37
Table 3 – 2: Literature findings and summary	41
Table 3 – 3: Summary of literature review of aged users' factors for mobile banking applications and occurrence count.....	48
Table 3 – 4: Moderators of aged users' perceptions of the security of mobile banking applications	50
Table 3 – 5: UTAUT2 constructs	54
Table 3 – 6: Questionnaire statements for Performance Expectancy	60
Table 3 – 7: Questionnaire statements for Effort Expectancy	62
Table 3 – 8: Questionnaire statements for Social Influence	64
Table 3 – 9: Questionnaire statements for Facilitating Conditions	66
Table 3 – 10: Questionnaire statements for Hedonic Motivation	67
Table 3 – 11: Questionnaire statements for Price Value	68
Table 3 – 12: Questionnaire statements for Habit	69
Table 3 – 13: Questionnaire statements for Perceived Privacy	70
Table 3 – 14: Questionnaire statements for Technological Trust	71
Table 3 – 15: Questionnaire statements for Perceived Risk.....	73
Table 3 – 16: Questionnaire statements for Perceived Security.....	75
Table 3 – 17: Questionnaire statements for Behavioural Intention.....	76
Table 3 – 18: Questionnaire statements for Use Behaviour	76
Table 4 – 1: Research methodology philosophy and approach: summary selection, as per Saunders et al. (2019).....	82

Table 4 – 2: Advantages and disadvantages of surveys	88
Table 4 – 3: Advantages and disadvantages of quantitative research	91
Table 4 – 4: Study sampling requirements	97
Table 4 – 5: Expert panel review participants' details	104
Table 4 – 6: Questionnaire Section B expert panel review feedback	106
Table 4 – 7: Questionnaire Section C expert panel review feedback	107
Table 4 – 8: Questionnaire Section A panel group feedback	110
Table 4 – 9: KMO values and correlation adequacy.....	113
Table 5 – 1: KMO and Bartlett's Test, compiled from survey data	127
Table 5 – 2: Eigenvalues for factors, compiled from survey data	128
Table 5 – 3: Rotated pattern mix, compiled from survey data	130
Table 5 – 4: Final factor names with factor loadings	133
Table 5 – 5: Cronbach Alpha coefficient values for the eight factors.....	135
Table 5 – 6: Tests of Normality for the factors.....	138
Table 5 – 7: Descriptive statistics per factor	139
Table 5 – 8: SEM Significance	141
Table 5 – 9: Model summary – Technology security perception dependent variable	143
Table 5 – 10: ANOVA table – Technological security perception dependent variable	144
Table 5 – 11: Coefficients – Technological security perception dependent variable	144
Table 5 – 12: Model summary – Risk behaviour dependent variable	146
Table 5 – 13: ANOVA table – Risk behaviour dependent variable	147
Table 5 – 14: Coefficients – Risk behaviour dependent variable.....	147
Table 5 – 15: Model summary – Intent and Use Behaviour dependent variable	148
Table 5 – 16: ANOVA table – Intent and Use Behaviour dependent variable	148
Table 5 – 17: Coefficients – Intent and Use Behaviour dependent variable	149
Table 5 – 18: Research hypotheses conclusion	150

LIST OF FIGURES

Figure 3 - 1: Workflow process of the creation of the proposed conceptual model .	36
Figure 3 – 2: PRISMA literature search flow diagram.....	39
Figure 3 – 3: UTAUT model (Venkatesh et al., 2003).....	52
Figure 3 – 4: UTAUT2 model (Venkatesh et al., 2012).....	54
Figure 3 - 5: The constructs derivation process	54
Figure 3 – 6: Conceptual model – Aged users’ mobile banking application security factors model.....	77
Figure 4 – 1: The research onion (Saunders et al. 2007)	81
Figure 4 – 2: The relationship between research design and research methodology (Mouton, 2001).....	84
Figure 4 – 3: The deductive approach sequence of steps.....	86
Figure 4 - 4: The questionnaire development process	100
Figure 5 – 1: Age distribution (n=286)	124
Figure 5 – 2: Education distribution (n=286).....	125
Figure 5 – 3: Mobile banking application duration distribution (n=286)	125
Figure 5 – 4: Mobile banking application proxy or assistance distribution (n=284).	126
Figure 5 – 5: Final factors: Revised Conceptual Model – Aged users’ mobile banking application security factors model	137
Figure 5 – 6: Descriptive statistics per factor.....	140
Figure 5 – 7: Resultant structural model.....	142
Figure 5 – 8: Derived structural model	142
Figure 6 – 1: Final validated Aged Users’ Mobile Banking Application Security Factors Model	160

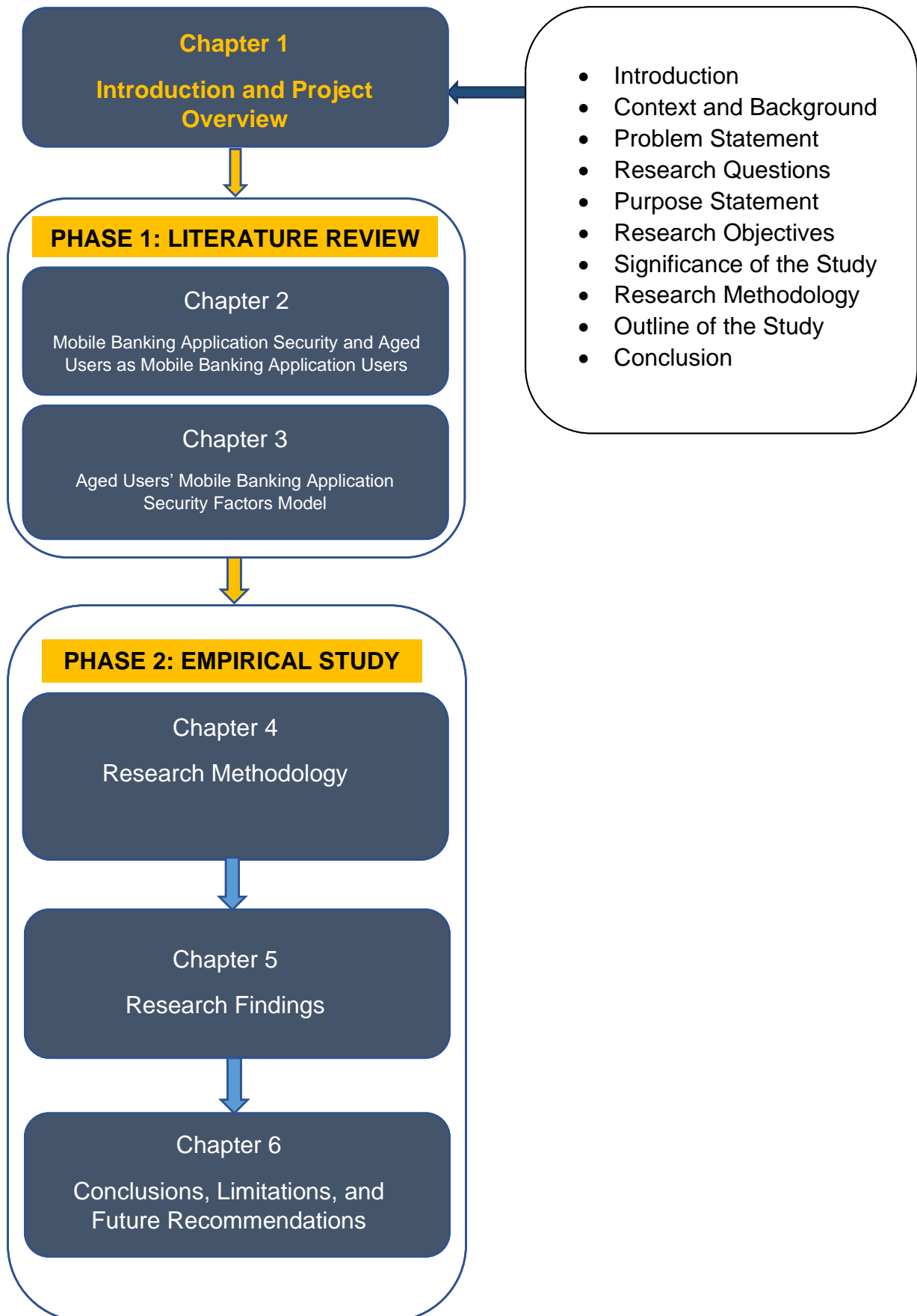
LIST OF APPENDICES

Appendix A: Ethical clearance approval	190
Appendix B: Participant information sheet.....	194
Appendix C: Consent letter	202
Appendix D: Questionnaires.....	204
Appendix E: Anonymous cover letter	237
Appendix F: Statistician confidentiality agreement	239
Appendix G: Factor Loadings.....	242
Appendix H: Reliability statistics.....	244
Appendix I: Structured Equation Modelling (SEM)	259
Appendix J: Multiple regression analysis.....	264
Appendix K: Editorial certificate.....	284

LIST OF ABBREVIATIONS

Abbreviation	Explanation
ASVA	Application Security Verification Standard
BASA	Banking Association of South Africa
DOI	Diffusion of Innovation
EFA	Exploratory Factor Analysis
FSCA	Financial Sector Conduct Authority
KMO	Kaiser-Meyer-Olkin
MFA	Multi-Factor Authentication
OECD	Organization for Economic Cooperation and Development
OWASP	Open Web Application Security Project
PAF	Principal Axis Factoring
PII	Personal Identifiable Information
POPIA	Protection of Personal Information Act
SAPS	South African Police Service
SASSA	South African Social Security Agency
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
UTAUT	Unified Theory of Acceptance and Use of Technology
UTAUT2	Extended Unified Theory of Acceptance and Use of Technology
WHO	World Health Organization

CHAPTER 1



INTRODUCTION AND PROJECT OVERVIEW

1.1 Introduction

This study investigates factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa. After reviewing the literature, a conceptual model was developed, informed by a self-formed hypothesis derived from the body of existing theories. This model was updated once the hypotheses had been tested. The outcome of this study provides an improved understanding of aged users' perceptions of the security of mobile banking applications. The resulting model can assist financial institutions in better designing mobile banking applications that are secure and easy to use, so as to become more digitally and socially inclusive of aged users.

The background and motivation for this study, as well as the problem statement, research objectives, and research questions, are introduced in this chapter. The high-level paradigm for the research design and methodology is also provided. The chapter concludes with the outline of the dissertation and a summary per chapter.

1.2 Context and background

The *Older Persons Act 13(2006)* of South Africa terms females above the age of 60 and males above the age of 65 as 'aged', and the demographics provided by Statistics South Africa (2020) show that the country's population is increasingly ageing. The growth rate among the aged has risen by 3% over the 2019 to 2020 period, compared with the 1.1% growth over the 2002 to 2003 period (Statistics South Africa, 2020). This is a lower-income demographic, which is dependent on retirement funding, family support, and government grants in South Africa (Ralston et al., 2015). The underprivileged aged who meet a set criterion as specified by the government (South African Government, 2017) are recipients of an older person's grant. This is paid by the South African Social Security Agency (SASSA) into the recipient's bank account (Vally, 2016).

Friemel (2014) states that aged adults use technology for several purposes, including banking (Van Boekel, Peek, & Luijkx, 2017). Aged users are recognizing the benefits provided by banking technology products – primarily the ability to remain

independent for longer (Seifert & Schelling, 2018). Therefore, mobile banking application adoption rates in South Africa have increased over the years due to multiple factors (BASA, 2021), including the overall interaction of users across all demographics with financial products and services. This has been intensified by the reduced use of cash by various businesses for security and digitization purposes, and the general increase of digital financial transactions (OECD, 2020). Aged users in South Africa use mobile banking applications for services such as prepaid facility reloading, payment of utility bills, transferring of money, balance checks, and transaction verification – all of which would previously have been conducted at a physical banking premise (Msweli, 2020).

However, age-related factors such as health status and the loss of physical, psychological, and cognitive abilities complicate everyday tasks for the elderly (Wilson et al., 2002). This could lead to an increased risk of visual, auditory, cognitive, and physical deficits (Wilson et al., 2002), which would make using mobile banking applications difficult. This can result in a decline in familiarity due to reduced usage of these mobile banking applications (Mendel & Toch, 2019), which in turn affects decision-making abilities (Brocklehurst & Laurenson, 2008). This aspect is of importance for this research, as it relates to how informed and enabled aged users are when using banking technology products, primarily mobile banking applications; this will guide their perception of how secure mobile banking applications are.

Aged users are prone to financial exploitation, which is a growing concern for the banking industry (BASA, 2021). Financial exploitation includes the elicitation of the aged user's details for scams and fraud (OECD, 2020). With cognitive decline may come the inability to identify if someone is not telling the truth to the aged user, which can result in exploitation (Asp et al., 2012). In some cases, even where they are aware of being victims of such exploitation, aged users may not report this to the relevant authorities (Titus, Heinzelmann, & Boyle, 1995; Van Wyk & Mason, 2001). This is especially of concern in South Africa, which has seen an increase in financial crime statistics (Police recorded crime statistics Republic of South Africa, 2022). This results in a loss of trust and confidence by aged users, due to the perceived lack of security provided by financial institutions for mobile banking applications (Ubam, Hipiny, & Ujir, 2021).

Most aged users depend on caregivers, through friends and family, or on paid financial assistance to fulfil banking needs once age-related factors restrict them from performing these functions themselves (Saukkonen et al., 2022). However, most mobile banking applications are not built to securely support third-party handling (OECD, 2020). In addition, allowing caregivers to assist aged users exposes the aged to exploitation, and exposes their personal and banking details to multiple users (Latulipe, Dsouza, & Cumbers, 2022). Seeking third-party support in using mobile banking applications is not always by choice for aged users; however, every individual has a right to be able to pay for a living, and the aged are included in this right (OECD, 2020).

Financial institutions must provide an environment that is safe and secure for all users to conduct banking transactions (BASA, 2021). There must be a secure and inclusive financial system, supported by the appropriate financial consumer protection arrangements (OECD, 2020).

1.3 Problem statement

Digital accessibility has become a growing need over the past few years for multiple banks globally, with consumers turning to mobile application-based solutions to conduct financial activities (Jin, Kuang, & Fan, 2021). Financial institutions continue to invest in the design and implementation of mobile banking applications that are usually designed to target younger users and professionals (Ubam et al., 2021). However, this takes place in a world where aged users are already struggling to use a smartphone without assistance, and where security concerns are one of the biggest barriers to the adoption of technology (Wong et al., 2018). Assistance to use a smartphone for aged users can be in the form of family or friends (Jayachandran, 2019) and, where none are available, aged users are forced to reach out to strangers or paid volunteers, knowingly or unknowingly exposing themselves to risk (OECD, 2020). The impact of complex security mechanisms and complex mobile application design challenges, which in most cases result in volunteers or proxies (Latulipe et al., 2022), has not been researched extensively for aged users in South Africa.

Mobile banking applications offer ease of use through flexibility and accessibility, with the added benefit of integrated built-in security mechanisms in users' devices

(Tiwari et al., 2020). Aged users are already at a disadvantage because of the natural decline in cognitive ability due to ageing (Wilson et al., 2002). They are therefore not able to realize the full benefits offered by these services, which in turn might also lead to reduced levels of familiarity (Mendel & Toch, 2019) and therefore reduced trust in such applications (Gefen, 2000). These aspects impact aged users' ability to perform normal banking activities, such as remembering how to execute functions on mobile banking applications or memorizing a security pin (Mendel & Toch, 2019). Such factors make the aged susceptible to being victims of financial crimes (Brocklehurst & Laurenson, 2008). However, little research has been done on the effects of security and cognitive factors on the use of mobile banking applications from a South African perspective.

Challenges and security issues faced by aged users have been reduced to disabilities and decline of cognitive abilities due to age, thereby restricting aged users to a deficit model (Wilson et al., 2002). This does not detract from the fact that these are valid concerns that can impact the design and use of mobile banking applications. It is important to acknowledge that these are not the only factors impacting the security of mobile banking applications for aged users. The probability exists that designing for better and improved security becomes limited and that the use of mobile banking applications by older users is restricted if they are reduced to their limitations and impairments, which is not what this study accomplishes (Johnson & Finn, 2017). This further highlights the importance of investigating the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users.

Banking institutions continue to improve services through advanced offerings of mobile banking application design, while the aged continue to face security challenges through the deterioration of physiological and psychological abilities (Wilson et al., 2002), volunteer and proxy challenges, and application design challenges to remain socially enabled and integrated (Vidal, 2019).

Ramnath (2018) states that there has been a general increase in the study and research of the use of mobile phones and the adoption of mobile banking applications globally. However, there is still limited information as to what factors influence the use of mobile banking applications by aged users in South Africa,

particularly aged users' perceptions of security. A few research projects carried out in South Africa had a broad focus, and were not defined to investigate security or the aged; studies include those conducted by researchers such as Assensoh-Kodua, Migiros, & Mutambara (2016), Msweli (2020), Ramnath (2018), Chigori et al. (2020), Koenaitse, Chuchu, & Villiers (2019), Garg, Garg, & Ledwaba (2014), Chigada & Hirschfelder (2017), Slazus & Bick (2022), and Koenaitse, Maziriri, & Chuchu (2021).

Understanding aged users' perception of the secure use of mobile banking applications, given advancements in mobile banking application design, is key to making it easier for aged users to securely use these applications, that is, improving their perceived ease-of-use (Zhuang, Toms, & Demartini, 2016). It also assists with the perceived usefulness and perceived security of aged users' use of mobile banking applications (Tahar et al., 2020). In addition, this might improve the overall adoption of mobile banking applications by aged users, as studies have shown that one of the main obstacles to adopting new technology is security concerns (Frik et al., 2019).

While studies by researchers like Baptista & Oliveira (2015) have examined the effect that certain characteristics have on the adoption of technology, together with UTAUT and UTAUT2, there were no studies found on perceived security within the context of mobile banking applications in South Africa.

In summary, the identified problems are:

- a) There is limited understanding of the impact of complex security mechanisms or processes for mobile banking applications on aged users in a country with as much financial crime as South Africa (BASA, 2021);
- b) There is limited research on perceived security within the context of mobile banking applications for the aged;
- c) There is a reduced level of trust by aged users in using mobile banking applications due to security issues (Gefen, 2000); and
- d) There is not a model to follow when creating mobile banking applications for the aged in South Africa that they may use securely.

The design of mobile banking applications for security should be guided by aged users' feedback, interpretation, and preferences (Sarcar et al., 2017). This can be modelled through a conceptual model, which reduces the possibility of creating

secure mobile banking applications based on incorrect and inconsistent requirements for the aged (Robinson et al., 2015). However, such a model does not currently exist for aged users in South Africa.

This motivates an investigation into aged users' perceptions of the factors that have a significant influence on the perception of security for the use of mobile banking applications, which may improve the design of secure mobile banking applications for aged users.

1.4 Research question(s)

What factors have a significant influence on the perception of security in the use of mobile banking applications by aged users in South Africa?

1.4.1 Research sub-questions

- a) What are the factors that influence aged users' perception of the security of mobile banking applications?
- b) What is the relationship between the factors that influence aged users' perception of the security of mobile banking applications?
- c) What are the factors that must be considered when designing secure mobile banking applications for aged users in South Africa?

1.5 Research objective(s)

1.5.1 Research aim

The aim of this research is to create an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications, by investigating the factors that have a significant influence on the perception of security of use of mobile banking applications by aged users in South Africa.

1.5.2 Research objectives

The following research objectives were answered through a scoping literature review:

- To analyse literature for factors that influence aged users' perception of the security of mobile banking applications;

- To develop the Aged Users' Mobile Banking Application Security Factors Model of the factors that influence aged users' perception of the security of mobile banking applications; and
- To develop a questionnaire based on the Aged Users' Mobile Banking Application Security Factors Model.

The following research objectives were answered through quantitative or empirical research:

- To determine the reliability and validity of the questionnaire;
- To investigate the relationship between the factors that influence aged users' perception of the security of mobile banking applications;
- To validate the Aged Users' Mobile Banking Application Security Factors Model; and
- To suggest recommendations for secure mobile banking applications for aged users, based on the Aged Users' Mobile Banking Application Security Factors Model.

Table 1 – 1 shows the link between research questions, objectives, chapters, and deliverables.

Table 1 – 1: Research questions, objectives, chapters, and deliverables

Research Question	Research Objective	Chapter	Deliverable
a) What are the factors that influence aged users' perception of the security of mobile banking applications?	To analyse literature for factors that influence aged users' perception of the security of mobile banking applications.	2	Literature concepts overview.
		3	Factors list.

Research Question	Research Objective	Chapter	Deliverable
	To develop the Aged Users' Mobile Banking Application Security Factors Model of the factors that influence aged users' perception of the security of mobile banking applications.	3	Research study: conceptual model based on current literature.
	To develop a questionnaire based on the Aged Users' Mobile Banking Application Security Factors Model.	3	Draft questionnaire.
b) What is the relationship between the factors that influence aged users' perception of the security of mobile banking applications?	To determine the reliability and validity of the questionnaire.	4	Defined research methodology.
		5	Final and validated questionnaire. Statistical analysis of results.
	To investigate the relationship between the factors that influence aged users' perception of the security of mobile banking applications.	5	Discussion of results. Tested hypothesis.
6) What are the factors that must be considered when designing secure mobile	To validate the Aged Users' Mobile Banking Application Security Factors Model.	5	Discussion of results. Tested hypothesis.

Research Question	Research Objective	Chapter	Deliverable
banking applications that are used by aged users in South Africa?	To suggest recommendations for secure mobile banking applications for aged users, based on the Aged Users' Mobile Banking Application Security Factors Model.	6	Research suggestions and recommendations.

1.6 Significance of the study

This study seeks to create an Aged Users' Mobile Banking Application Security Factors Model, founded in literature and based on the perceptions of aged users on the factors that have a significant influence on the perception of the security of use of mobile banking applications by aged users. Such a model does not currently exist in this format; the development thereof will therefore contribute to the design and use of mobile banking applications in South Africa as a developing country.

This study will also improve the understanding of aged users' perceptions of the security of mobile banking applications. It is envisaged that this study will help financial institutions to better design mobile banking applications that are secure and easy to use, so as to become more digitally and socially inclusive of this demographic.

The contributions of this study are:

- Methodological: The study will contribute a validated questionnaire based on the constructs developed from literature.
- Practical: The study will contribute a recommendation for mobile banking application development for the aged.
- Theoretical: Through hypothesis testing, a new theory, which is a novel extension of UTAUT2, will be suggested; it offers fresh insights for the creation of mobile banking applications for South Africa's aged users.

1.7 Research methodology

Saunders, Lewis, & Thornhill (2019) demonstrate a research onion, which will be used as basis for the research methodology for this study. Table 1 – 2 shows the application thereof in this study. The methodology will be discussed in detail in Chapter 4.

Table 1 – 2: Research methodology, philosophy, and approach: summary selection (Saunders et al., 2019)

Research onion layer	Research methodology selection
Research philosophy	Positivist
Research approach	Deductive
Research strategy	Survey
Choices	Mono method (Quantitative)
Time horizon	Cross-sectional
Techniques and procedures	Data collection (Questionnaire)
	Data analysis (Inferential and descriptive statistics)

1.7.1 Research philosophy

The positivist philosophy is based on the researcher being separate or disconnected from the object of the study, thereby enabling the researcher to assume an objective view of the study, which is known as objectivism (Neuman, 2014). This renders this philosophy fit for this study, as the role of the researcher is restricted to the collection of data on aged users and to the objective interpretation of the collected data.

1.7.2 Research approach

This is a descriptive study. Robson (2002) defines descriptive research as an inquiry that depicts the accurate profile of people, events, or a situation. This approach was enabled by means of a survey of aged users.

A deductive approach was used to develop hypotheses from the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) on the security factors, to derive variables from the theory, and then to assess these variables using a questionnaire as survey instrument.

1.7.3 Research strategy

This study employed the use of the survey research strategy to collect data on aged users' perceptions, which is suitable for descriptive research (Saunders et al., 2019).

1.7.4 Research methodology choice

This research was quantitative in nature. A data collection technique was employed that produces numerical data (Saunders et al., 2019).

1.7.5 Research time horizon

A cross-sectional time horizon was used, as the study was conducted at a particular point in time (Saunders et al., 2019). The cross-sectional time horizon is mostly used in combination with the survey strategy (Saunders et al., 2019). A three-week time interval was allowed for data collection.

1.7.6 Research data collection

This study made use of a questionnaire that was administered over the Internet; this enabled consistency of the collection of results across all respondents (Saunders et al., 2019), and allowed the researcher to include respondents across multiple locations within South Africa.

1.7.6.1 Sampling frame

The sampling frame comprised consenting aged users in South Africa.

1.7.6.2 Sampling technique

This research made use of convenience sampling, which is a non-probability sampling procedure that allows for the random selection of cases based on convenience and availability to acquire the required sample (Saunders, 2019; Creswell & Creswell, 2018).

1.7.6.3 Sample size

The following relationship was used to determine the sample size (Gerber & Hall, 2017):

$$\underline{\textit{Minimum}} \textit{ number of respondents} = \textit{Total number of questions in the questionnaire} \times 5$$

The study questionnaire consists of 53 questions, therefore at least 265 respondents were included in the study.

1.7.7 Research data analysis

Descriptive and inferential statistics were used to analyse the data for the study. Descriptive statistics were used to outline, present, sort, and group the data, and to present data graphically (Creswell & Creswell, 2018). Inferential statistics were used for generalizations from the sample population. This was achieved using measurements from the population sample to compare the behaviour groups. Statistical data analysis includes the investigation of trends and patterns, as well as the associated relationships using quantitative data. Statistical analysis software such as SSPS were used for statistical data analysis.

1.7.8 Data validation

There are four distinct types of validity, namely, face validity, content validity, construct validity, and predictive validity (Saunders et al., 2019).

In this study, face validity, content validity, and construct validity were used.

1.7.9 Data reliability

Roberts, Priest, & Traynor (2006) described reliability as referring to the level of consistency to which a test instrument can reproduce the same results. For this study, reliability was determined using Cronbach's Alpha coefficients (Cronbach, 1951).

SEM, followed by multiple regression analysis methods, were used to test the hypothesis, and validate the model due to their suitability in elaborating theories and concepts without having to choose from a variety of different statistical techniques or methods (Tabachnick, Fidell, & Ullman, 2013).

1.7.10 Ethical considerations

For this research, ethical principles were ensured by obtaining research ethics approval from the University of South Africa before conducting the study.

According to Altawalbeh, Alkhateeb, & Attarabeen (2019), considerations in research ethics include:

- Ensuring privacy and confidentiality of the data collected;

- Devoting more time to the data collection process and the consent procedure for aged users;
- Ensuring that aged users are treated as autonomous individuals; and
- Ensuring that the cultural beliefs of aged users are respected.

1.8 Outline of the study

This section outlines the structure of the research and the content of the chapters.

Chapter 1: Introduction and project overview

This chapter introduces the research study, the research objectives, and the problem statement.

Chapter 2: Mobile banking application security and aged users as mobile banking application users

An overview is provided of the concepts of the study, focusing primarily on user perception, security, mobile banking applications, and aged users in South Africa.

This forms the first part of Phase 1 of the research, the literature review.

Chapter 3: Aged Users' Mobile Banking Application Security Factors Model

An overview of the literature relevant to the research is provided in Chapter 3. It accounts for known aged user perceptions on the security of mobile banking applications as well as existing security factors on mobile banking applications for the aged, while highlighting the gaps in the current research conducted in South Africa.

The hypotheses for the study are included, and the hypothesized conceptual model is proposed.

The conceptual model is put forth based on the existing literature and serves as the cornerstone for the questionnaire.

This forms the second and final part of Phase 1 of the research, the literature review.

Chapter 4: Research methodology

This chapter discusses the research methodology and the data collection instrument. This includes the research strategy, research approach, and research design.

This forms the first part of Phase 2 of the research, the empirical study.

Chapter 5: Research Findings

The results that were deduced from the collected data are discussed in detail; descriptive and inferential statistical analyses are outlined.

This forms the second part of Phase 2 of the research, the empirical study.

Chapter 6: Conclusions, Limitations and Future Recommendations

This chapter presents the conclusions drawn from the research and how they relate to the research questions. The expected contribution and future research are included.

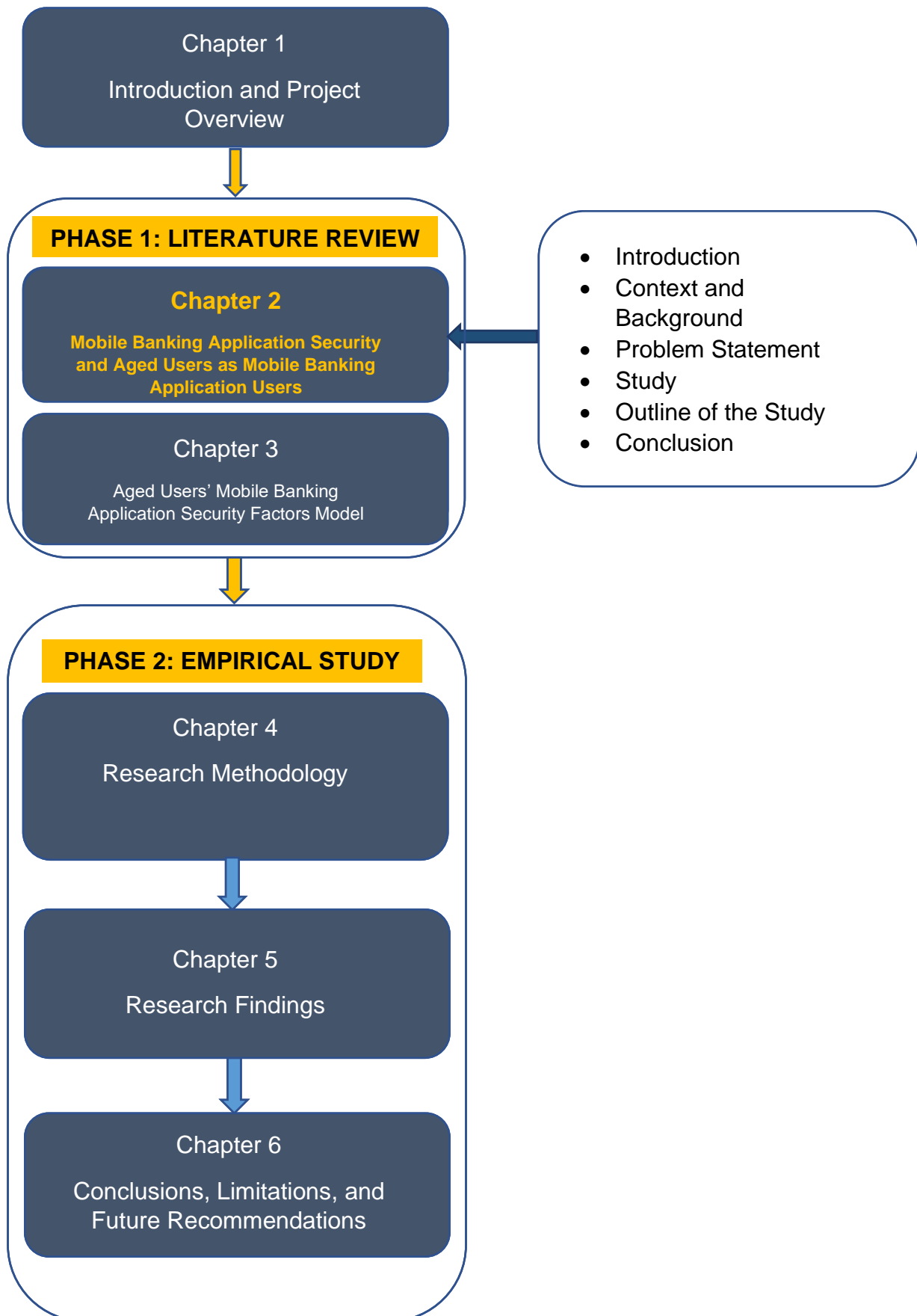
This forms the third and final part of Phase 2 of the research, the empirical study.

1.9 Conclusion

The background and motivation to this research is discussed in Chapter 1. In addition, the problem statement, research objectives and research questions are discussed. The research process overview is detailed through a high-level overview of the research paradigm for the research design and methodology, ending with the outline and chapter summary of the dissertation.

Chapter 2 provides an overview of the concepts of the study, primarily user perception, security, mobile banking applications, and aged users in South Africa.

CHAPTER 2



MOBILE BANKING APPLICATION SECURITY AND AGED USERS AS MOBILE BANKING APPLICATION USERS

2.1 Introduction

Chapter 2 provides an overview of the concepts of the study, primarily user perception, security, mobile banking applications, and aged users in South Africa. It constitutes the beginning of the literature review for the study.

The overview of the concepts provided in this chapter will form the basis of the literature review to address the first research objective: To analyse the literature for factors that have a significant influence on aged users' perception of security of use of mobile banking applications.

2.2 User perception

According to Mesquita (2012), the success or failure of technology applications and whether the benefit of the applications is being realized can mostly be found by investigating users' perceptions (Mesquita, 2012). This study therefore includes an investigation of the factors that have a significant influence on aged users' perception of security of the use of mobile banking applications, to better design mobile banking applications that are secure and easy to use by this user group.

2.2.1 Definition of perception

Zhuang et al. (2016) define user perception as being associated with measures of the perceived usability of a product or service. These measures include the ease with which an application can be used, the perception of time when using the application, and the usefulness of the results once the application has been used. All of these are measured once a user has interacted with the application and would also require that the user answers some questions.

Understanding a user's perception of an application is key to obtaining detail pertaining to aspects of the application that meet or do not meet the user's expectations or that are a concern for the user (Nguyen et al., 2021).

Emotions, stimuli, and opinions all impact perception (Peruma, Palmerino, & Krutz, 2018). Therefore, perception is in play from the moment an aged user learns about

the existence of mobile banking applications and their function, uses the mobile banking application, and evaluates how the aged user feels about the mobile banking application (Zhuang et al., 2016).

O'Brien & Toms (2009) discuss the User Engagement Scale, which is a multi-dimensional measure that is used to calculate the six aspects of user experience, as per Table 2 – 1.

Table 2 – 1: The User Engagement Scale with the six user perception aspects (O'Brien & Toms, 2009)

Aspect	Description
Aesthetic appeal	This relates to the perception of the appeal of the visual appearance of an interface to an application.
Novelty	This relates to the curiosity that is evoked by the content of an application.
Focused attention	This relates to how mentally concentrated an activity is for the user, as well as the flow and absorption.
Felt involvement	This relates to the sense and feeling of being enticed and entertained while interacting with an application.
Perceived usability	This relates to the cognitive way in which a user responds to an interface on an application or to the content of the application.
Endurability	This relates to the comprehensive or overall assessment of the experience, as well as the future intentions once the application has been used.

User engagement is a measure of the standard of a user's interaction with a digital system, such as a mobile banking application, which is characterized by the depth of the user's cognitive, temporal, active, and behavioural investment (O'Brien, 2016).

The User Engagement Scale is a tool that is used as a measure of user

engagement; it has been used across several digital domains (O'Brien & Toms, 2009). O'Brien (2016) has researched the numerous settings across which the User Engagement Scale has been used to evaluate engagement, including online news, online videos, social network technologies, video games, consumer applications, and information search applications.

Measuring and understanding user engagement has increasingly become an area of interest within the technology fraternity, resulting in a need to design for user engagement with applications (O'Brien & Cairns, 2016). Therefore, user engagement is dependent on the user context, with each digital environment featuring unique technological features that are linked to users' motivations to achieve a particular end goal (O'Brien, Cairns, & Hall, 2018).

Being able to understand aged users' perception of the security of mobile banking applications will therefore require the ability to understand the user engagement of aged users.

2.3 Mobile banking applications

The transition from a traditional economy to a digital economy has been a global trend, primarily the digital transformation within the banking and financial sector (Elena, Ekaterine, & Gyuzal, 2018). Over the past years, banking technology has evolved and seen rapid growth in innovations and technologies, particularly with respect to customer self-service (Yousafzai & Yani-de-Soriano, 2012). Research has shown that financial institutions highlight the advantages of these self-service innovations and technologies to banking customers to improve overall customer banking experience and satisfaction (Chirani & Ghofrani, 2010) and to minimize the bank's running expenses (Kim, Chun, & Song, 2009). With banks now able to offer services and operations online, geographic barriers are broken, and users can enjoy a personalized and custom banking experience (Aldiabat, Al-Gasaymeh, & Rashid, 2019).

Therefore, mobile banking applications have been emphasized and adopted by banks to provide instantaneous financial services (Chen et al., 2018). According to Esmaeili et al. (2021), Afshan & Sharif (2016), Tiwari et al. (2020), and Al-Jabri & Sohail (2012), some of the advantages of using mobile banking applications include:

- Ease of access from anywhere and at any time;
- Reduced banking costs;
- Eco-friendly, paperless transacting;
- Personalization of the mobile banking application according to the customer's needs and requirements;
- Ability to set up alerts or push notifications for easy and effective communication of payments and changes, as well as any bank's deals and promotions;
- Ability to track bank transaction activities without having to go to a physical bank; and
- Ability to transfer funds, make instant payments (including payment of bills), and conduct day-to-day transactions.

2.3.1 Use and availability

South Africa has a population of approximately 60 million people (Statistics SA, 2022), of which 20 to 22 million own a smartphone (Statista, 2022). This accounts for at least a third of the country's population. However, according to the United Nations Development Programme (2021) and the Human Development Report (2020), South Africa has been recorded globally as having one of the highest levels of inequality, with 18.9% of the population living on less than USD 1.90 per day. A 2021 Finscope survey revealed that the use of mobile banking applications is an issue for low-income households, as most are social grant beneficiaries who have funds deposited into their bank accounts or SASSA accounts (Vally, 2016).

The FSCA Financial Sector Outlook Study (2022) identified that South African banks had improved mobile banking applications, particularly post the Covid-19 pandemic, to reduce the dependency on physical bank branches. This saw an increase in the number of users who made use of mobile banking applications. In turn, this resulted in competitive benefits for banks as it offered the opportunity to present different ways of conducting banking transactions (Barati & Mohammadi, 2009).

Table 2 – 2 lists South Africa's current locally controlled banks and their mobile banking application status, according to BASA (2021), the Reserve Bank of South Africa (2022), and the FSCA Financial Sector Outlook Study (2022).

Table 2 – 2: Locally controlled South African banks and mobile banking application status

Bank Name	Digital Bank (No physical premises)	Mobile Banking Application
ABSA Group Limited	No	Yes
African Bank Limited	No	Yes
Bidvest Bank Limited	No	Yes
Capitec Bank Limited	No	Yes
Discovery Limited	Yes	Yes
FNB	No	Yes
Grindrod Bank Limited	No	No
Investec Bank Limited	No	Yes
Ithala	No	No
Mercantile Bank Limited	No	Yes
Nedbank Limited	No	Yes
Sasfin Bank Limited	No	Yes
Standard Bank of South Africa	No	Yes
Tyme Bank	Yes	Yes
Ubank Limited	No	Yes

Of South Africa's 15 locally controlled banks, 13 provide mobile banking applications, constituting approximately 87% coverage. This is supported by Chigada & Hirschfelder (2017), who identify that mobile banking applications in South Africa present a new era within the financial services industry, especially with the increased number of users owning mobile phones.

The use and availability of mobile banking applications in South Africa have become an essential interface between South African banks and the general population, which includes lower-income and aged users (Ramnath, 2018).

2.3.2 Design concepts and guidelines

Design guidelines exist for a framework that is practical and ethical for decision-making, that enhances appropriateness of practice, and that provides a sense of accountability and responsibility for mobile banking application designers and

developers (Shitkova et al., 2015). This framework would be similar to those that exist in the USA, provided through the Federal Financial Institutions Examination Council (FFIEC) and the National Institute of Standards and Technology (NIST) (Carter & Zheng, 2015), to guide the design of mobile banking applications and to increase security (Carter & Zheng, 2015), for example by employing multi-factor authentication.

There are existing guidelines for developers when designing secure mobile banking applications (Poston, 2021), such as the Open Web Application Security Project (OWASP) Mobile Application Security Verification Standard (OWASP, 2022). However, OWASP only has chapters in select cities in African countries as of 2022, and South Africa does not form part of that list.

No set industry standards or frameworks for South Africa to guide the build and design of mobile banking applications could be found at the time of this study.

However, application legislation exists for all mobile banking applications, as per Table 2 – 3 (Veitch, 2016).

Table 2 – 3: South Africa legislature for mobile banking applications

Name	Abbreviation	Description
<p><i>Consumer Protection Act 68 of 2008</i> (Consumer Protection Act, 2014)</p>	<p>CPA</p>	<ul style="list-style-type: none"> • Provides strict requirements for the wording and content that is included in the mobile banking application. Plain and understandable language must be used, and non-misleading descriptions of services are to be provided. • The mobile banking application must have complete and comprehensive terms and conditions of use to protect the user as well as the bank, and these should comply with the CPA.

Name	Abbreviation	Description
<i>Electronic Communicates and Transactions Act 25 of 2002 (Electronic Communications and Transactions Act, 2010)</i>	ECTA	<ul style="list-style-type: none"> • Facilities and regulates all electronic communications and transactions. • The mobile banking application should allow a user to review a transaction before committing or submitting it. In addition, depending on the transaction type, there should be an option to cancel or submit an instruction for a transaction previously submitted. • Mobile banking applications should also be sufficiently secure, as per the accepted and regulated technological standards.
<i>Copyright Act 98 of 1978 (Copyright Act 98 of 1978, 2015)</i>	N/A	<ul style="list-style-type: none"> • Regulates that the developer of the mobile banking application ensures ownership of their Intellectual Property.
<i>Protection of Personal Information Act 4 of 2013 (POPIA, 2021)</i>	POPIA	<ul style="list-style-type: none"> • Regulates that any personal information that is used for the mobile banking application is limited to that which is necessary for its specific purpose. • Ensures the integrity and confidentiality of the personal information obtained through the mobile banking application.

From Table 2 – 3, four key acts can be found in the mobile banking application legislature within South Africa. Based on the descriptions of each act, these are broad in scope, and there is no act specifically for security.

Veitch (2016) continues to state that several laws apply to mobile banking applications; Table 2 – 3 contains the key acts that developers should consider for mobile banking application development.

The literature that has been reviewed identifies design concepts and guidelines for the aged that can be included when building mobile banking applications to ensure that they offer a secure and easy-to-use experience. This includes:

- Use of better lighting based on age (Rogers, Gilbert, & Cabrera, 1997);
- Implementing auditory functions (Lee, Poliakoff, & Spence, 2009);
- Catering for socio-cultural factors (Law & Abrahão, 2014);
- Unofficial proxy support for reduced security and data privacy risks (Latulipe et al., 2022);
- Automatic sign-out after inactivity (Ubam et al., 2021); and
- A single-step approval process (Iqbal et al., 2020).

However, the research has been limited in scope and application; further, relevant studies have not been conducted in South Africa, thus identifying a research gap.

2.3.3 Security by design

Mobile banking applications process sensitive data and therefore need to function in a secure environment (Osho et al., 2019). Security is one of the fundamental issues that impact mobile banking applications (Chanajitt, Viriyasitavat, & Choo, 2016), as the information contained in such applications includes users' transaction data, Personal Identifiable Information (PII), and banking credentials.

Balcerzak et al. (2017) discuss user-centred design when considering the design of banking technology for aged users. This is a design that focuses on users and their needs at each phase of the development process, meaning that the security concerns of aged users are considered as part of the design. In addition, participatory design puts the aged user at the centre of the design process. This study included the design of a platform that was to be used by aged users to choose a volunteer to assist them with a focus on security, due to their declining cognitive

and physical abilities (Wilson et al., 2002). The inclusion of aged users as part of end-user testing was found to improve the design and use of the application, and proved to be an effective tool in solution design when improving digital application security for aged users.

Følstad (2017) discusses how design feedback can provide insight into the daily problems that are faced by users. The conclusions from such feedback may affect later steps in the creation of mobile banking applications, particularly with respect to the security of mobile banking applications by aged users.

In work done by Jin et al. (2021), banking practice challenges were identified for user experience of mobile banking applications. Mobile banking applications were not made with older users in mind; aged users face legibility issues because of font size. This is inevitable with ageing, as aged users often have visual impairments (Wilson et al., 2002), which makes it challenging to navigate the screens in mobile applications. This already leads to a loss of trust and of a sense of security (Asp et al., 2012) in using the application, which can only be built and regained with regular use of the mobile banking application by aged users. The latter are therefore forced to request assistance from other family members, friends, neighbours, and volunteers (any available caregivers) to use these applications, which opens them up to risk, as this means exposing secure personal and financial details (OECD, 2020).

The present study found that using non-glare glass and better lighting (Rogers et al., 1997) and implementing auditory functions in mobile application design (Lee, Poliakoff, & Spence, 2009) would benefit aged users and empower them to request official bank assistance when in need, without compromising their security.

To create and provide an optimal user experience that is not just specific to aged users, but that is inclusive of all users, Law & Abrahão (2014) discuss the principles that must be applied in application design. This includes catering for cognitive factors, aesthetics, socio-cultural factors, and any additional factors that can impact the interaction of a user and that should therefore be included in the design. Their study also discusses the potential barriers that can be faced.

Sarcar et al. (2017) discuss how aged users' mobile interface design is influenced by perception, memory, human factors, and motor movement, which in turn impact the use of the application by the aged user. They also discuss a need for set design

principles to start segmenting the design of interfaces for aged users and better cater to their needs (Sarcar et al., 2016).

According to Chen et al. (2018), He et al. (2015), Constantin (2014), and White (2013), there are security requirements that must be included in all mobile banking applications to ensure security compliance; these are briefly discussed in the sections that follow.

2.3.3.1 No default passwords

This is Requirement 2.19 of the OWASP (2022) ASVS 3.0.1 “Authentication Verification Requirements” section. This requirement states that there should not be any default passwords used in an application, that is, a preconfigured password.

This is a key requirement, as aged users can have challenges with memorizing passwords (Sarcar et al., 2017) and a default password can be easier to use, which would compromise the security of the mobile banking application for the aged user.

2.3.3.2 Biometric login

Biometric login is a security measure for authorizing access to the mobile banking application through a verification process that confirms the unique biological characteristics of a user (Bhattacharyya et al., 2009). Many mobile device makers are now incorporating biometric safety features in the build of mobile devices; therefore, when developers build applications such as for mobile banking, they can leverage these features to create prevalent security measures (Yildirim and Varol, 2015).

Two main techniques can be used for biometric logic, namely (Bhattacharyya et al., 2009):

- Fingerprint technology; and
- Facial recognition technology.

According to Wilson et al. (2002), aged users can be prone to the loss of cognitive and physical abilities, which can impact the ongoing use of mobile banking applications. The use of biometric authentication eases the dependency of mobile banking applications on aged users’ cognitive and physical abilities for the authentication process, for which the challenged aged users in turn revert to third parties for assistance (Latulipe et al., 2022).

2.3.3.3 Multi-factor authentication

Multi-factor authentication (MFA) is a secure form of authentication that requires the application of more than a single authentication technique from various independent credential categories (Dasgupta, Roy, & Nag, 2017). Therefore, multi-factor authentication is a combination of two or more types of authentication that is used to securely authenticate users. Once implemented on mobile banking applications, the risks associated with malicious intent by users trying to access the aged user's bank account are reduced (Amin, UI Haq and Nazir, 2017).

2.3.3.4 Push notifications

According to IBM (2021), a push notification is a short and brief message that appears in the form of a pop-up on a user's device from a mobile application. Push notifications are opt-in alerts that enable a user to take an action; for a mobile banking application this can include (Rogozhkina, 2022):

- Real-time notification of transactions;
- Real-time notification of non-mobile banking application logins; and
- Security-based one-time PIN verification for transactions.

This allows for immediate fraudulent activity awareness for aged users, and acts as a security mechanism.

2.3.3.5 Automatic logout

According to the PCI Security Standards Council (2019), any application that allows access to credit cards offered by banks should not be active for more than 15 minutes. Therefore, a mobile banking application session should be deactivated, and the user must authenticate again (Ubam et al., 2021).

With the propensity towards a decline in cognitive ability of aged users, including memory loss (Wilson et al., 2002), there is a possibility of them forgetting to log out of the mobile banking application; this security risk can be taken advantage of by anyone with access to the aged user's mobile device. The automatic logout functionality ensures that, even if the aged user does not log out of the mobile banking application, the session is deactivated, thus protecting the aged user's accounts and data.

2.3.3.6 Older mobile banking application version blacklisting

If a mobile banking application's version is old, a notification should be sent to the user to update it from the official application source, such as the bank's website, and the user should not be allowed to use the old application (Chen et al., 2018). Older versions of mobile banking applications normally have vulnerabilities, security bugs, or unresolved issues that can put the aged user's interaction at risk, as a user becomes more prone to attackers (Chen et al., 2020).

2.3.3.7 Sensitive data encryption

Encryption is a process that allows for the encoding of data such that only the intended recipient or authorized users can access the data (IBM, 2022). Sensitive bank user details that would normally be in plain text, such as a user's bank card number, transactional data, and bank account details (Sangeetha & Sumathi, 2018), are encrypted using an algorithm to generate ciphertext, which can only be read if decrypted.

Therefore, encryption facilitates confidentiality of sensitive data by preventing unauthorized users from accessing it. Mobile banking applications should only transmit data that is encrypted.

2.3.3.8 Secure transfer protocols

A secure transfer protocol is a network protocol that can be used for securely managing files and sensitive data, including accessing and transferring files and data (Rescorla & Schiffman, 1999). This ensures that all connections and communication that are made using the mobile banking application are secure (Chen et al., 2018). The secure transfer protocols assist financial organizations in ensuring that data and file transfer regulations, such as the *Electronic Communicates and Transactions Act 25 of 2002* (ECTA) in South Africa, are met as customer data, funds, and any other sensitive data can be securely transferred (Veitch, 2016).

2.3.3.9 Security logging

Security logging includes storing all the security events for the mobile banking application on the user's device while the user session is active (He et al., 2015). This includes activities such as user authentication.

Once the aged user terminates the active session by logging out of the mobile banking application, or the session times out due to inactivity, the security events are sent to the server for any required further checks and analysis (Panja et al., 2013).

2.3.3.10 Rooted or jailbreak device check

If a device is rooted or has a jailbreak, it means that the software restrictions that were built in by the device manufacturer have been removed, giving the device user system administrator privileges to install and run software other than what the device manufacturer would have made available for the specific device (Raut, Prabhu, & Agrawal, 2021). This introduces risk as such software is not verified, therefore jailbroken and rooted devices have a higher risk of malware (Harris, Patten, and Regan, 2013).

If a mobile banking application is to be installed on such a device, then the aged user's data is at risk; therefore, checks are necessary to ensure that the device is not jailbroken or rooted before installation of a mobile banking application can proceed, thereby protecting aged users' data.

2.4 Aged users in South Africa

According to the *Older Persons Act 13* (2006), an aged person is defined as a person who is 65 years of age and older in the case of males and 60 years and older in the case of females. The ageing population in South Africa forms part of a bigger global increase in age (WHO, 2020) due to lower fertility rates and increased longevity (United Nations, 2015). This trend is manifested approximately three times faster in middle- and low-income countries compared to more developed countries (Chatterji et al., 2015). The growth rate among the aged has risen by 3% over the 2019 to 2020 period, compared to the 1.1% growth over the 2002 to 2003 period (Statistics South Africa, 2020). The WHO World Report on Ageing and Health (WHO, 2015) projects that the number of the aged in South Africa will increase to 15.4% of the total population by 2050. In South Africa, this lower-income demographic is dependent on retirement funding, family support, and government grants (Ralston et al., 2015).

There has not been much research done on the aged who utilize technology, with most studies focusing on other areas of study (Vaportzis, Giatsi, Clausen, and Gow,

2017). Aged users have more discretionary income and larger amounts of available time compared to younger users (Norman, 2019), which makes them a compelling demographic for research.

2.4.1 Aged users as mobile banking application users

Although there exist several empirical studies on the high level of the adoption of mobile banking applications by users, there are not many studies that assess the use of mobile banking applications amongst aged users, nor the perceptions of aged users on factors impacting the adoption of mobile banking applications, including their views on security. A study by Assensoh-Kodua et al. (2016) found that research that has been conducted on mobile banking in South Africa has prioritised issues of greater concern, as such neglecting the issues of assessing mobile banking needs and the measurement of impact. They discovered that most of the research has been conducted using academic models and practitioner participation.

While the use of mobile devices and the uptake of mobile banking applications have both increased globally (Ramnath, 2018), there is still limited information as to what factors influence the use of mobile banking applications by aged users in South Africa, particularly with respect to security. Some of the studies that have been done in South Africa have been broad in scope, not restricted by age, and were conducted by researchers such as Assensoh-Kodua et al. (2016), Msweli (2020), Ramnath (2018), Chigori et al. (2020), Koenaithe et al. (2019), Garg et al. (2014), Chigada & Hirschfelder (2017), Slazus & Bick (2022), and Koenaithe et al. (2021).

Of these researchers, only Msweli (2020) focused on aged users. According to Msweli (2020), the use of mobile banking applications by the aged is lower compared to the other age groups.

Msweli & Mawela’s (2021) research identified barriers that affect South Africa’s aged users’ adoption of mobile banking. They also identified barriers to, enablers of, the adoption of mobile banking, as shown in Table 2 – 4.

Table 2 – 4: Barriers and enablers of adoption of mobile banking applications by aged users in South Africa (Msweli & Mawela, 2021)

Enablers	Barriers
Convenience	Security

Enablers	Barriers
Unlimited access	Trust
Cost-effectiveness	Age
	Language
	Cognitive factors
	Lack of information
	Lack of understanding
	Complexity of mobile banking applications
	Resistance to change

2.4.2 Aged users as a growing banking customer segment

Societal changes have resulted in the aged becoming responsible for their expenses and needs, and not just dependent on their children for financial support (Pieterse, 2008). Aged users receive social grants or pensions that can be deposited into their bank accounts, or through individual retirement investments of various forms (Ralston et al., 2015). This means that several of the aged remain economically active and can manage their banking affairs. Through this, aged users are a target demographic for several businesses (Mattila, Karjaluoto, & Pento, 2003).

Based on the reported growth rate for the aged from Statistics South Africa (2020), the uptake of pensions in South Africa increased in parallel with the increase in numbers of the aged, therefore making this a growing demographic for banks and various businesses.

The South African government has also put measures in place, such as the amended *Pension Funds Act* of 1997, that has made it mandatory for all working people to contribute to provident and pension funds to ensure that they have active sources of income at retirement. This policy naturally increases the number of aged people who can remain economically active and contributes to the banks' active customer base.

2.4.3 Mobile banking application security for the aged

The banking industry continues to grow and integrate digital technologies as part of its development. This has meant that banking businesses have been moving online and becoming digital at an increasing rate (Barrett et al., 2015). However, the

financial services and products are designed for all users and are not designed to specifically cater to the aged; therefore, this demographic already faces a challenge in keeping up with the rate at which banking technology evolves (Jin et al., 2021).

Across the globe, aged users are starting to make use of digital platforms due to the longer waiting times at physical banks, even if the adoption rates are not as high as those of younger users (Jin et al., 2021). The main concerns in using mobile banking applications that have been raised include the overall security of these banking digital platforms (Jin et al., 2021).

In a study by Ubam et al. (2021), three security issues were identified, highlighting the importance of security in e-banking; these related to secure verification, secure transaction authorization codes, and automatic sign-out after inactivity. Financial institutions have strict measures in place for users to verify and identify, according to the Financial Intelligence Centre Act, 2001; this verification can be in the form of knowledge or possession. With the decline in cognitive abilities of aged users, it can be easy to forget verification information (Wilson et al., 2002); therefore, having this as an uncomplicated process can contribute to the facilitation of a secure and easy transaction. Modification of the design of mobile banking applications to implement secure verification that uses a single-step approval process proved that aged users prefer a fast and easy verification method (Iqbal et al., 2020). Nicholson et al. (2013) found that aged users can sometimes struggle with novel authentication systems.

Financial fraud is the most common type of financial crime committed against the aged globally (OECD, 2020). This has continued to increase over time, and reports include caregivers committing these crimes against the aged. Caregivers can include family, friends, neighbours, or paid and unpaid volunteers (OECD, 2020).

DeLiema (2017) analysed financial exploitation of the aged and found that this was more prevalent where the aged user had no friends or family and, therefore, where aged users were socially isolated. The study also proceeds to suggest the prevention of social isolation as a means of lowering the levels of exploitation. However, trust in using a mobile banking application is lost as security is compromised for the aged user, and therefore the likelihood of using the mobile banking application is drastically reduced.

2.5 Conclusion

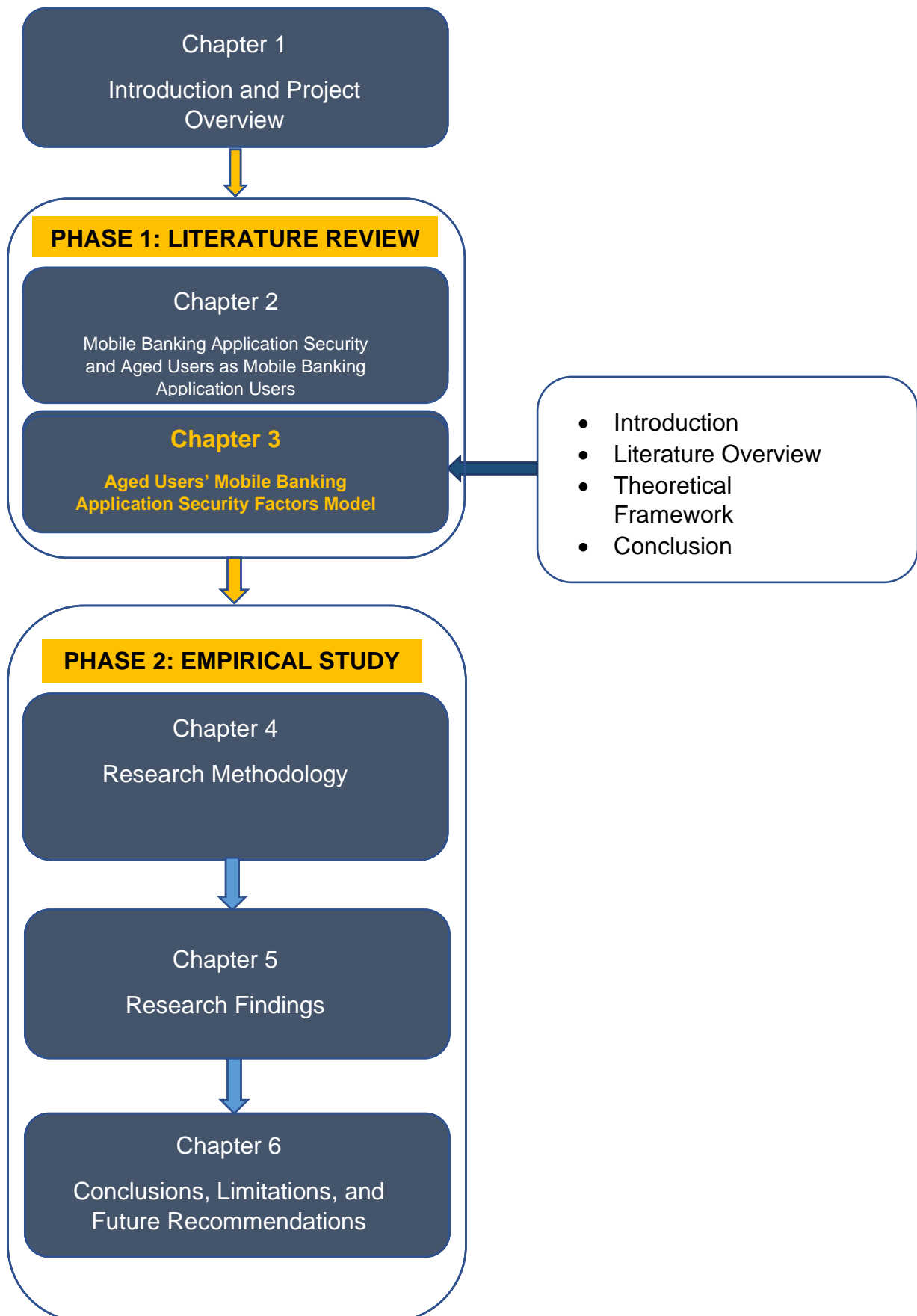
An overview of the concepts of mobile banking applications and their associated security, including the existing design guidelines, were discussed in Chapter 2.

Chapter 3 provides an overview of the literature that relates to known aged user perceptions on the security of mobile banking applications, as well as to existing factors on the security of mobile banking applications for the aged, while highlighting the gaps in the current research conducted in South Africa.

The hypotheses for the study are postulated, and a hypothesized conceptual model is proposed.

This conceptual model is proposed based on the known literature, and forms the basis for the development of the study's questionnaire.

CHAPTER 3



AGED USERS' MOBILE BANKING APPLICATION SECURITY FACTORS CONCEPTUAL MODEL

3.1 Introduction

Chapter 3 provides an overview of the review of existing literature, including the literature search and analysis findings for known aged user perceptions of the security of mobile banking applications, as well as existing security factors pertaining to mobile banking applications for the aged. The chapter begins with a review of existing literature on the security factors for aged users in using mobile banking applications, which are categorized and grouped to form constructs that will be used in the hypothesized model. Moderators for the study are also identified from the existing literature.

The theories of acceptance of technology are briefly discussed, including UTAUT2, which is used to inform this study. The hypotheses are postulated, and the questions that will be included in the questionnaire are formulated per hypothesis. The hypothesized model is then proposed, using the constructs from the literature.

This chapter will address the following research objectives:

- To analyse literature for factors that influence aged users' perception of the security of mobile banking applications;
- To develop the Aged Users' Mobile Banking Application Security Factors Model of the factors that influence aged users' perception of the security of mobile banking applications; and
- To develop a questionnaire based on the Aged Users' Mobile Banking Application Security Factors Model.

The flow of the process to create the proposed conceptual model is as per Figure 3 – 1.

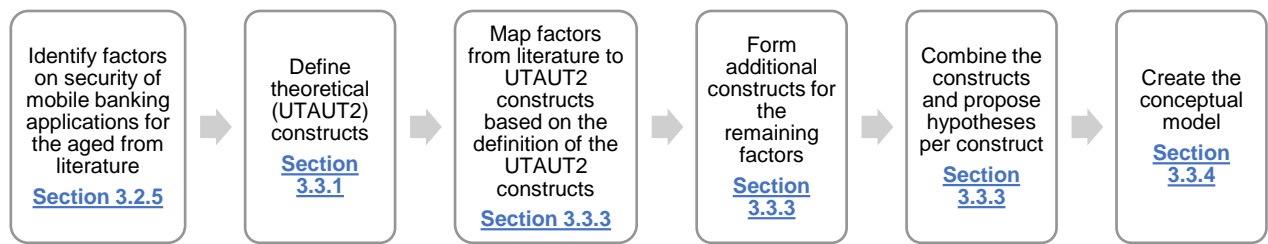


Figure 3 - 1: Workflow process of the creation of the proposed conceptual model

3.2 Literature Overview

This research adopts a scoping literature review approach, which is conducted using the Arksey and O'Malley framework (Arksey & O'Malley, 2005). An initial assessment of the body of work is done through a scoping literature review to determine the most important concepts that are available in a particular field of study (Grant & Booth, 2009). Therefore, the scoping literature review provides an ideal tool to determine the scope of literature for a topic, and to identify the volume of literature, studies, and overviews that are available on the topic (Arksey & O'Malley, 2005). This helps to identify research gaps in the literature (Arksey & O'Malley, 2005).

For this study, the scoping literature review aimed to gain an overview of the factors that have a significant influence on aged users' perception of the security of use of mobile banking applications.

3.2.1 Keywords

Academic research databases or search engines are used when searching for material that applies to the research topic. It is essential to choose the right keywords for this search to ensure comprehensiveness. This helps the researcher to find pertinent information and reduces the amount of irrelevant data found or returned.

The keywords used for the literature search are:

elderly, seniors, older adults, mobile banking, security, design, mobile application design

The following search string was used across the academic research databases or search engines:

“elderly” OR “seniors” OR “older adults” OR “aged”

AND “mobile banking” OR “banking”

AND “on-line security” OR “security”

AND “design” OR “user-centred design” OR “mobile application design”

3.2.2 Inclusion and exclusion criteria

Inclusion and exclusion criteria are applied to choose the articles to include in or exclude from the scoping review. To ensure the objectivity of the process, these requirements were set up before the scoping review.

Table 3 – 1: Literature review inclusion and exclusion criteria

Include	Exclude
Scholarly Articles from 2017 – 2022	Pre-2017 studies
English publications	Non-English publications
Recognized academic search databases, engines, and publishers	Unpublished data, review manuscripts, case reports, commentaries
Articles containing the keywords as per the defined search string	Articles with keywords that do not pass the search string
Research on aged people	Research on non-aged people
Financial and Technology sector	Health sector

3.2.3 Databases

To find articles that fit the study’s search criteria, the following databases were searched:

- IEEE
- ACM Digital Library
- Gale
- EBSCO

- Emerald
- Scopus

3.2.4 Literature search and analysis

The following steps were followed to filter and select the articles for the literature view:

1. The initial search for literature from all the listed academic databases, based on the provided keywords, returned a total of 379 potentially relevant articles.
2. The duplicates were then removed, leaving a total of 241 articles.
3. After reading all the abstracts, only 62 articles remained.
4. A full-text scan was conducted, and the number of articles was further reduced to 15.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology was used in this scoping literature review approach. This is a method that is used to improve the transparency of a literature review through a defined 27-item checklist and a four-phase flow diagram (Tricco et al., 2018).

The four phases, as included by (Tricco et al., 2018), are:

- Identification;
- Screening;
- Eligibility; and
- Included.

The stages are shown in Figure 3 – 2 of the PRISMA flow diagram, from statistics of the literature search, to screening and selection of the articles to be used in the study, to analysis and scanning of those articles.

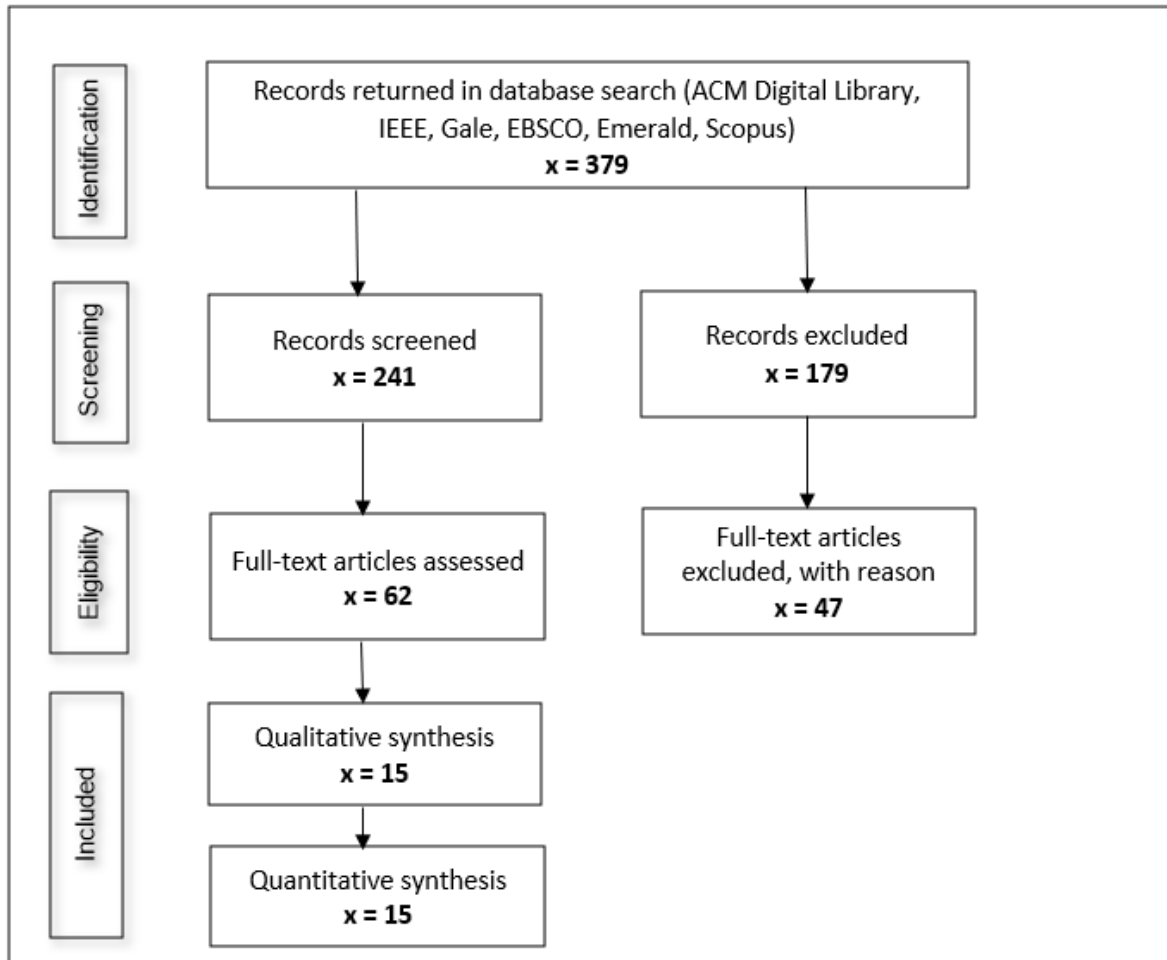


Figure 3 – 2: PRISMA literature search flow diagram

3.2.5 Factors on the security of mobile banking applications for the aged

Table 3 – 2 has a summary of the studies that could be found on mobile banking application usage for the aged, the design, and the security concerns surrounding mobile banking applications. This was compiled using the listed search terms and keywords, and was restricted to the past five years (2017–2022).

The resulting literature was filtered to select the articles that applied to this study.

The table includes:

- Year – The year in which the study was conducted.
- Country – The country in which the study was conducted.
- Country Group – The Country Group under which the research area country falls according to the World Economic Outlook Database (International Monetary Fund, 2022).

- Source – The reference to the study.
- Factors – The identified factors from aged users when using mobile banking applications, to also be considered for use in the Aged Users' Mobile Banking Application Security Factors Model.
- Method – The data collection method for the study.
- Model Created – Identifies whether a model was created in this study.
- Finding – A summary of the findings per study.

Table 3 – 2: Literature findings and summary

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
2017	Ukraine	Developing	Balcerzak et al. (2017)	None	<ul style="list-style-type: none"> • Proxy trust • Proxy authentication • In-application support • Emergency assistance • Technological trust 	Case Study	No	<p>The inclusion of aged users in the design and development phase helps build sufficient security measures and improved usability of applications for the aged; therefore, aged users' feedback and perceptions are critical to effective build processes.</p> <p>In addition, applications for aged users should include security measures that foster the development of trust.</p>
2020	Multiple	Developing	Msweli & Mawela (2020)	None	<ul style="list-style-type: none"> • Emergency assistance • Technological trust • Technology readiness • Adequate use and exposure • Cost of banking 	Survey	No	<p>Aged users have unique requirements, barriers, and enablers that need to be understood so that adequate design guidelines are proposed.</p> <p>A gap was identified in research focusing on the elderly and mobile banking.</p>
2021	Malaysia	Developed	Ubam et al. (2021)	None	<ul style="list-style-type: none"> • Secure verification • Secure authorisation process 	Survey	No	<p>Design for mobile banking applications correlates to aged users' needs – particularly security, loading time, and user interface elements. These all contribute to</p>

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
					<ul style="list-style-type: none"> • Automatic sign-out (with inactivity) • Pleasurable user experience 			an enjoyable experience for the aged user and are dependent on an aged user-friendly interface.
2021	China	Developing	Jin et al. (2021)	None	<ul style="list-style-type: none"> • Perceived privacy loss • Adequate use and exposure 	Survey	No	Age influences mobile banking application use and behaviour. Low familiarity, security, and usability are barriers to the usage of mobile banking applications.
2019	USA	Developed	Mendel & Toch (2019)	Grounded Theory Approach	<ul style="list-style-type: none"> • Perceived privacy loss • Complex security mechanisms • Password management • Proxy trust 	Survey	Yes	Familiarity with aged users' preferences and concerns about mobile security and privacy offers essential design guidance for creating technology that can lower barriers.
2017	Finland Japan UK Canada	Developed	Sarcar et al. (2017)	None	<ul style="list-style-type: none"> • Human factors, perception, memory loss • Motor movement of aged users • Experience 	Case study	No	Aged users' mobile interface design is influenced by perception and memory, which impact the use of the technology by the aged user.

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
2020	Saudi Arabia	Developed	Iqbal et al. (2020)	None	<ul style="list-style-type: none"> • Complex privacy management mechanisms • Complex authentication mechanisms • Perceived privacy loss • Complexity of mobile banking applications • Perceived usefulness • Experience 	Survey	Yes	Improved security in the design of mobile banking applications for the aged provides user satisfaction, ease of use, and a secure experience.
2022	Finland	Developed	Saukkonen, P. et al. (2022)	None	<ul style="list-style-type: none"> • In-application support • Perceived privacy loss • Complexity of mobile banking applications • Proxy trust 	Case study	No	Development of digital services should include the natural decline in functioning for aged users, and support must be easily accessible and secure.

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
2018	Czech Republic	Developed	Klímová et al. (2018)	Theory	<ul style="list-style-type: none"> • Experience • Adequate use and exposure 	Survey	No	<p>Age is a decisive factor in the use of mobile banking applications by aged users.</p> <p>Aged users increasingly use mobile applications for daily activities, and those who receive training on using technology products are more confident, aware, and less prone to security risks compared to those who do not.</p>
2022	USA	Developed	Johnson (2022)	None	<ul style="list-style-type: none"> • Perceived privacy loss • Legibility challenges • Experience • Complexity of mobile banking applications • Motor movement of aged users • Lack of adequate facilitating conditions 	Case study	No	<p>Age is a decisive factor in the use of mobile banking applications by aged users.</p> <p>Application design for aged users should consider aged users' varied capabilities, usage patterns, and preferences.</p>

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
2022	Canada	Developed	Latulipe et al. (2022)	None	<ul style="list-style-type: none"> • Proxy trust • Proxy authentication • Experience • Complex privacy management mechanisms • Perceived privacy loss • Preventative security knowledge gap • Password management • Adequate use and exposure • No social support or influence 	Survey	No	There are increased privacy and security issues that could lead to financial exploitation of aged users when people are assisting them in the use of mobile banking applications. Banking applications' design should cater to these unofficial proxies while minimizing security risks. Social influence also plays a role in aged users' decision to use mobile banking applications.
2021	United Kingdom	Developed	Morrison, Coventry, & Briggs (2021)	None	<ul style="list-style-type: none"> • Preventative security knowledge gap 	Case study	No	Aged users are keen to use technology, with security being a key requirement; however, trying to keep the experience secure generates anxiety and avoidance. Mobile banking application developers and

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
					<ul style="list-style-type: none"> • Complex privacy management mechanisms • Complex authentication mechanisms • Password management • Device security • Adequate use and exposure 			<p>policy makers should ensure that aged users have accessible expertise and available information on how to securely make use of these applications.</p>
2020	Canada	Developed	Rajaobelina et al. (2020)	None	<ul style="list-style-type: none"> • Perceived privacy loss • Experience • Perceived usefulness • Technological trust 	Survey	Yes	<p>Trust has an impact on an aged user's perception of the security of a mobile banking service. Aged users also have different experiential needs when using mobile banking applications, which should be factored into the design.</p>
2021	China	Developing	Cham et al. (2021)	None	<ul style="list-style-type: none"> • Perceived privacy loss • Experience 	Survey	Yes	<p>Aged user perception and attitude provided feedback that was significant in identifying adoption barriers. Security risks</p>

Year	Country	Country Group	Citation	Theory	Factors	Method	Model Created	Finding
					<ul style="list-style-type: none"> • Perceived usefulness • Complexity of mobile banking applications • Preventative security knowledge gap • Adequate use and exposure • No social support or influence 			<p>result in resistance to adopting mobile banking applications.</p> <p>Social influence also plays a role in aged users' decision to use mobile banking applications.</p>
2020	India	Developing	Tiwari et al. (2020)	Innovation Adoption Model	<ul style="list-style-type: none"> • Perceived security compromise 	Survey	Yes	<p>The likelihood of users using mobile banking applications increases if the applications are fully secure, particularly for aged users.</p> <p>There is a dependency between age and mobile banking application use and adoption.</p>

The literature findings from the 15 different studies in developed and developing countries were distilled into 27 distinct factors that influence aged users' perception of the security of mobile banking applications.

Table 3 – 3 summarises the list of factors, with a count of occurrence for each factor.

Table 3 – 3: Summary of literature review of aged users' factors for mobile banking applications and occurrence count

Factor	Occurrence Count	Country Group Occurrence	
		Developing Country Group	Developed Country Group
1. Perceived privacy loss	8	X	X
2. Adequate use and exposure	7	X	X
3. Experience	7	X	X
4. Complexity of mobile banking applications	4	X	X
5. Proxy trust	4	X	X
6. Technological trust	3	X	X
7. Password management	3		X
8. Complex privacy management mechanisms	3		X
9. Perceived usefulness	3	X	X
10. Preventative security knowledge gap	3	X	X
11. Proxy authentication	2	X	X
12. In-application support	2	X	X
13. Emergency assistance	2	X	
14. Motor movement of aged users	2		X
15. Complex authentication mechanisms	2		X

Factor	Occurrence Count	Country Group Occurrence	
		Developing Country Group	Developed Country Group
16. No social support or influence	2	X	X
17. Technology readiness	1	X	
18. Secure verification	1		X
19. Secure authorisation process	1		X
20. Automatic sign-out (with inactivity)	1		X
21. Complex security mechanisms	1		X
22. Human factors, perception, memory loss	1		X
23. Legibility challenges	1		X
24. Device security	1		X
25. Perceived security compromise	1	X	
26. Pleasurable user experience	1		X
27. Cost of banking	1	X	

Table 3 – 3 shows that developing countries identify with 15 out of the 27 factors on the security of mobile banking applications for the aged (56%), while developed countries identify with 23 out of the 27 aged user factors (85%).

According to Msweli & Mawela (2020), there is a gap in the research on aged users and mobile banking applications; therefore, the factors from both the developed and developing countries will be used for this study.

3.2.5.1 Moderators

The literature review identified moderators of aged users' perception of the security of mobile banking applications. An independent variable, known as a moderator,

modifies the nature of the relationship between other study variables (Sun & Zhang, 2006). These characteristics impact aged users' perceptions of the factors that impact the security of mobile banking applications (Sun & Zhang, 2006), according to the studies that have been reviewed. These are detailed in Table 3 – 4.

Table 3 – 4: Moderators of aged users' perceptions of the security of mobile banking applications

Characteristic	Description	Source
Age	The age of the user of the mobile banking application.	<ul style="list-style-type: none"> • Klímová et al. (2018) • Jin et al. (2021)
Education	The level of knowledge that the aged user has acquired through school.	<ul style="list-style-type: none"> • Morrison et al. (2021) • Cham et al. (2021)
Experience	The knowledge or skills acquired by aged users through a period of practical use of the mobile banking application.	<ul style="list-style-type: none"> • Sarcar et al. (2017) • Iqbal et al. (2020) • Klímová et al. (2018)
Cognitive ability	This refers to aged users' mental abilities.	<ul style="list-style-type: none"> • Sarcar et al. (2017) • Morrison et al. (2021)
Proxy	Someone who is given the authority by the aged user to conduct banking transactions on their behalf.	<ul style="list-style-type: none"> • Balcerzak et al. (2017) • Mendel & Toch (2019) • Saukkonen, P. et al. (2022) • Latulipe et al. (2022)

3.3 Theoretical Framework

3.3.1 Theories

A theory is defined as a collection of relationships, overarching assumptions, and presumptions that interpret facts (Ramnath, 2018). This means that a theory can offer a collection of explanatory factors to be used for predicting a particular phenomenon (Samaradiwakara & Gunawardena, 2014).

Theories have been proposed and developed on technology acceptance due to the variety of aspects that influence clients, end users, and businesses' decisions to use or adopt technology. Some of the theories include:

- Technology Acceptance Model (TAM);
- Theory of Reasoned Action (TRA);
- Theory of Planned Behaviour (TPB);
- Unified Theory of Acceptance and Use of Technology (UTAUT); and
- Extended Unified Theory of Acceptance of Technology (UTAUT2).

This study will adopt UTAUT2 to inform the conceptual model.

3.3.1.1 Unified Theory of Acceptance and Use of Technology (UTAUT)

Technology acceptance has increasingly become a field of interest for several researchers, as can be evidenced by the research work done and the technology acceptance models that are available. This has also included the acceptance of mobile banking and of mobile banking applications, as conceptualised by means of the following models:

- Technology Acceptance Model (TAM) (Davis, 1989);
- Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1977);
- Theory of Perceived Risk (TPR) (Featherman & Pavlou, 2003);
- Theory of Planned Behaviour (TPB) (Ajzen, 1991); and
- Diffusion of Innovation Theory (DOI) (Rogers, 1995).

Due to the limitations of these models, Venkatesh et al. (2003) proposed the UTAUT model. The latter was created by consolidating all the previous models or theories, excluding the Theory of Perceived Risk (TPR), into a single model to manage the

limitations of the previous models. The following additional models were included to create the UTAUT model:

- Integrated Model of Technology Acceptance and Planned Behaviour (TAM-TPB) (Taylor & Todd, 1995);
- PC Utilisation Model (MPCU) (Thompson, Higgins, & Howell, 1991);
- Motivational Model (MM) (Davis, Bagozzi, & Warshaw, 1992); and
- Social Cognitive Theory (SCT) (Bandura, 1986).

Four constructs make up the UTAUT model, as illustrated in Figure 3 – 3.

These are Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions.

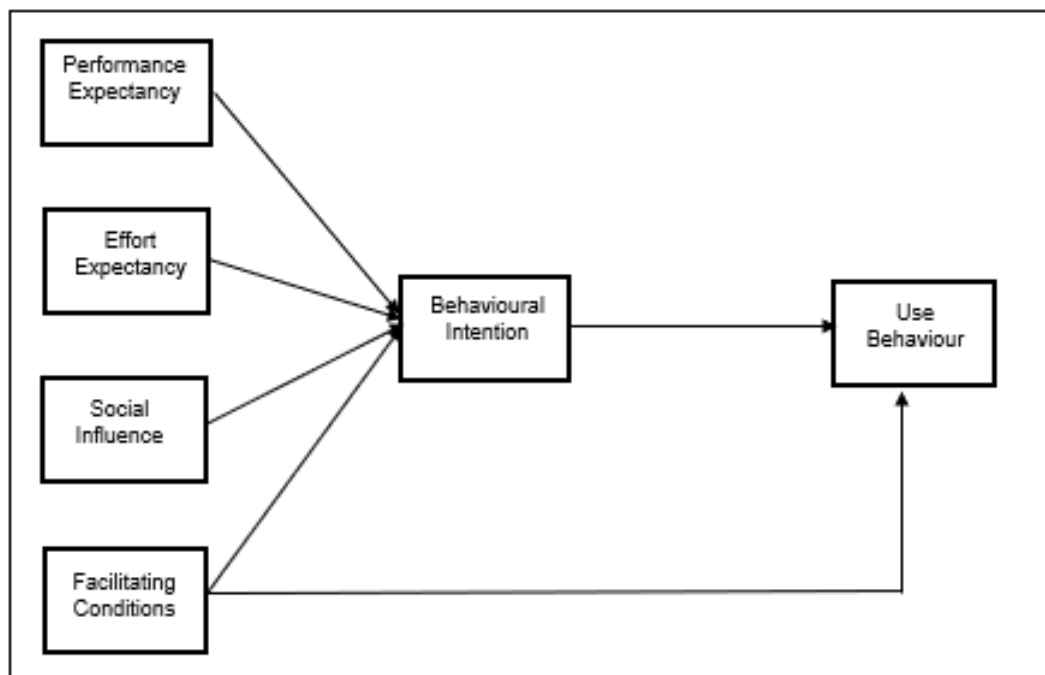


Figure 3 – 3: UTAUT model (Venkatesh et al., 2003)

This model was more accurate in its predictions of acceptance within an organizational setting, and managed to include characteristics such as age, experience, and gender (Venkatesh, Brown, & Bala, 2013). Due to this, the UTAUT model became a preferred model for technology acceptance (Venkatesh and Zhang, 2010) and was applied across several industries, including mobile banking prediction (Afshan & Sharif, 2016; Bhatiasevi, 2016). However, the model's efficacy was limited to organizational settings rather than individual users (Negahban & Chung, 2014),

necessitating its adaptation and modification to be inclusive of all users in all contexts. In addition, the model could not meet some of the prerequisites for measuring the usage and success of technology, such as user satisfaction and technology performance (Montesdioca & Maçada, 2015).

3.3.1.2 Extended Unified Theory of Acceptance of Technology (UTAUT2)

The Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) was proposed and developed by Venkatesh, Thong, & Zu (2012). It was proposed as an extension to the Unified theory of acceptance and use of technology (UTAUT), which had been proposed and developed to predict individual users' and organizations acceptance of technology (Venkatesh et al., 2003).

Three new constructs were introduced by Venkatesh et al. (2012) to manage the flaws of UTAUT in excluding the individual user context, namely, Hedonic Motivation, Price Value, and Habit (Merhi, Hone, & Tarhini, 2019). In addition, Venkatesh et al. (2012) also introduced user characteristics, namely, age, gender, and experience, as moderators of the effects between the independent constructs. This resulted in the Extended Unified Theory of Acceptance of Technology (UTAUT2).

Seven independent variables (constructs) constitute the UTAUT2 model, namely, Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Hedonic Motivation, Price Value, and Habit, and two dependent variables, namely, Behavioural Intention and Use Behaviour (see Figure 3 – 4).

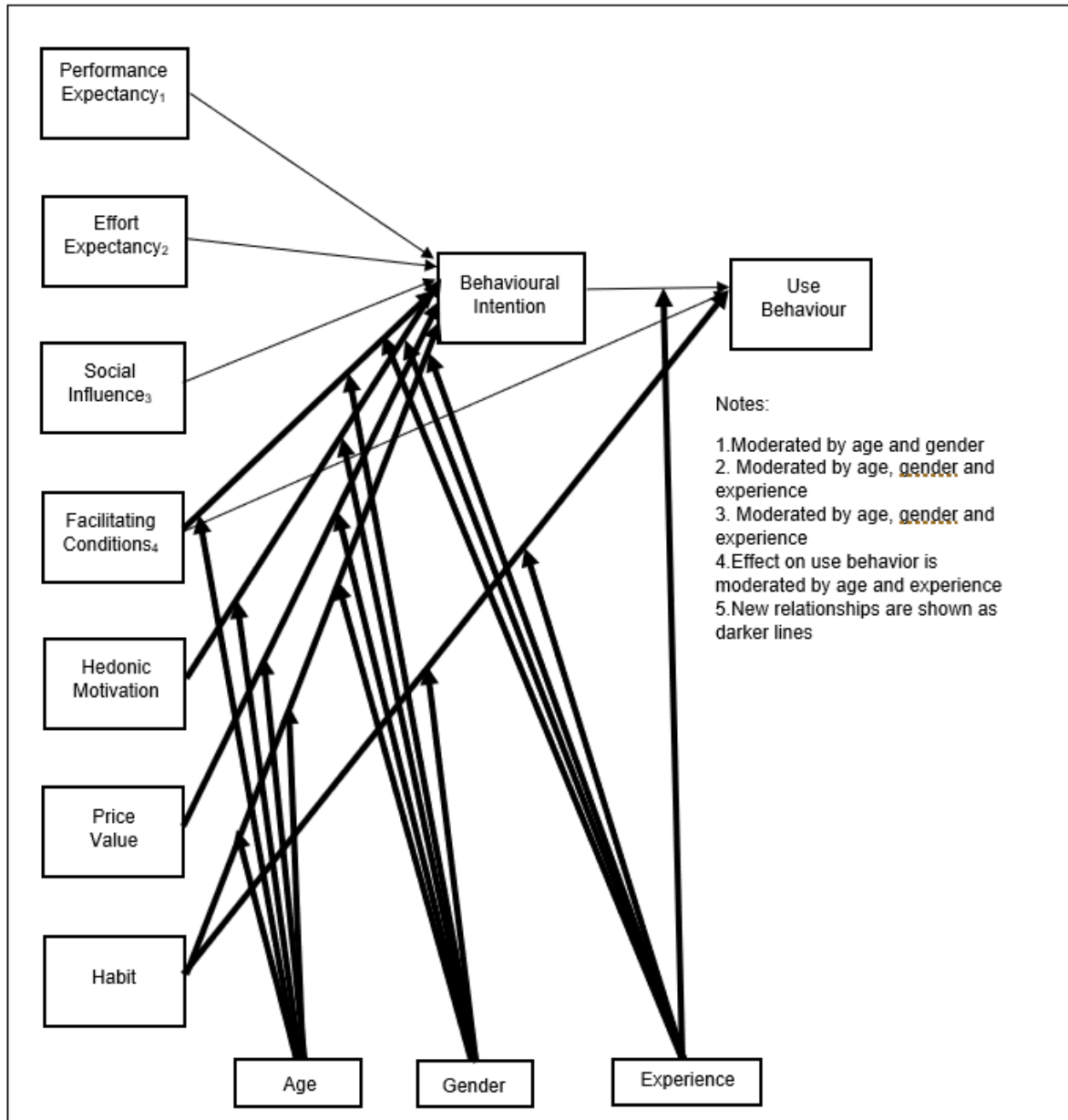


Figure 3 – 4: UTAUT2 model (Venkatesh et al., 2012)

The current constructs for UTAUT2, as outlined in Figure 3 – 4, are defined in Table 3 – 5.

Table 3 – 5: UTAUT2 constructs

Construct	Variable type	Description	Source
Performance Expectancy	Independent	The degree to which the use of technological innovation can	Venkatesh et al. (2003)

Construct	Variable type	Description	Source
		benefit a user while conducting certain activities.	
Effort Expectancy	Independent	The degree to which a user finds a technological innovation easy to use or that it requires minimal effort.	Venkatesh et al. (2003)
Social Influence	Independent	The degree to which a user believes that they should use a technological innovation based on the feedback and input of their social network.	Venkatesh et al. (2003)
Facilitating Conditions	Independent	The degree to which a user perceives there to be sufficient support and resources to adopt and use a technological innovation.	Venkatesh et al. (2003)
Hedonic Motivation	Independent	The degree of pleasure obtained from using a technological innovation.	Venkatesh et al. (2012)
Price Value	Independent	The degree to which a technological innovation's cost measures against the benefit of using the technological innovation.	Venkatesh et al. (2012)
Habit	Independent	The degree to which users automatically adopt certain behaviours when using a technological innovation because of learning.	Venkatesh et al. (2012)
Behavioural Intention	Dependent	A user's readiness or motivation to perform a certain behaviour.	Venkatesh et al. (2003)

Construct	Variable type	Description	Source
Use Behaviour	Dependent	A user's behaviour of use is measured by the actual frequency of a particular technology use.	Venkatesh et al. (2003)

UTAUT2 allowed for the analysis of individual users' technology usage within a voluntary setting, and managed to better differentiate between intended and actual technology use (Venkatesh et al., 2012). Numerous industries, including mobile banking, have made extensive use of, and validated, UTAUT2 (Alalwan, Dwivedi, & Rana, 2017; Merhi et al., 2019; Aldiabat et al., 2019).

While UTAUT2 has been validated in research across several industries, a few gaps remain in terms of constructs within the banking industry, particularly regarding security. As a result, Wechuli, Franklin, & Jotham (2017) have suggested that UTAUT2 lacks concepts essential to the use of technology, particularly in banking where security is essential.

This study will not extend UTAUT2, but will use it to inform the Aged Users' Mobile Banking Application Security Factors Model. In addition, the available literature does not demonstrate that UTAUT2 has been studied for factors that influence the perception of security of mobile banking applications, nor does the literature demonstrate a relationship between the UTAUT2 model and the factors that influence the perception of the security of mobile banking applications. Studies by Merhi et al. (2019), Pratama & Renny (2022) and Soodan & Rana (2020) modified and extended UTAUT2 with security as an additional independent variable, so as to develop insight into the adoption of mobile banking technology and to address the shortcomings of UTAUT2. However, none of the studies investigated the factors that influence the security variable and, subsequently, the direct influence of the perception of security (without other independent variables) on the intention to use and actual use of mobile banking applications. In addition, several studies in the literature were also found to not employ the moderating variables of UTAUT2 in the analysis of mobile banking technology adoption (Gupta, Manrai, & Goel, 2019; Lin, Lin, & Ding, 2020; Mohd Thas Thaker et al., 2021). Therefore, the study will focus

only on the identification of the factors that influence the perception of security on use behaviour.

The Aged Users' Mobile Banking Application Security Factors Model will therefore only be informed by UTAUT2, and will not constitute an extension of UTAUT2.

3.3.2 Constructs

Since this study was informed by UTAUT2, the names of its seven constructs were adopted for the proposed model. The variables and questions for each construct were revised, and the definitions were updated in the context of this study to refer to mobile banking applications and aged users. The 27 factors derived from literature (see Table 3 – 2) were mapped across the revised constructs, based on their definition and the logic of the factor relative to the construct. Based on the definitions of the constructs, some of the factors could not be mapped to the seven constructs.

The following factors could not be mapped to the seven constructs: perceived privacy loss, technological trust, proxy trust, proxy authentication, password management, secure verification, secure authorization process, automatic sign-out (with inactivity), device security and perceived security compromise. Therefore, four new additional constructs were developed and defined, based on the context of the factors, namely:

- Perceived Privacy (perceived privacy loss);
- Technological Trust (technological trust);
- Perceived Risk (proxy trust, proxy authentication);
- Perceived Security (password management, secure verification, secure authorization process, automatic sign-out (with inactivity), device security and perceived security compromise).

The process that was followed is outlined in Figure 3 – 5.

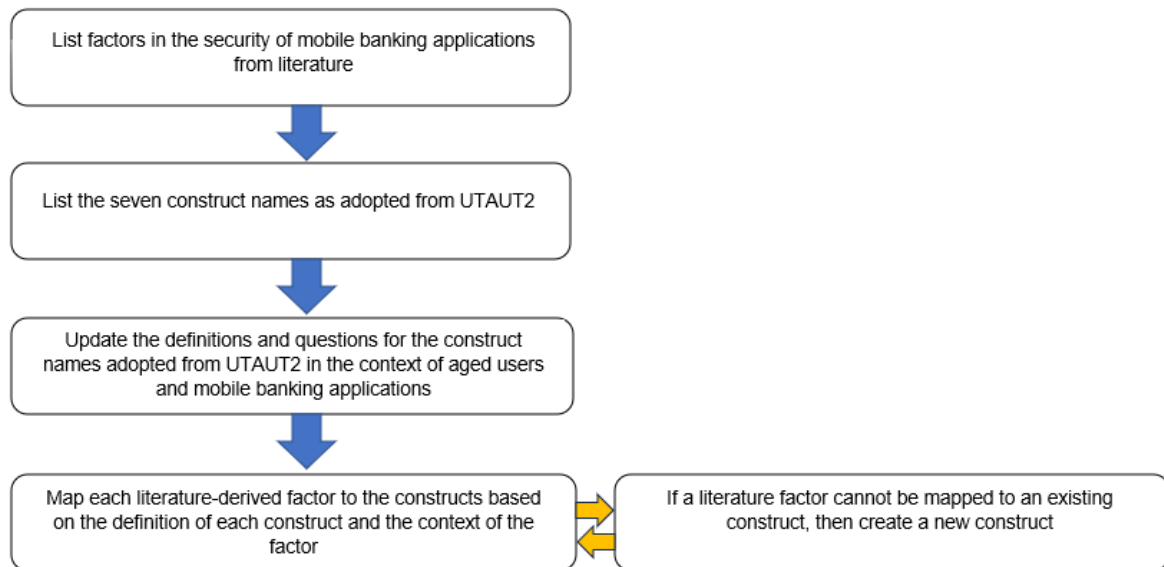


Figure 3 - 5: The constructs derivation process

In the next section, hypotheses are postulated for each construct.

3.3.3 Hypotheses

The section discusses the adopted constructs (independent variables) from UTAUT2 in the order in which they are presented in Figure 3 – 4, followed by the additional constructs as derived from the literature (independent and dependent variables). This is concluded by the adopted constructs (dependent variables) from UTAUT2 (see Table 3 – 5 for definitions of the adopted constructs (both independent and dependent) of UTAUT2).

Adopted UTAUT2 constructs as per Figure 3 – 4:

i. Independent variables

- Performance Expectancy
- Effort Expectancy
- Social Influence
- Facilitating Conditions
- Hedonic Motivation
- Price Value
- Habit

ii. Dependent variables

- Behavioural Intention
- Use Behaviour

For each of the seven independent and the 2 dependent constructs adopted from UTAUT2, the questions are revised and the definitions are updated in the context of this study to refer to mobile banking applications and aged users. For the additional constructs derived from literature, questions are proposed from the reviewed literature and from the factors from which the constructs are derived.

The following hypotheses have been developed, based on the literature review, to help address the main research question of this study. In addition, the questions to be included in the questionnaire are proposed.

3.3.3.1 Performance Expectancy (PE)

Informed by UTAUT2, this construct is defined as the degree to which mobile banking applications are perceived to be of good use by aged users (Venkatesh et al., 2003). Based on this definition, performance expectancy is the attained gain from using a mobile banking application. Research done by Merhi et al. (2019) discusses that performance expectancy has been forecast as one of the most critical factors influencing the use of mobile banking applications. Performance expectancy was referred to as a relative advantage in the Diffusion of Innovation (DOI) model by Rogers (1995), and as perceived usefulness in TAM by Davids (1989).

The following factors from literature (Table 3 – 2) are related to Performance Expectancy:

- Perceived usefulness – Aged users were found to adopt and use mobile banking applications if the gain of using the mobile banking application was realized (Cham et al., 2021).

The following hypothesis is suggested:

H1: Performance Expectancy positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the related statements proposed for the questionnaire are:

Table 3 – 6: Questionnaire statements for Performance Expectancy

Code	Statement	Source	Original UTAUT2 question
PE1	The use of mobile banking applications is useful in my daily life.	Venkatesh et al. (2003), Venkatesh et al. (2012)	I find the mobile Internet useful in my daily life.
PE2	The use of mobile banking applications helps me complete banking tasks quickly.		Using the mobile Internet helps me accomplish things more quickly.
PE3	The use of mobile banking applications increases my productivity.		Using mobile Internet increases my productivity.

3.3.3.2 Effort Expectancy (EE)

Informed by UTAUT2, this construct is the degree to which mobile banking applications are perceived to be easy to use by aged users (Venkatesh et al., 2003). Based on this definition, effort expectancy means that minimal effort is required to effectively use a mobile banking application. Effort expectancy was referred to as Complexity in the Diffusion of Innovation (DOI) model by Rogers (1995) and as perceived ease of use in TAM by Davids (1989). Venkatesh et al. (2012) found that there is a close association between users' willingness to use mobile banking applications and the perceived ease of use of mobile banking applications.

The following factors from the literature (Table 3 – 2) are related to Effort Expectancy:

- Motor movement of aged users – Aged users can suffer a decline in motor movement, and small tasks such as using a mobile banking application and completing a task can be tedious, requiring more effort. Where less effort is required, aged users are found to complete tasks easily (Johnson, 2022).
- Human factors, perception, memory loss – Aged users can suffer a decline in the ability to remember, with the decline in cognitive ability, and this should be included in the design of mobile banking applications for aged users (Sarcar et al., 2017). Sarcar et al. (2017) found that this aspect impacts the perception of the experience of using the mobile banking application by aged users. With

the secure nature of mobile banking applications (Osho et al., 2019) and the need for aged users to be able to remember passwords, it is important that there is minimal effort required for an aged user to still use the mobile banking application despite human factors and memory loss (Sarcar et al., 2017).

- Legibility challenges – The mobile banking application’s interface should cater to aged users, as legibility challenges can be higher with the aged (Johnson, 2022). This can lead to avoidance of use due to the fear of making mistakes, as more effort is required to use the mobile banking application with legibility challenges; mobile banking applications that are legible for aged users require less effort to use (Sarcar et al., 2017).
- Complexity of mobile banking applications – With the evolving growth of technology, the development of mobile banking applications has resulted in complex applications that are difficult to access and use securely by aged users (Saukkonen, P. et al., 2022). The required effort to use mobile banking applications is reduced if the mobile banking applications are simple, easy to access, free of complexity, and can be used securely by aged users (Saukkonen, P. et al., 2022).
- Complex authentication mechanisms – To access and use a mobile banking application, an aged user must be successfully authenticated. However, the complex authentication mechanisms on mobile banking applications, especially when they do not cater to aged users’ decline in cognitive ability, require significant effort from aged users (Iqbal et al., 2020). Authentication is a key factor in the security of mobile banking applications (Amin et al., 2017), and the easier it is for the aged user to authenticate and use the mobile banking application, the more they use the mobile banking application (Iqbal et al., 2020).
- Complex security mechanisms – Security is a key feature for use of mobile banking applications by aged users. However, when the security mechanisms are complex and difficult to use, more effort is required from the aged user, which can result in avoiding use of the mobile banking application (Mendel & Toch, 2019). The less effort that is required to navigate the security mechanisms on a mobile banking application, such as enabling push notifications on transactions of a set threshold (Rogozhkina, 2022), the more

aged users are inclined to use mobile banking applications (Mendel & Toch, 2019).

- Complex privacy management mechanisms – Security is a key concern for aged users, and the complex privacy management mechanisms on mobile banking applications can lead to anxiety and therefore avoidance to use mobile banking applications, as stated by Coventry and Briggs (2021). When less effort is required to navigate privacy management mechanisms on a mobile banking application, such as updating the contact preferences for accounts on mobile banking applications for aged users, aged users will be more inclined to use mobile banking applications (Coventry and Briggs, 2021).

This study assumes that the likelihood of aged users using mobile banking applications increases if they are easy to use. The following hypothesis is suggested:

H2: Effort Expectancy positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the following statements are proposed for the questionnaire:

Table 3 – 7: Questionnaire statements for Effort Expectancy

Code	Statement	Source	Original UTAUT2 question
EE1	Learning how to use mobile banking applications is easy.	Venkatesh et al. (2012)	Learning how to use mobile Internet is easy for me.
EE2	My interactions with mobile banking applications are clear and understandable.		My interaction with the mobile Internet is clear and understandable.
EE3	Mobile banking applications are easy to use.		I find mobile Internet easy to use.
EE4	It is easy for me to become skilful at using mobile banking applications.		It is easy for me to become skilful at using mobile Internet.
EE5	Elements on the mobile banking application (such as screen	Johnson (2022)	Not applicable; derived from literature.

Code	Statement	Source	Original UTAUT2 question
	display) make it easy to use mobile banking applications.		

3.3.3.3 Social Influence (SI)

Venkatesh et al. (2003) define social influence as the degree to which a user perceives technology to be appreciated by the social network or community that is close or important to that user. This can be attributed to the effect that the influence of social media, friends, and family have on a user's behaviour and perception (Venkatesh et al., 2012). Social Influence was referred to as Image in the DOI model by Rogers (1995). With technology increasingly becoming a part of everyday life, aged users are often influenced by others to use technology; this can be through friends, family, or social media (Koosha, 2018).

The following factors from the literature (see Table 3 – 2) are related to Social Influence:

- No social support or influence – Aged users lean on the support of the people around them; feedback from this community impacts their decisions, particularly regarding the use of mobile banking applications (Latulipe et al., 2022). Trying to keep the experience of using the mobile banking application secure in the absence of this support generates anxiety and avoidance (Cham et al., 2021).

The following hypothesis is suggested:

H3: Social Influence positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 8: Questionnaire statements for Social Influence

Code	Statement	Source	Original UTAUT2 question
SI1	The people who are important to me think that I should use mobile banking applications.	Venkatesh et al. (2003), Venkatesh et al. (2012)	People who are important to me think that I should use mobile Internet.
SI2	The people who influence my behaviour think that I should use mobile banking applications.		People who influence my behaviour think that I should use mobile Internet.
SI3	The people whose opinions that I value prefer that I use mobile banking applications.		People whose opinions that I value prefer that I use mobile Internet.
SI4	The people who are important to me support my use of mobile banking applications.	Latulipe et al. (2022)	Not applicable; derived from literature
SI5	I have confidence in using mobile banking applications if my friends and family also use them.		

3.3.3.4 Facilitating Conditions (FC)

Informed by UTAUT2, this construct represents the degree to which aged users believe that they possess the resources to support the use of a mobile banking application (Venkatesh et al., 2003). Facilitating Conditions are referred to as compatibility in the Diffusion of Innovation (DOI) model by Rogers (1995), and as perceived behavioural control in the TPB model by Ajzen (1991). For a user to use a mobile banking application, they need to be able to:

- Install applications;
- Use the Internet;
- Use a mobile device;
- Understand basic security mechanisms (such as the login functionality); and
- Understand security vulnerabilities.

Baptista & Oliveira (2015) state that a user with access to the facilitating conditions that support the above (such as support chats, demonstrations of functionality, and manuals on the use of functionality) will have a greater intention to use an application.

The following factors, derived from literature (see Table 3 – 2) are related to Facilitating Conditions:

- Preventative security knowledge gap – It is important to ensure that aged users are schooled in, and aware of, the preventative measures that ensure a secure experience when using the mobile banking application (Latulipe et al., 2022).
- Technology readiness – According to Msweli & Mawela (2020), aged users were found to be lacking when it came to the propensity to use modern technologies. This can impact the use of mobile banking applications by aged users, as it leads to a lack of resources; aged users need to be confident enough to trust and use the mobile banking applications (Msweli & Mawela, 2020).
- In-application support – Support that is readily available and easy to access within the mobile banking application is key for the aged user, as this fosters the development of trust in using the mobile banking application (Balcerzak et al., 2017). This is useful when aged users face security challenges or have security-related queries that need prompt attention.
- Emergency assistance – Assistance should be readily and easily available for aged users while using the mobile banking application, especially in the case of an emergency (Balcerzak et al., 2017). This can include scenarios whereby an aged person is not able to withdraw their funds because someone else is accessing these funds.
- Adequate use and exposure – Aged users are increasingly making use of mobile banking applications for daily activities, and those who receive training on using technology products are more confident, aware, and less prone to security risks compared to those who do not (Klímová et al., 2018).

The following hypothesis is suggested:

H4: Facilitating Conditions positively influences the Perceived Security of mobile banking applications.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 9: Questionnaire statements for Facilitating Conditions

Code	Statement	Source	Original UTAUT2 question
FC1	I have the resources necessary to use mobile banking applications.	Venkatesh et al. (2003), Venkatesh et al. (2012)	I have the resources necessary to use mobile Internet.
FC2	I have the knowledge to use mobile banking applications.		I have the knowledge necessary to use mobile Internet.
FC3	Mobile banking applications are compatible with other technologies (such as mobile phones) I use.		Mobile Internet is compatible with other technologies I use.
FC4	I can get help from others when I have difficulties using mobile banking applications.		I can get help from others when I have difficulties using mobile Internet.
FC5	There is sufficient support offered by the financial institutions for using mobile banking applications.	Balcerzak et al. (2017)	Not applicable; derived from literature

3.3.3.5 Hedonic Motivation (HM)

Informed by UTAUT2, this construct represents the degree to which mobile banking applications are perceived to provide pleasure, enjoyment, and amusement; it can also be described as the amusement obtained from using the mobile banking application by aged users (Venkatesh et al., 2003). Venkatesh et al. (2012) discovered that there is a strong connection between the rate of increase in pleasure

of using a mobile banking application, to the acceptance of use of mobile banking applications by users.

The following factors from literature (see Table 3 – 2) are related to Hedonic Motivation:

- Pleasurable user experience – An aged user-friendly and appealing user interface, with security elements such as notifications and buttons that are easy to use and view by aged users, were found to be key features to be considered in the design of mobile banking applications for aged users, as this contributed to a pleasurable experience (Ubam et al., 2021).

The following hypothesis is suggested:

H5: Hedonic Motivation positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 10: Questionnaire statements for Hedonic Motivation

Code	Statement	Source	Original UTAUT2 question
HM1	Using a mobile banking application is fun.	Venkatesh et al. (2012)	Using mobile Internet is fun.
HM2	Using a mobile banking application is enjoyable.		Using mobile Internet is enjoyable.
HM3	Using the mobile banking application is very exciting.		Using mobile Internet is very entertaining.

3.3.3.6 Price Value (PV)

Informed by UTAUT2, this construct represents aged users' reasoning between the monetary cost of using mobile banking applications and the perceived benefits of the use of mobile banking applications (Venkatesh et al., 2012). If the benefits of using a mobile banking application are perceived to outweigh the cost, then the price value is positive. Services that have a positive price value are more likely to attract customers (Merhi et al., 2019).

The reduced cost of mobile banking applications that also offer a secure banking experience will contribute to the overall use of mobile banking applications by users (Esmaeili et al., 2021; Afshan & Sharif, 2016; Al-Jabri & Sohail, 2012).

The following factors from literature (see Table 3 – 2) are related to Price Value:

- Cost of banking – South Africa is a developing country; as such, secure low-cost banking is important to aged users. This can be offered by mobile banking applications (Msweli & Mawela, 2020).

The following hypothesis is suggested:

H6: Price Value positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 11: Questionnaire statements for Price Value

Code	Statement	Source	Original UTAUT2 question
PV1	Mobile banking applications are priced.	Venkatesh et al. (2012)	Mobile Internet is priced.
PV2	Mobile banking applications provide good value for money.		Mobile Internet is a good value for the money.
PV3	At the current price, the mobile banking applications provide good value.		At the current price, mobile Internet provides a good value.

3.3.3.7 Habit (HB)

Informed by UTAUT2, this construct represents the degree to which aged users learn to perform certain behaviours on the mobile banking application automatically (Venkatesh et al., 2012). As such, habits can be created if a mobile banking application is frequently used. According to research done by Venkatesh et al. (2012), habit is one of the determining factors that have been used to predict users' behavioural intention to use mobile banking applications in several studies.

Aged users have shown that they develop trust in mobile banking applications if they develop a habit of using mobile banking applications by becoming familiar with the applications (Gefen, 2000).

The following factors from literature (see Table 3 – 2) are related to Habit:

- Experience – Klímová et al. (2018) found that aged users who increasingly make use of mobile banking applications have experience in the use thereof, and are more confident, aware, and less prone to security risks compared to those who do not.

The following hypothesis is suggested:

H7: Habit positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 12: Questionnaire statements for Habit

Code	Statement	Source	Original UTAUT2 question
HB1	The use of mobile banking applications has become a habit for me.	Venkatesh et al. (2012)	The use of mobile Internet has become a habit for me.
HB2	I am addicted to using mobile banking applications.		I am addicted to using the mobile Internet.
HB3	I must use mobile banking applications.		I must use mobile Internet.
HB4	I have adequate experience to use mobile banking applications.	Klímová et al. (2018)	Not applicable; derived from literature

3.3.3.8 Perceived Privacy (PP)

This aspect was derived from literature as an additional independent variable; it represents the degree to which aged users perceive that personal information can be kept safe and without being compromised while using mobile banking applications (Westin, 1968). Privacy concerns have been shown as inhibitors to mobile

technology adoption across several studies (Johnson et al., 2020). Research done by Johnson et al. (2020) found that perceived privacy could impact the user's intention to adopt and use mobile payment systems.

Aged users need to be convinced of, and be comfortable with, the privacy of mobile banking applications.

The following factors from literature (see Table 3 – 2) are related to Perceived Privacy:

- Perceived privacy loss – This has to do with aged users' data, and the fear of losing privacy or it being compromised (Cham et al., 2021). The lower the perceived privacy loss, the higher the probability that the aged user will make use of the mobile banking application (Cham et al., 2021).

The following hypothesis is proposed:

H8: Perceived Privacy positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 13: Questionnaire statements for Perceived Privacy

Code	Statement	Source	Original UTAUT2 question
PP1	My personal information is safe when using mobile banking applications.	Cham et al. (2021)	Not applicable; derived from literature
PP2	Mobile banking applications offer sufficient privacy protection measures.		
PP3	Unauthorized people will not be able to view the details I input while transacting on the mobile banking application.		
PP4	My transaction information is protected when using mobile banking applications.		

Code	Statement	Source	Original UTAUT2 question
PP5	Mobile banking applications keep my private information protected.		

3.3.3.9 Technological Trust (TT)

This aspect was derived from literature as an additional independent variable; it represents the trust that the aged user has in the channel or medium used for banking transactions (i.e., the mobile banking application) (Apau & Koranteng, 2019). Due to the role of technology in facilitating mobile banking transactions, it has an impact on users' desire to transact using mobile banking applications (Apau & Koranteng, 2019). According to Merhi et al. (2019), technological trust is one of the key influencers of behavioural intention due to the existence of an inverse relationship with perceived risk. This means that greater technology trust will lower perceived risk and will have a favourable effect on aged users' willingness to use mobile banking applications.

The following factors from literature (see Table 3 – 2) are related to Technological Trust:

- Technological trust – The trust that an aged user has in using the mobile banking application is an important dimension of the perception of secure use of the mobile banking application by the aged user (Rajaobelina et al., 2020).

The following hypothesis is suggested:

H9: Technological Trust positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 14: Questionnaire statements for Technological Trust

Code	Statement	Source	Original UTAUT2 question
TT1	I can trust mobile banking applications.	Rajaobelina et al. (2020)	

Code	Statement	Source	Original UTAUT2 question
TT2	Mobile banking applications restrict unauthorized access.		Not applicable; derived from literature
TT3	I can trust mobile banking applications to accurately process transactions.		

3.3.3.10 Perceived Risk (PR)

This aspect was derived from literature as an additional independent variable; it represents the potential loss that an aged user can suffer while trying to use a mobile banking application to attain a specific desired outcome (Paek & Hove, 2017). In the TPR model, Featherman & Pavlou (2003) define perceived risk as the potential loss that a user can suffer while trying to attain a specific desired outcome when using a mobile banking application. Research done by Chen & Holsapple (2013) shows that perceived risk can influence a user's trust and the security of a mobile banking application. Based on this, aged users will not use a mobile banking application if they consider it to be risky.

The following factors from literature (see Table 3 – 2) are related to Perceived Risk:

- Proxy trust – A proxy can be a known or unknown person to the aged user, who can assist the aged user in their inability to complete certain tasks, including banking. Balcerzak et al. (2017) found that aged users have a difficult time trusting unknown people in this regard, due to their perceived risk and fear of a negative outcome with the proxy. As a result, if there is trust with a designated proxy, this may increase the aged user's mobile banking application use (Balcerzak et al., 2017).
- Proxy authentication – Balcerzak et al. (2017) discuss the use of a trustworthy external organization to ensure that a proxy is successfully authenticated before assisting an aged user, due to the risks of using an unauthenticated proxy. The OECD (2020) found that even people known to aged users and appointed as proxies can pose a risk to the aged user while transacting on

their behalf on mobile banking applications; therefore, a diligent authentication process should be used with the proxies to minimize perceived risk.

The following hypothesis is suggested:

H10: Perceived Risk positively influences the Perceived Security of mobile banking applications by aged users.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 15: Questionnaire statements for Perceived Risk

Code	Statement	Source	Original UTAUT2 question
PR1	Using mobile banking applications does not put my privacy at risk.	Balcerzak et al. (2017)	Not applicable; derived from literature
PR2	People trusted to assist me with using mobile banking applications do not pose a risk to my funds.		
PR3	Criminals cannot try and take control of my account if I use mobile banking applications.	Latulipe et al. (2022)	
PR4	The chances of losing my money if I use mobile banking applications are low.		
PR5	It is harmless for me to use mobile banking applications.		

3.3.3.11 Perceived Security (PS)

This aspect was derived from literature as an additional dependent variable; it represents the degree of trust that mobile banking applications can securely transmit sensitive information without any breaches (Merhi et al., 2019).

With security being one of the fundamental issues that impact mobile banking applications (Chanajitt et al., 2016), the use of mobile banking applications is a concern to aged users because of the possible security breaches by malicious users

(Mendel & Toch, 2019). The UTAUT2 model did not include security in the acceptance of technology; however, the perception of security while using mobile banking technology applications has been noted as one of the main inhibitors of the use and growth of mobile banking technology (Merhi et al., 2019). Aged users' trust in mobile banking applications will be non-existent without aged users being convinced of the security of mobile banking applications.

The following factors from the literature (see Table 3 – 2) are related to Perceived Security:

- Password management – Morrison et al. (2021) found that aged users struggle with password management, and do not trust applications such as password managers to assist with password management for mobile banking applications.
- Secure verification – A study conducted by Ubam et al. (2021) found that secure verification was the second most critical factor for aged users on mobile banking applications; therefore, secure verification when accessing mobile banking applications is a key feature for aged users.
- Secure authorization process – A study conducted by Ubam et al. (2021) found that a secure authorization process was the fourth most critical factor for aged users on mobile banking applications; therefore, having a secure authorization process for transactions is a key feature for aged users.
- Automatic sign-out (with inactivity) – Ubam et al. (2021) found that aged users preferred to use mobile banking applications if they had an automatic sign-out with inactivity to enhance the secure experience for the user.
- Device security – Morrison et al. (2021) found that device security contributes to the use of mobile banking applications, as aged users who did not find their devices secure did not use mobile banking applications as much as those who did.
- Perceived security compromise – Tiwari et al. (2020) found that the likelihood of aged users using mobile banking applications increases if the applications are fully secure, due to the concern of the security being compromised.

The following hypothesis is suggested:

H11: Perceived Security positively influences Behavioural Intention by aged users to use mobile banking applications.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 16: Questionnaire statements for Perceived Security

Code	Statement	Source	Original UTAUT2 question
PS1	Mobile banking applications are secure.	Mendel & Toch, 2019	Not applicable; derived from literature
PS2	My user data on mobile banking applications is secure.		
PS3	My transaction details on mobile banking applications are secure.		
PS4	The mobile banking applications have diligent security controls.	Morrison et al. (2021)	
PS5	My interaction with mobile banking applications is secure.		
PS6	There is nothing to worry about regarding the security of the mobile banking applications.		

3.3.3.12 Behavioural Intention (BI)

Venkatesh et al. (2003) define behavioural intention as an aged user’s readiness or motivation to use a mobile banking application. Venkatesh et al. (2012) state that the use of mobile banking applications is significantly influenced by behavioural intention; it therefore measures aged users’ relative strength of intention to use the mobile banking application.

The following hypothesis is suggested:

H12: Behavioural Intention to use mobile banking applications positively influences the actual Use Behaviour of mobile banking applications.

Therefore, the statements proposed for the questionnaire are:

Table 3 – 17: Questionnaire statements for Behavioural Intention

Code	Statement	Source	Original UTAUT2 question
BI1	I intend to continue using mobile banking applications in the future.	Venkatesh et al. (2003), Venkatesh et al. (2012)	I intend to continue using mobile Internet in the future.
BI2	I will always try to use mobile banking applications in my daily life.		I will always try to use mobile Internet in my daily life.
BI3	I plan to continue to use mobile banking applications frequently.		I plan to continue to use mobile Internet frequently.

3.3.3.13 Use Behaviour (UB)

Venkatesh et al. (2003) define use behaviour as an indicator of how frequently an aged user uses a mobile banking application. A study conducted by Wu et al. (2012) found that use behaviour is influenced by Behavioural Intention.

The statements proposed for the questionnaire are:

Table 3 – 18: Questionnaire statements for Use Behaviour

Code	Statement	Source	Original UTAUT2 question
UB1	I regularly use mobile banking applications.	Cham et al. (2021), Rajaobelina et al. (2020)	Not applicable; derived from literature
UB2	I use mobile banking applications for all my banking needs.		
UB3	I have increased my use of mobile banking applications over time.		

3.3.4 Conceptual Model – Aged users’ mobile banking application security factors model

Based on the suggested hypotheses, the following conceptual model is proposed (Figure 3 – 6).

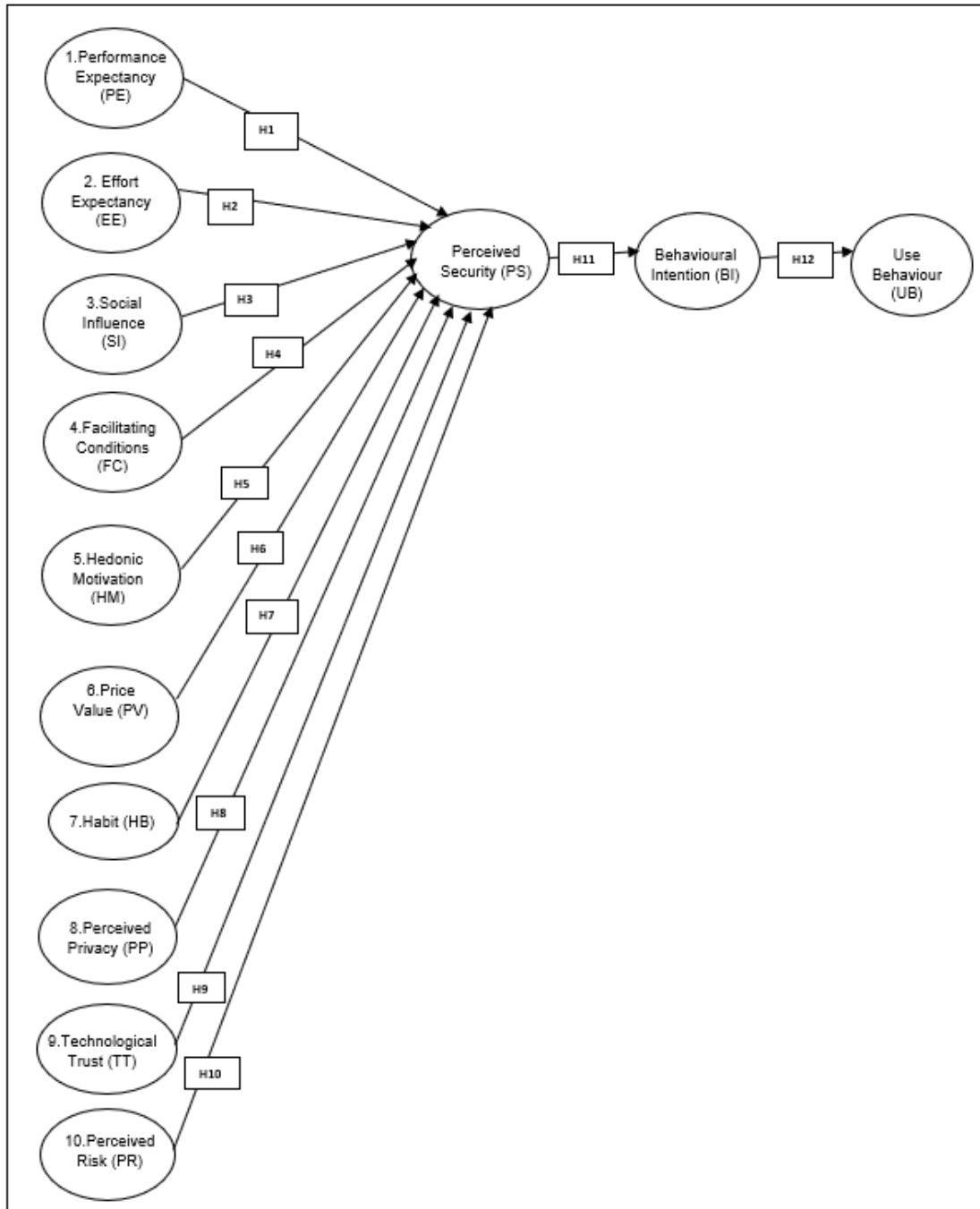


Figure 3 – 6: Conceptual model – Aged users’ mobile banking application security factors model

This model was updated on completion of the data collection for the study.

3.4 Conclusion

Chapter 3 provided an overview of the details of the literature review, including the literature search and analysis findings for known perceptions of aged users on the security of mobile banking applications, as well as existing security factors on mobile banking applications for the aged. This chapter concluded the literature review for the study.

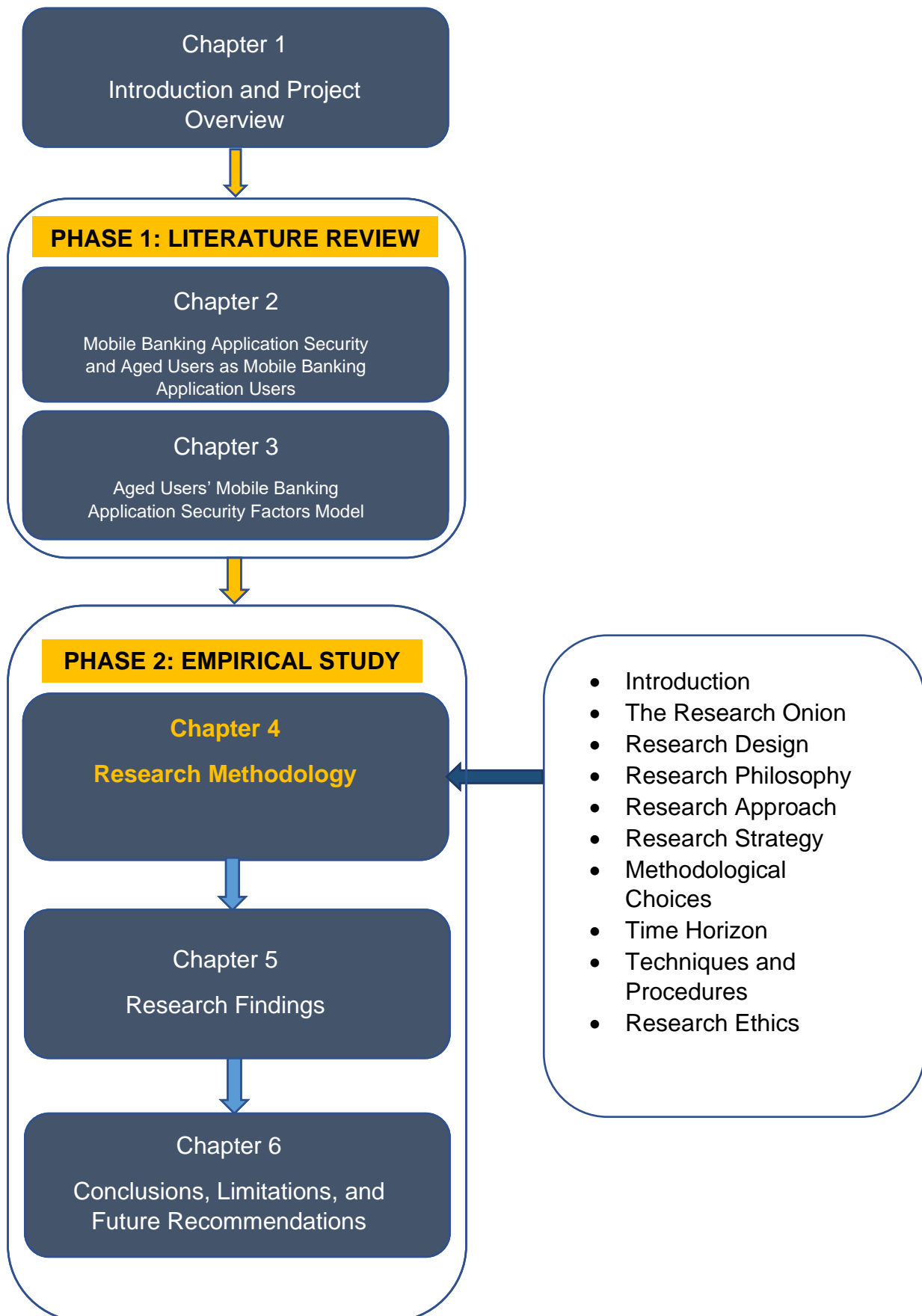
The theories of acceptance of technology were discussed, with UTAUT2 highlighted as informing the study, the hypotheses for the study postulated, and the hypothesized model was proposed for the Aged Users' Mobile Banking Application Security Factors Model.

This chapter addressed the following objectives:

- To analyse literature for factors that influence aged users' perception of the security of mobile banking applications;
- To develop the Aged Users' Mobile Banking Application Security Factors Model of the factors that influence aged users' perception of the security of mobile banking applications; and
- To develop a questionnaire based on the Aged Users' Mobile Banking Application Security Factors Model.

Chapter 4 will provide an overview of the research methodology adopted for this study as well as the data collection instrument. This will include the research strategy, research approach, and research design.

CHAPTER 4



RESEARCH METHODOLOGY

4.1 Introduction

Chapter 4 provides an overview of the research methodology adopted for this study to meet its research objectives. The research methodology provides the operational elements of the research, by providing a map of the overall research process adopted for the study. Denzin and Lincoln (2005) state that a study's research methodology is shaped by the phenomena of interest for the study, as well as the nature of the research questions. Therefore, the underlying presumptions about the research validity serve as a guide for research, as well as the methods that are adopted and considered suitable for the study. The research methodology used to address the research questions is covered in this chapter. The chapter also covers the study's data collection instrument, the methods used for data collection and data analysis, as well as the rationale behind the selection of the method for this study.

This study used a questionnaire as survey instrument, which was developed using the constructs that were determined in the literature review in Chapter 3. An expert panel review and a pilot test were conducted to ensure the validity of the questionnaire by confirming its accuracy and understandability. The descriptive analysis of the data was performed using the Statistical Package for the Social Sciences (SPSS) to determine standard deviations, means, and frequencies. Exploratory Factor Analysis (EFA) was conducted to validate the questionnaire, and the study hypotheses were tested using multiple regression analysis.

4.2 The research onion

Saunders et al. (2019) demonstrate a research onion as a means of outlining the data collection methods and representing the methods selected for this study.

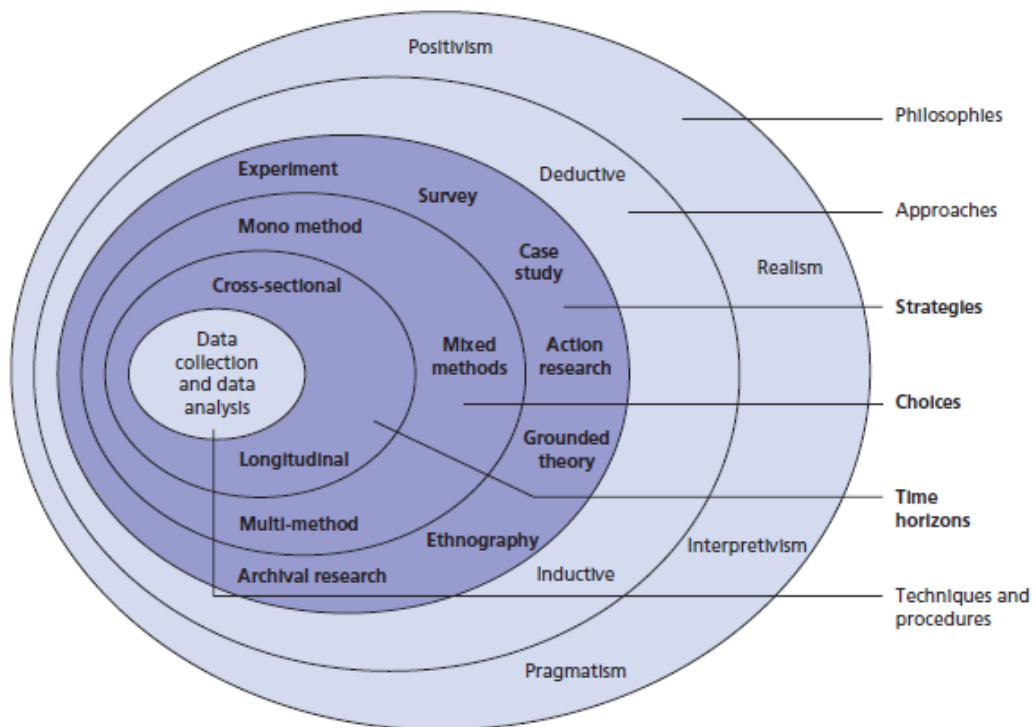


Figure 4 – 1: The research onion (Saunders et al. 2007)

The research onion created by Saunders et al. (2007) serves as an illustration of the stages that are involved in the development of research. This is represented as an onion, with each layer representing one of the various stages of the research. The research onion visually provides a representation of the development of a research methodology. Saunders et al. (2019) advises that a researcher should work from the outer to the inner layers of the research onion when developing a research methodology. When viewed from the outside of the research onion, each layer offers a more thorough description of a particular step in the research process (Saunders et al., 2019). Therefore, the inner layer of the onion can only be viewed by peeling the outer layer; this indicates the nature of the research process, namely, that one step is covered before proceeding to the next step.

The Saunders research onion forms the basis of the research methodology for this. Table 4 – 1 shows the selections for the research methodology, as applicable to this study. The research methodology selections are detailed in this chapter, starting from Section 4.4.

Table 4 – 1: Research methodology philosophy and approach: summary selection, as per Saunders et al. (2019)

Research onion layer	Research onion section	Research methodology selection
Research philosophy	Research design	Positivist
Research approach	Research design	Deductive
Research strategy	Research design	Survey
Choices	Research design	Mono method (Quantitative)
Time horizon	Research tactics	Cross-sectional
Techniques and procedures	Research tactics	Data collection: Questionnaire
		Data analysis: Inferential and descriptive statistics

4.3 Research design

Malhotra (2010) defines research design as the framework or the blueprint that is used to guide and inform a research project, including the details of the processes followed, as required for the documented project. The research design illustrates the key components of the research, including but not limited to the measure, areas, and samples, and how these are used to address the research objectives (Mouton, 2001). Mouton (2001) goes on to describe the research design as a methodical strategy used to increase the reliability of the research and its findings.

Saunders et al. (2019) state that the research design serves as a plan of action for moving from one point of the research to the next. This would be from the study's research questions or pertinent research objectives that must be satisfied, to the answers that the study must provide regarding the research questions or objectives. Saunders et al. (2019) also proceed to add that, by adhering to the idea that the research study should be designed first, the researcher enhances the study's planning and implementation phases. This assists with the intended results that are obtained, and guarantees that the information obtained is accurate and relevant to the problem being studied.

4.4 Research philosophy

Saunders et al. (2019) terms research philosophy as a comprehensive term that is used to denote the thinking that supports the development of the knowledge and the nature of knowledge for a research study. According to Bryman (2016), the research philosophy is a body of ideas about the nature of the phenomena that the study is trying to understand.

Paradigms are used to bring order to the way in which research is conducted. A paradigm is a collection of beliefs and ideas for understanding and observation that have an impact on what the researcher sees and how it is perceived or understood by the researcher (Babbie, 2021). A paradigm is made up of methodology and methods, as well as ontology and epistemology (Scotland, 2012). Therefore, a paradigm can be thought of as a philosophical framework that has assumptions on two dimensions: ontology and epistemology (Scotland, 2012).

Methodology refers to the study and analysis process for research, together with the tools and techniques that are adopted to conduct the research (Grix, 2004). It includes a discussion on how the research should be undertaken, and should include the details of the research procedures and processes that have been included to conserve the objectivity of the research, while answering the research question (Mouton, 2001). The methodology should therefore guide the researcher on the appropriate type of data that is required for the study and the applicable data collection tools. Through a methodological question, the researcher should be able to ask how the world should be studied (Rehman & Alharthi, 2016). For this study, the researcher outlined a research methodology as adapted from the research onion of Saunders et al. (2019).

Mouton (2001) demonstrates the relationship between research design and research methodology in Figure 4 – 1.

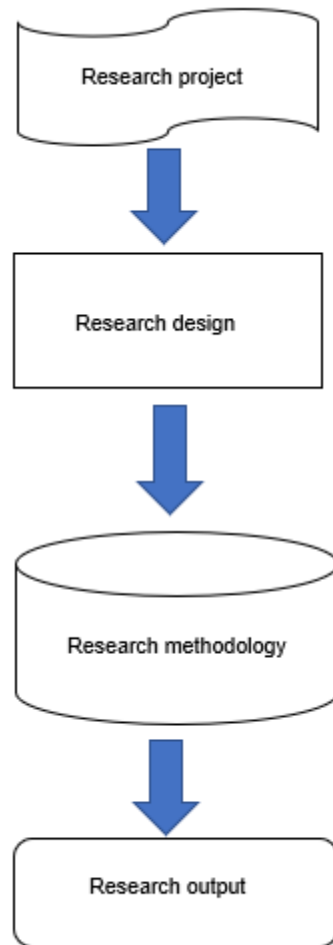


Figure 4 – 2: The relationship between research design and research methodology (Mouton, 2001)

Ontology is referred to as the nature of the researcher's beliefs about reality (Scotland, 2012). The researcher has assumptions about reality and, through an ontological question, the researcher can inquire about the kind of reality that exists (Rehman & Alharthi, 2016). It can be positivist, realistic, interpretivist, or pragmatic (Saunders et al., 2019). For this study on the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users, the perceptions shared by aged users during the data collection are their own alone, and no one else's. For this reason, a positivist philosophy is adopted.

Epistemology is the study of knowledge to achieve valid and acceptable results, and refers to what can be accepted as valid beliefs (Wahyuni, 2012). It includes the analysis of the relationship that exists between the way the researcher collects and interprets data, and the researcher's interpretation of the truth and knowledge with

respect to the topic that is being researched. (Collis & Hussey, 2003). Through an epistemological question, the researcher can debate “the possibility and desirability of objectivity, subjectivity, causality, validity, generalisability” (Patton, 2002:134). This knowledge can be empirical, meaning that it can be described as based on phenomena that are observed or experienced, or intuitive (i.e., indicating that it is based on beliefs). This study made use of empirical knowledge by conducting an empirical study on factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa. The findings, which could be observed and measured, and the conclusions of the study were made from the empirical evidence collected.

4.4.1 Research paradigm

The positivist paradigm or philosophy is a traditional form of research that is also referred to as empirical science (Creswell, 2013). It relates to the various ways that knowledge can be acquired, and is used to describe the connections between two or more variables (Saunders et al., 2019). There are two assumptions associated with this philosophy: first, there is absolute order in this world and, second, all phenomena can be objectively studied (Oates, 2006). The positivist philosophy is based on the researcher being separate or disconnected from the object of the study, therefore enabling the researcher to assume an objective view of the study, which is known as objectivism (Neuman, 2014). Neuman (2014) explains that researchers who adopt positivist philosophies are detached from the research object, and are not considered variables in the research.

This paradigm includes the identification of constructs and the examination of theory that already exists and, therefore, is used in studies or exercises that are required to test a hypothesis (Saunders et al., 2019). Three techniques are used with the positivist paradigm, namely: refutability, reductionism, and repeatability (Oates, 2006). According to Oates (2006), refutability is when a researcher duplicates another researcher’s study but comes to a different conclusion or finding, thereby refuting the first researcher’s work. Reductionism occurs when a compound problem is broken down and becomes a collection of smaller or less complex problems, thereby making it easier to investigate and conduct research on (Galliers, 1985). Repeatability tests whether the same result can be obtained by conducting the same research multiple times, in the same manner (Oates, 2006).

The positivist paradigm is deductive and makes use of quantitative data, which is normally collected from a sizeable sample of the population under study (Saunders et al., 2019). This paradigm was chosen for this study, since it supports a quantitative data collection process that allows for the development of a model based on a statistical analysis of user perceptions. The study required observing the data objectively as it included the formulation and testing of hypotheses to derive deductions, generalize, and make conclusions.

4.5 Research approach

Deductive or inductive research approaches could be considered (Saunders et al., 2019). The deductive approach requires that a researcher develops or makes use of an existing theory to be used in developing hypotheses. The researcher then conducts a review of the existing literature and uses the relevant variables from the literature to test the hypotheses (Creswell, 2013). The data for the phenomenon under study is collected and analysed (Saunders et al., 2019). This approach involves testing an existing theory and attempting to validate the theory using the findings or outcomes of the study's data (Leedy & Ormrod, 2019). The validation or testing of the theory can confirm or refute the theory, or indicate whether the theory needs to be updated (Saunders et al., 2019). The process flow for the deductive approach is demonstrated in Figure 4 – 3.

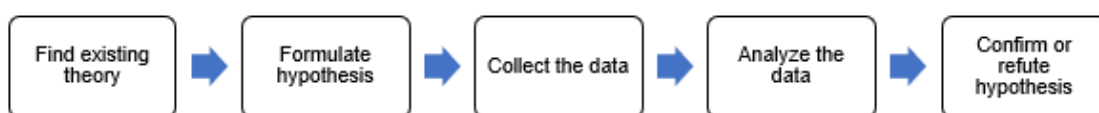


Figure 4 – 3: The deductive approach sequence of steps

The deductive method was used in conducting this study. The researcher conducted a literature study, proposed hypotheses, conducted data collection and analysis, and tested the hypotheses.

The deductive approach aligns with the positivist paradigm, as selected for this study, in making use of quantitative data (Saunders et al., 2019).

4.6 Research strategy

The research strategy provides the process by which the study is conducted (Saunders et al., 2019). Several research strategies exist, namely, action research, archival research, case study, ethnography, experiment, grounded theory, and survey.

The survey strategy is normally used to interpret quantitative data that is collected from a sample of the population under study, and the description of the pattern or trend identified can be quantitative or numeric (Creswell, 2013). The researcher can then make conclusions about the population from the findings of the data gathered from the sample of the population under study (Creswell, 2013). For this study, the survey strategy was used to provide a numerical representation of the factors that have a significant influence on the perception of security of the use of mobile banking applications by aged users in South Africa. The study tested the relationship that exists between the theoretical constructs and variables by using questions that were formulated from theoretical constructs (Saunders et al., 2019).

Saunders et al. (2016) state that economic use of surveys enables data collection. Surveys require that a large amount of data be collected to ascertain the relationship that exists between the identified literature constructs (Saunders et al., 2019). The standardized collection of data by means of surveys allows for easy analysis thereof (Saunders et al., 2019). The survey strategy is dependent on the respondent's ability to answer the questions posed in the questionnaire, as there are restrictions on how many questions can be asked. Therefore, the questions must be well-drafted and clear to elicit high-quality answers from respondents (Saunders et al., 2019).

Table 4 – 2 shows the advantages and disadvantages of adopting a questionnaire-based survey strategy (Oates, 2006; Saunders et al., 2019).

Table 4 – 2: Advantages and disadvantages of surveys

Advantages	Disadvantages	Management of disadvantages in this study
Cost-effective	Respondents can provide dishonest answers.	Dishonest answers were managed through: <ul style="list-style-type: none"> • Avoiding leading questions in the questionnaire statements. • Using an anonymous survey, this was stated to the participants. • Not offering incentives for completing the survey questionnaire, as stated to the participants.
Offers a quick way to get results	Questions can be incorrectly interpreted.	The questionnaire statements were simple and concise, without the use of double-barrelled or leading questions. The questionnaire was also examined by a pilot group and an expert panel, and updates were applied based on the feedback provided.

Advantages	Disadvantages	Management of disadvantages in this study
Easy to format by allowing for open or closed questions, therefore allowing for the collection of a large amount of data.	Some questions can be omitted or left unanswered.	A user did not need to complete all the questions in the questionnaire. This disadvantage did not apply to the study.
Offers scalability as questionnaires can be administered online.	Does not allow for capturing of feelings or emotions.	This study did not investigate feelings or emotions; therefore, this disadvantage did not apply to the study.
Offers data that is easy to analyse and visualize.	Does not cater for accessibility issues, for example, users who cannot see.	The population for this study comprised of aged users who make use of mobile banking applications; they would therefore be able to complete the survey questionnaire electronically or by using a hard copy thereof.
Allows respondents to remain anonymous, especially if completed online or when using email.		
No time constraints to complete the questionnaire.		

4.7 Methodological choices

Creswell (2013) states that multiple factors are used to determine the most applicable research method for a study. The type of research methodology to be used can be determined by the research problem, including the experience of the researcher, the external environment and factors, and the audience with whom the results of the research are shared. Research methods can be qualitative, quantitative, or mixed methods (Creswell, 2013). This refers to the way the data will be gathered and analysed, and to the kinds of conclusions that can be drawn from the data (Creswell, 2013).

This research will adopt the mono-method methodological choice, using a quantitative approach. Mono method means that the research makes use of a single data collection method and related data analysis strategies (Saunders et al., 2019).

4.7.1 Quantitative research

Some paradigms allow for the use of a quantitative research approach, as was selected for this study, in alignment with the positivist philosophy. The information gathered through quantitative research is quantifiable, and can therefore be measured (Saunders et al., 2019). The quantitative research method allows for the quantification of data, through the collection and analysis of numerical data (Creswell, 2013). According to Winter (2000), quantitative research can be used to break down a research phenomenon into measurable categories for easier interpretation. Tools that can be used to collect quantitative data include survey questionnaires and experiments; the data can then be analysed statistically (Winter, 2000). From a sample of the research population under study, variables can be measured, and relationships can be derived from the variables through correlations. This includes the testing of a theory or theories, which is dependent on the development of hypotheses (Winter, 2000).

Table 4 – 3 shows the advantages and disadvantages of quantitative research (Collis and Hussey, 2003; Rahman, 2016; Saunders et al., 2019).

Table 4 – 3: Advantages and disadvantages of quantitative research

Advantages	Disadvantages	Management of disadvantages in this study
The researcher for the study plays an independent role	Excludes the meaning and explanation of phenomena	The study did not investigate the meaning or explanation of factors that influence the security of mobile banking applications; therefore, this disadvantage did not apply to the study.
The variables are measurable, that is, they can be measured	Due to the nature of it being time-framed, it only provides a snapshot in time of phenomena.	The study was meant to investigate the factors that have a significant influence on the security of mobile banking applications at a specific point in time; therefore, this disadvantage did not apply to the study.
Allows for quantification of large amounts of data	Richness of data can be lost if errors are made in the data quantification process.	To successfully analyse the data without sacrificing its richness, a professional statistician's services were enlisted.
It is easy and economical to conduct	This can result in the over-generalization of phenomena.	It has been stated as part of the sample population definition of the study that this cannot be used as a generalization of all aged users in South

Advantages	Disadvantages	Management of disadvantages in this study
		Africa. Inferential statistics were used to allow the researcher to generalize the research results (Saunders et al., 2019).
Analysis of data is simplified and takes less time, as differential and inferential software packages can be used		
Provides high reliability as findings can be generalized due to the use of a sample population in the research		

The quantitative method was adopted for this study, whereby the relationship between the identified variables and constructs from the literature were tested.

According to Creswell (2013), the quantitative method is appropriate where it is required to recognize factors that have an impact on the outcome of a study. Consequently, the quantitative approach was employed, which investigates the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa.

4.8 Time horizon

The research time horizon is defined as the relevant timeframe for the study, and the collection of data at a specific point in time, as defined by the researcher (Saunders et al., 2019). It represents the length of time the researcher spends studying the population sample, and it is chosen based on the study's clearly stated research objectives and the nature of the necessary investigation (Saunders et al., 2019). The

researcher can study a population over a long period of time or at a specific point in time. According to Saunders et al. (2019), research can be cross-sectional or longitudinal.

4.8.1 Longitudinal

Longitudinal studies are conducted over a long period of time, and sampling of the data are repeated to obtain data at various intervals (Saunders et al., 2019). The same population members are sampled when data is gathered; there are no new samples. The outcome of the research is not realized in a short space of time, thus making longitudinal studies reliable from a cause-and-effect perspective. However, longitudinal studies are time-consuming (Saunders et al., 2019).

4.8.2 Cross-sectional

Through cross-sectional research, a research phenomenon can be investigated at a specific point in time (Saunders et al., 2019). This research occurs over a short period of time. Data is gathered from the research sample only once at a given point in time; there is no repetition of the data collection from the population sample (Creswell, 2014). Surveys are mostly used as the data collection tool in cross-sectional studies (Saunders et al., 2019).

This study, which was conducted at a specific moment in time and was time-constrained, used the cross-sectional time horizon to investigate the factors that significantly influence the perception of security in the use of mobile banking applications by aged users in South Africa. The data collection took place over three weeks.

The sample used for this study was not followed over time, nor was there a later follow-up with the respondents to the questionnaire.

4.9 Research procedures and techniques

The sampling, data collection, and data analysis techniques used in this study are discussed in this section.

4.9.1 Sampling technique

One of the most important steps in the research process is choosing the population that will be the subject of the study. The researcher must identify the appropriate

population to respond to the study objectives, test the research hypotheses, and supply the required data (Creswell, 2013). In cases where the population is large and the researcher does not have access to the entire population, a representative sample of the population is used, as identified through a sampling process (Saunders et al., 2019). When it is not feasible or cost-effective to collect data from the entire population, sampling is a useful method (Saunders et al., 2019). Based on the study that was done on the sample and the researcher's knowledge of the sample, generalizations can be made about the population being studied (Saunders et al., 2019).

According to Saunders et al. (2019), there are two different kinds of sampling techniques: probabilistic sampling, also known as random sampling, and non-probabilistic sampling, also known as non-random sampling.

Non-probabilistic sampling includes the pre-selection of a sample by the researcher, which is determined by defined characteristics; as such, there is no random selection (Creswell, 2013).

As the researcher is aware of the likelihood that the population will be represented and how easily the confidence intervals for the statistical analysis can be estimated, probabilistic sampling includes random selection (Saunders et al., 2019). In probabilistic sampling, each participant in the population being studied has a chance of being chosen (Creswell, 2013).

Convenience sampling, a type of non-probability sampling, was used in this study. In convenience sampling, individuals are included in the sample that will make the study the easiest and most convenient for the researcher (Cohen, Manion, & Morrison, 2011). This can be due to geographical location, willingness to participate in the study, or availability at the time of the study (Creswell, 2013).

- Aged users' societies – The convenience sampling method comprised the selection of societies with aged user members in South Africa. This included:
 - A book club for aged users;
 - A cooperative is a group of people who voluntarily work together in an association that they own and run themselves to address their shared social and economic needs (Okem, 2016); and
 - A church.

The aged user societies were distributed throughout South Africa.

- Study survey – The convenience sampling method was used in the survey, which was electronically administered and shared with aged users from the participating societies; responses were provided by willing participants.

This study also made use of purposive sampling, known as judgment sampling, which is a form of non-probability sampling (Etikan, Musa, & Alkassim, 2016). In purposive sampling, the people that form the sample are deliberately selected to be included in the study by the researcher due to the qualities that they possess and the degree of proficiency with the study phenomenon (Etikan et al., 2016). These qualities can be that of experience with or knowledge of the study phenomenon. Additionally, participants must be willing and able to participate (Etikan et al., 2016).

- Expert panel – The expert panel was identified by means of purposive sampling; participants were selected from various specialist fields, namely academic and information security consultants.
- Pilot group – The pilot group was identified by means of purposive sampling, with aged user participants selected due to their willingness and availability to take part in the study.

4.9.2 Sample

For the research's findings to be generalizable, the sample should accurately reflect the traits of the entire group being studied by the researcher (Cohen et al., 2011). The target population, sample size, and analytical unit are discussed in this section.

4.9.2.1 Unit of analysis

To respond to the research questions and accomplish the research objectives, a unit of analysis is the main unit that is examined in the study (Creswell, 2013). The unit of analysis in this study is the aged user, because it focuses on the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa.

4.9.2.2 Sample size

Cohen et al. (2011) state that a population's diversity should be considered when determining the sample size for a research study: for a more diverse population, a

larger sample size is required. Additionally, elements such as the study's objectives influence the size of the sample (Cohen et al., 2011).

According to O'Rourke & Hatcher (2013), there is a dependency between the questions that form the data collection instrument (i.e., the questionnaire) and the sample size. For this study, the sample size was calculated using the following statistical recommendation for evaluating the questionnaire's reliability and validity (Gerber & Hall, 2017):

$$\text{Minimum number of respondents} = \frac{\text{Total number of questions in the questionnaire}}{5} *$$

The study questionnaire consisted of 53 (fifty-three) questions; therefore, approximately 265 responses were needed. A limitation of this approach is that the sample was not representative of aged users in the societies that participated in the study, nor of aged users in South Africa. Non-probability sampling, according to Gerber & Hall (2017), prevents the results from being generalized to the population. With consideration of this sampling approach, inferential statistics were used to enable the researcher to generalize the research findings (Saunders et al., 2019).

A minimum of five experts were required for the expert panel. According to De et al. (2021), there is a general guideline to use 5 – 15 experts for an expert panel review. The expert sample was chosen specifically to review the questionnaire (Cohen et al., 2011). According to Kumar (2011), the selection of a sample of experts is reliant on their ability to provide information based on the expert's in-depth knowledge and experience with the study phenomena. Six individuals formed the expert panel in this study.

According to Saunders et al. (2019), the minimum number for a pilot study should be 10 respondents. This pilot group for study comprised 16 individuals.

4.9.2.3 Target Population

The study sample is drawn from a group called the target population, which possesses the study characteristics (Saunders et al., 2019). The target population for this study comprised aged users in South Africa who make use of mobile banking applications.

The sampling requirements for the aged users for this study are listed in Table 4 – 4.

Table 4 – 4: Study sampling requirements

Segment	Minimum number required	Minimum Age	Skills and experience Required	Location
Study survey	270	65	Mobile banking application use	South Africa
Expert panel	5	-	<ul style="list-style-type: none">• Academic• Information security	Non-specific
Pilot group	10	65	Mobile banking application use	South Africa

4.9.3 Data collection

The process of gathering information to address the research questions is known as data collection (Saunders et al., 2019). Primary or secondary data collection is possible (Saunders et al., 2019). Primary data collection was used in this study. According to Creswell (2018), primary data collection is the process of gathering information directly from the area of study through observation and the use of questionnaires or surveys.

The researcher made use of the organisation's gatekeeper for access to aged users in the societies from which the data was collected. The gatekeeper controls access to the organization and makes the final decision regarding whether the researcher will be allowed access to undertake the research, based on the details that the researcher would have provided (Saunders et al., 2019). According to Robson (2002), acceptance and consent to invite, participate, and use the collected data must be granted by the intended aged user participants. Saunders et al. (2019) state that the main reasons for the gatekeeper reviewing and controlling access to research participants (in this case, the aged users' organization) are:

- To ensure that there is perceived value in research about the organization, and that it does concern the user group within the organization;
- To ensure that the topic of the research is not sensitive, and to guarantee the confidentiality of the information that would be required, in the event of confidential information being collected, to protect aged users; and
- To ensure the credibility and competence of the researcher.

The gatekeeper for the pilot group for this study was a trustee committee representative of the residential complex. The gatekeepers of the societies participating in the study comprised a pastor of the church, an administrator of the reading club, and an administrator of the cooperative.

4.9.3.1 Data collection instrument

This study used a questionnaire as data collection instrument. According to Dawson (2002), questionnaires allow for responses from a larger number of people from the population sample. Questionnaire design is dependent on the type of contact that will be made with respondents (Saunders et al., 2019). For this research about aged users, a self-administered questionnaire was used. The latter is specifically designed so that the respondent can complete it without the researcher or interviewer's assistance (Saunders et al., 2019). In this research, the questionnaire was electronically administered over the Internet (Internet-mediated questionnaires). Internet-mediated questionnaires were chosen for this study due to the consistency of the results collected from all the respondents (Saunders et al., 2019) and to better cater to respondents across multiple locations within South Africa.

According to Dawson (2002), questionnaires allow for responses from a larger number of people from the population sample. In addition, questionnaires allow for the collection of responses from many people in a study, including people who are in remote locations (Rowley, 2014). The respondents to a questionnaire are required to respond to and finish a specific set of pre-established questions (Rowley, 2014). To ensure the reliability of the data that is collected, the respondents must be able to interpret the questions in the questionnaire in the same manner; therefore, the questionnaire has to be simply and correctly worded (Rowley, 2014). Rowley (2014) further states that the effort needed to administer and complete the questionnaire will decrease when it is better worded.

Saunders et al. (2019) discuss that studies that require quantitative data collection normally use questionnaires as the suitable or appropriate data collection tool. This is due to the ability of the questionnaire to adequately present closed questions. It allows for the collection of data that is numerical and can be analysed statistically (Saunders et al., 2019).

The self-administered survey tool used for this study was standardized for the sample's senior users. The questionnaire was designed so that the respondents could not stray and give answers that went beyond the bounds of each of the questions that were asked. The respondents could only choose the best response from a list of available options to accomplish this.

The study questionnaire made use of statements that were obtained from the literature review on the constructs from UTAUT2 and the four additional constructs that were added from the literature (see Chapter 2). The questions were organized by constructs. There was a total of 53 questions for the questionnaire. In addition, a section was added for demographical details for the respondent (this did not include personally identifiable information).

Figure 4 – 4 shows the flow of the process to develop the data collection instrument.

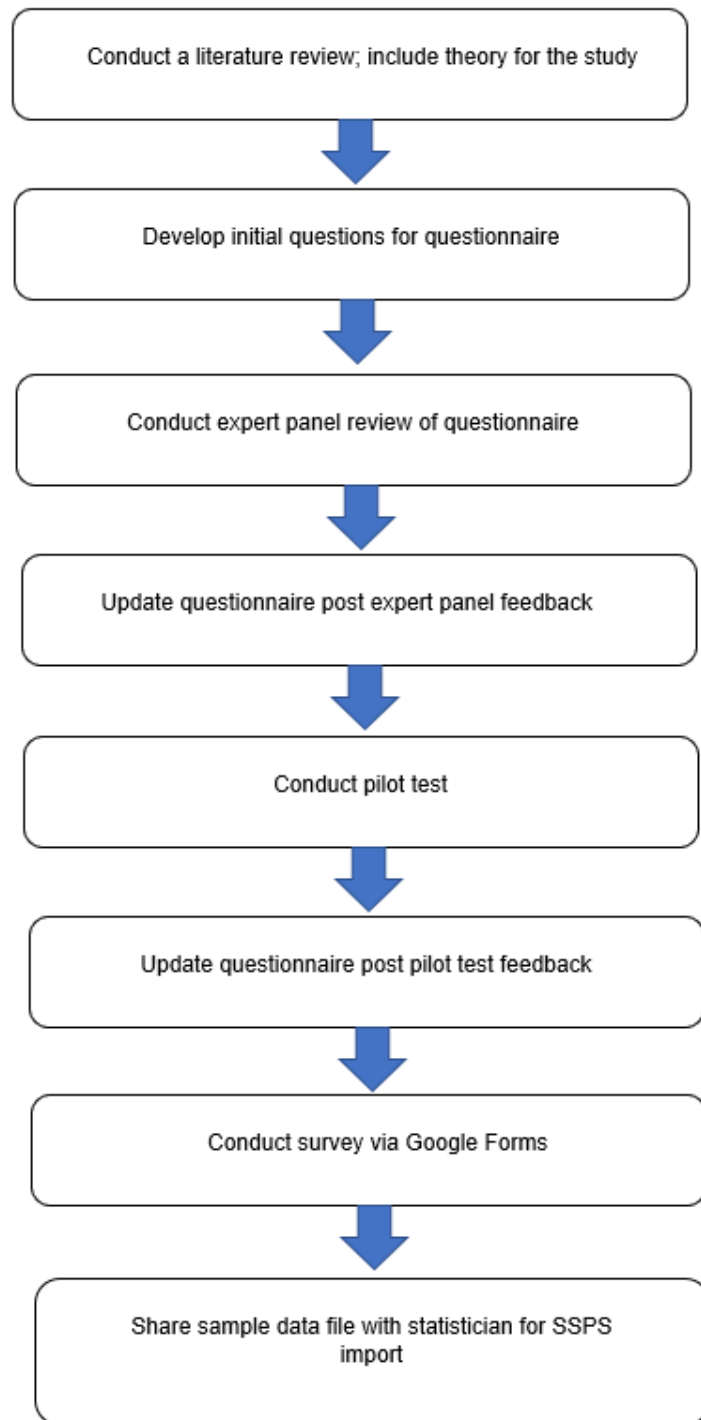


Figure 4 - 4: The questionnaire development process

4.9.3.1.1 Questionnaire design

According to Saunders et al. (2019), questionnaires are not effective in descriptive research due to the requirement that respondents answer open-ended questions. Questionnaires are preferable for analytical and prescriptive research, as with the current study, where the purpose is to investigate the factors that have a significant

influence on the perception of security for the use of mobile banking applications by aged users in South Africa and to understand the relationship between variables.

Rowley (2014) suggests that the design of a questionnaire influences the response rate of the questionnaire, as well as the reliability and validity of the data collected.

The following considerations are suggested when designing the questionnaire (Rowley, 2014; Deport & Rustenburg, 2011):

- The purpose of the questionnaire should be clearly explained;
- Questions should be divided into open and closed categories. Closed questions have a limited number of options or grading scales that can be used to respond;
- The questionnaire's questions and statements should all be written in plain language;
- The questionnaire's design needs to be organized, with no questions or statements repeated more than once;
- The amount of time needed to complete the questionnaire should be considered; and
- Pilot testing should be conducted before the final questionnaire is administered.

Using the considerations from Rowley (2014) and De Vos, Delport & Fouche (2011), the following aspects were observed during the development of the questionnaire for this study:

- The questionnaire was developed using literature and informed by UTAUT2 as a guideline;
- The questionnaire design was easy to follow and was professional;
- The layout of the questionnaire was structured into sections in a methodical format;
- Detailed and clear instructions guided the respondent on what was to be completed in each section of the questionnaire; and
- The length of the questionnaire and the duration required to complete the questionnaire by aged users were considered, without compromising on the responses provided. In this study, respondents were asked closed questions using a Likert scale to indicate how strongly they agreed or disagreed with

each of the statements made. The questionnaire was designed to take approximately **15 minutes** to complete.

The questionnaire included a summary of the study at the start to explain the study's goals and to inform the aged respondents about the confidentiality of the data gathered during the study.

The questionnaire was divided into two sections:

Section A: Demographic profile

This section comprised questions pertaining to demographic information of the respondents, such as age, level of education, experience in using mobile banking applications, cognitive abilities (difficulty remembering when using mobile banking applications, difficulty concentrating when using mobile banking applications, and visual challenges when using mobile banking applications), and the use of a proxy for banking.

Section B: Perceptions of factors that influence the security of mobile banking applications.

This section comprised questions on factors that have a significant influence on the perception of security when using mobile banking applications, as derived from the hypotheses. The section was guided by the constructs, as taken from the conceptual model in Figure 3 – 6, in which each question or statement was measured using a five-point Likert scale.

4.9.3.1.2 Questionnaire refinement

A questionnaire design process includes pre-testing, that comprises several iterations of refinement before the final questionnaire can be administered (Saunders et al., 2019). Before administering the final questionnaire, pre-testing was done through an expert panel review and a pilot review to ensure the internal reliability and validity of the questionnaire (Saunders et al., 2019).

4.9.3.1.2.1 Expert panel review

An expert panel is a small group of independent specialists from the fields included in the research study, who can offer expert opinions, insight, and input (Neuman, 2014). Saunders et al. (2019) advise that a group of experts are included before the

pilot testing phase to provide feedback on the questionnaire's appropriateness, representativeness, and suitability. According to Saunders et al. (2019), this assists with demonstrating content validity and allows the researcher to revise and update the questionnaire before pilot testing commences and before the final questionnaire is administered to the final target population.

The following process was followed for the study's expert panel review:

The expert panel had to meet a set criterion as stated in Table 4 – 4, as well as the following:

- A minimum of five experts were required. According to De et al. (2021), there is a general guideline to use 5 –15 experts for an expert panel review;
- The expert panel had to include academics as well as information security specialists;
- The experts needed to be available; and
- The experts needed to be willing to participate.

The questionnaire for the expert panel (see **Appendix D1**) was shared with each of the experts. The experts had to complete a participant consent form (see **Appendix C1**), and were provided with an expert panel participant information form (see **Appendix B1**). The expert panel questionnaire included background information for the expert, that is, the current job title, field of experience, and working years of experience.

The expert panel evaluated the questionnaire statements with respect to two aspects, namely, whether a statement is essential and whether it is clear. Experts were asked to indicate their response to the questionnaire statements in the following four columns:

- Essential;
- Not essential;
- Item is clear; and
- Item is unclear.

The expert panel did not complete the questionnaire, and statistical analyses were not conducted on the expert reviewers' answers.

i. Expert panel review participants

Table 4 – 5 shows the details of the six experts that formed the expert panel review, including the field of expertise, job title, details of experience in information security, years of working experience, and highest educational qualification.

Table 4 – 5: Expert panel review participants’ details

Expert	Field	Job title	Information security experience	Years of experience	Highest qualification
1	Information Security Operations	Information Security Risk Analyst	Conducting security risk assessments on current and new systems and applications.	6 years	BSc Honours in IT
2	Information Security Audit	Technology Risk Director	Audit experience.	20 years	MSc in Computer Science
3	Information Management	Information Specialist	Information Management, Security, and Governance at a Group level.	12 years	Honours in Information Science
4	IT Controls Assurance	Audit Partner	Information security auditing experience across multiple industries.	23 years	MSc in Computer Science

Expert	Field	Job title	Information security experience	Years of experience	Highest qualification
5	Data Analytics	Technical Architect	Designing, creating, and maintaining security systems within the financial industry.	15 years	Bachelors in IT
6	Information Security Governance	Chief Information Security Officer (CISO)	Guiding technical and non-technical teams on compliance with security policies.	31 years	Cambridge Advanced Diploma in Project Management

The expert panel reviewed the original questionnaire that was designed by the researcher (see **Appendix D1**). Each expert was contacted via email, and the questionnaire, consent, and participation information letter were shared. The feedback from the expert panel was provided electronically and shared via email with the researcher. The questionnaires for the experts included a section for comments in the demographic profile section of the questionnaire, and instructions to guide the experts on marking the questionnaire statements as essential or not essential, and clear or not clear.

ii. Expert panel review feedback

The experts reviewed Sections B and C of the expert panel questionnaire (see **Appendix D1**).

The feedback from the experts is presented in Table 4 – 6:

Table 4 – 6: Questionnaire Section B expert panel review feedback

Section B questionnaire statement	Expert panel feedback	Researcher action
Please indicate your age	<ul style="list-style-type: none"> • Update the aged user responses for the age selection from 80+ to Over 80 • Update the question to indicate that the age is in years 	<p>The response for age selection was updated as per the expert panel feedback.</p> <p>The question was updated to indicate that age was in years.</p>
Please indicate your highest level of education	None	None
Please indicate your experience using a mobile banking application	Simplify the question	The question was simplified and updated as per the expert panel feedback.
Please indicate all challenges related to using a mobile device as applicable to you	Update all the aged user responses for clarity.	The responses were updated to include 'when using a mobile banking application'.
Please indicate if you have someone authorized to conduct banking on your behalf	None	None

The actions taken by the researcher to update the demographical section (Section B) of the questionnaire with the expert panel feedback were added to Table 4 – 6.

The items that the experts identified as not essential or not clear are listed in Table 4 – 7.

The number of experts that provided feedback was added in the same line as the questionnaire item; where more than one expert provided feedback that the item was not essential or not clear, this was indicated.

Table 4 – 7: Questionnaire Section C expert panel review feedback

Section C questionnaire item	Item evaluation	Number of experts that provided evaluation	Researcher action
3	Not clear	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
5	Not clear	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
11	Not essential	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
14	Not clear	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
16	Not clear	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
18	Not clear	2	The questionnaire statement was updated for clarity.

Section C questionnaire item	Item evaluation	Number of experts that provided evaluation	Researcher action
19	Not essential	1	The questionnaire statement was adapted from a verified questionnaire (Venkatesh et al., 2012) and was therefore not updated.
30	Not clear	1	The questionnaire statement was updated for clarity.
35	Not clear	1	The questionnaire statement was updated for clarity.
36	Not clear	1	The questionnaire statement was updated for clarity.
37	Not clear	1	The questionnaire statement was updated for clarity.
43	Not clear	1	The questionnaire statement was updated for clarity.
45	Not clear	3	The questionnaire statement was updated for clarity.

Where the experts provided feedback that a questionnaire item was not essential, as per Table 4 – 7, the item was revised to better communicate the fundamentality of the statement within the construct and was updated.

Questionnaire items that were not clear, were revised and updated to provide better clarity.

However, this was only done for the questionnaire statements that were derived from literature and not for those adapted from the questionnaire of Venkatesh et al. (2012), as per the references in Section 3.3.3. This was indicated in Table 4 – 7 under the ‘researcher action’ column.

On completion of the expert review, the feedback was incorporated and the questionnaire was updated before being made available to the pilot group.

4.9.3.1.2.2 Pilot testing

This technique is used to ensure that the research data collection instrument works as intended and that the respondents fully comprehend the questions (Hilton, 2015). Saunders et al. (2019) contend that pilot testing is critical to ensure the reliability of the data as well as the validity of the questionnaire designed for the study. The level of understanding of the questionnaire's content and the justification for the questions should be tested to validate the questionnaire (Saunders et al., 2019). Rowley (2014) claims that pilot testing helps to determine whether the questionnaire is simple to understand and complete, as well as whether the questions are clear and logical. This lessens the chance of study bias (Rowley, 2014). Further, the response rate can be increased through pilot testing, and sampling errors can be minimized (Hilton, 2015).

According to Oates (2006), the pilot test can assist the researcher in identifying five issues with the developed questionnaire prior to administering it to study participants. These aspects were included in the pilot test for this study:

- The difficulties experienced by respondents in answering some of the questions;
- The identification of questions that were vague or ambiguous;
- The clarity of instructions that needed to be followed;
- The degree to which predefined responses could include all answers; and
- The accuracy of the duration needed to finish the questionnaire and respond to all the questions.

The following process was followed for the study's pilot test:

The users for the pilot test had to meet a set criterion as stated in Table 4 – 4, as well as the following:

- A minimum of 10 users were required, according to Saunders et al. (2019);
- All users needed to be at least 65 years of age;
- The aged users needed to be able to use a mobile banking application;

- The aged users needed to be available; and
- The aged users needed to be willing to participate.

The questionnaire for the pilot test (see **Appendix D2**) was shared with each of the aged users that formed part of the pilot group. In addition, the aged users had to complete a participant consent form (see **Appendix C2**) and a pilot user information form (see **Appendix B2**).

Non-probabilistic purposive sampling was used for the pilot group. The gatekeeper shared the study details with the aged users that formed the pilot testing group, including the electronic questionnaire, and interested participants were recruited by the gatekeeper. To ensure that the contact information of the aged users remained private, the gatekeeper shared the link for the electronically administered questionnaires with the 16 recruited participants. There was no direct interaction between the participants and the researcher.

Pilot group feedback

The 16 pilot group users reviewed sections A and B of the panel group questionnaire (see **Appendix D2**).

The feedback from the experts is presented in Table 4 – 8:

Table 4 – 8: Questionnaire Section A panel group feedback

Section B questionnaire statement	Pilot group feedback	Researcher action
Please indicate your age	None	None
Please indicate your highest level of education	None	None
Please indicate your experience using a mobile banking application	None	None
Please indicate all challenges related to using a mobile device as applicable to you	None	None

Section B questionnaire statement	Pilot group feedback	Researcher action
Please indicate if you have someone authorized to conduct banking on your behalf	Rephrase the statement as it is ambiguous; some aged user participants have joint accounts or secondary signatories and, therefore, have people authorized to bank on their behalf.	The question was rephrased and updated as per the pilot group feedback.

The actions taken by the researcher to update the demographical section (Section A) of the questionnaire with the panel group feedback we are indicated in Table 4 – 8.

For Section B of the questionnaire, the pilot group’s overall feedback was quite positive, with the following shared:

- The pilot participants felt at ease responding to all the questionnaire statements;
- The pilot participants did not request clarity or explanations on any of the questions; and
- The participants were advised that they were able to complete the questionnaire in under 15 minutes.

The feedback was incorporated into the questionnaire on completion of the pilot test, and the questionnaire was updated. The updated questionnaire comprised the final data collection tool for this study’s target population (see **Appendix D3**).

4.9.3.1.3 Questionnaire administration

The gatekeeper shared the study details with the aged users, including how the study could be completed. This included the option to use the electronically administered questionnaires or a printed copy of the questionnaire, depending on the aged user’s preference. Interested participants could be recruited by the gatekeeper. Where a printed copy was used, the gatekeeper stored the responses in a box in a secure area for safekeeping until they could be shared with the researcher. The

signed consent forms were kept separately from the completed questionnaires. To ensure that participants' contact information remained private, only the gatekeepers shared the link for the electronically administered questionnaires with participants.

There was no direct interaction with the participants by the researcher; only the gatekeeper interacted with the participants to identify, recruit, and send the survey link, and collected hard copy questionnaire responses where applicable. The researcher did not engage directly with the participants. No personal information was collected as part of the questionnaire, and all electronically administered and printed questionnaires were anonymous.

4.9.4 Data analysis

The data analysis process and interpretation of findings were carried out after the data collection process (Saunders et al., 2019). Quantitative research produces numerical data that can be quantified and presented in a manner that allows the researcher to answer the research questions and meet the research objectives. The quantitative data can range from frequency of occurrences to complex data counts (Saunders et al., 2019). For data to be considered useful for a study, it needs to be analysed and the results interpreted using quantitative data analysis techniques and tools. The results are presented using graphs, tables, diagrams, or charts, as such allowing for the comparison of data (Saunders et al., 2019). As a result, statistical relationships between variables can be presented visually (Saunders et al., 2019). The Statistical Packages for Social Sciences (SPSS) tool, which can analyse huge datasets, was used to analyse the quantitative data for this study.

The quantitative information gathered from the study's aged user respondents was analysed using both descriptive and inferential statistics.

This study made use of the following data analysis methods, statistics, and procedures to analyse the quantitative data, as discussed in the sections to follow:

- Factor analysis;
- Descriptive statistics; and
- Inferential statistics:
 - Structural Equation Modelling (SEM); and
 - Multiple regression analysis.

4.9.4.1 Factor analysis

Coefficients are used to show the relationship between the variables and each factor (Sreejesh et al., 2014). The resulting data is summarized so that it is readable and that the identified patterns and relationships are easy to understand (Sürücü & Maslakçi, 2020). Factor analysis can either be confirmatory or explanatory (Saunders et al., 2019). When the researcher has no expectations regarding the number or nature of the factors, Explanatory Factor Analysis (EFA) is used. This means that the researcher has to develop a theory by investigating the main variables (Taherdoost, Sahibuddin, & Jalaliyoon, 2014). EFA is one of the methods used to determine whether each question in the questionnaire loads onto the underlying theoretical framework of the construct to be measured, that is, it shows the fundamental connections between the variables being measured (Gerber & Hall, 2017).

This study used EFA as it implemented an adapted questionnaire.

Before conducting EFA, a test was run to see if it would be feasible to evaluate the statements in the questionnaire (Gerber & Hall, 2017). The Kaiser-Meyer-Olkin (KMO) test and the sampling adequacy value were used to accomplish this (Sreejesh et al., 2014). This value, which ranges from 0 to 1, measured the relationship of the statements on which EFA would be performed. If the relationship is strong, then the questionnaire statements correlate with each other and can be grouped into factors; if it is weak, the questionnaire statements do not correlate and cannot be grouped into factors (Gerber & Hall, 2017).

Table 4 – 9 shows the KMO values and the related adequacy correlation interpretations per value (Shrestha, 2021).

Table 4 – 9: KMO values and correlation adequacy

KMO value	Correlation adequacy interpretation
< 0.50	Unacceptable
0.50 – 0.59	Tolerable
0.60 – 0.69	Passable
0.70 – 0.79	Average
0.80 – 0.89	Good
> 0.90	Excellent

As per Table 4 – 9, if a KMO is of a higher value than 0.8, then it is considered of good sampling adequacy, while a KMO of a value greater than 0.9 is considered of excellent sampling adequacy.

4.9.4.2 Descriptive statistics

According to Saunders et al. (2019), descriptive statistics enables the researcher to compare and numerically describe variables. According to Field (2009), descriptive analysis uses statistical techniques to describe the data set. A variable is statistically described using the central tendency and the dispersion (Mishra et al., 2019).

Central tendency can be assessed in three different ways, and the measures of central tendency are values that are typical or average (Saunders et al., 2019).

According to Manikandan (2011), this includes:

- Computing the mode, which is the frequency of occurrence of a value within a dataset;
- Computing the median, which is the middle value in a sorted or ranked dataset; and
- Computing the mean, which is the average value of all the data values in the dataset.

The dispersion represents the distribution of the data values around the central tendency values (Mishra et al., 2019).

4.9.4.3 Inferential statistics

Inferential statistics allow a researcher to take data from a sample and make inferences about the larger population (Saunders et al., 2019). Inferential statistics therefore allow the researcher to generalize the research results. Nicholas (2010) states that hypotheses can be tested using inferential statistics.

According to Field (2009), by using inferential statistics, the researcher can ascertain how different variables relate to one another.

4.9.4.3.1 Structural equation modelling

The model was validated using Structural Equation Modelling (SEM). This is a statistical technique that allows concurrent estimation and testing of relationships that are hypothesized within a conceptual framework (Gefen, Straub, & Boudreau, 2000). SEM helps in identifying the relationships between dependent and

independent variables. Weston & Gore (2006) define SEM as a collection of statistical techniques that allow researchers to test multivariate models. The goal of SEM is partly similar to that of factor analysis, in that it attempts to provide a summary of the relationships between variables that is parsimonious (Weston & Gore, 2006). The difference between SEM and other methods, which is also an advantage of SEM, is that it allows for the estimation and testing of relationships between constructs (Hoyt, Warbasse, & Chu, 2006). SEM allows for the representation of constructs using multiple measures, unlike other general linear models, which address issues of measure-specific errors. This is critical, as it assists researchers in establishing the construct validity of factors (Hoyt et al., 2006).

According to Thakkar (2020), six steps are included in SEM, namely, data collection, model specification, identification, estimation, evaluation, and modification.

The SEM method was chosen for this study due to its suitability in elaborating theories and concepts without having to use a selection of multiple statistical methods or techniques (Tabachnick et al., 2013). In addition, the suitability of the technique when there is a transition between dependent and independent variables for behavioural intentions (Wang & Wang, 2019) made it a good fit for the study. To establish the relationships between the concepts for validating the conceptual model, SEM was applied to the factors resulting from the EFA.

4.9.4.3.2 Multiple regression analysis

To test the hypotheses, multiple regression analysis was used as the statistical technique for data analysis. It is a powerful technique that enables accurate and quantitative estimations of the effects of several different factors on an interesting variable (Fisher, 1980).

It is an extension of linear regression, which is a process that is used to predict a variable's value, whereby that value is dependent on another variable's influence (Montgomery, Peck, & Vining, 2013). The predictive variable therefore becomes the dependent variable, as it depends on another variable's influence. When two or more variables influence the value of a dependent variable, this is known as multiple regression. Regression-based data can be used to derive information, which can then be evaluated using multiple regression analysis.

Multiple regression analysis requires that assumptions are satisfied, that statistical tests are able to establish how accurate the model fits the data, and that difficulties while interpreting the results of the data are addressed. The latter are normally caused by the violation of assumptions (Mendenhall, Sincich, & Boudreau 2003). Due to its suitability for elaborating theories and concepts without requiring the use of a variety of different statistical methods or techniques, the multiple regression analysis method was chosen for this study (Tabachnick et al., 2013). In addition, the suitability of the technique when there is a transition between dependent and independent variables for behavioural intentions (Wang & Wang, 2019) made it a good fit for the study.

This study made use of the Model Summary and Coefficient tables produced as part of the multiple regression analysis. The Model summary tables were used to assess how the variance in the dependent variable is explained by the independent variables. The Coefficient tables were used to identify whether the independent variables were significant predictors of the dependent variable.

4.9.5 Data quality

4.9.5.1 Validity

According to Anastasi & Urbina (2010), a measuring instrument's validity indicates how well it can measure the things for which it is intended. Research validity is significant and reflects the calibre of a study (Saunders et al., 2019). Pilot testing should be done, according to Saunders et al. (2019), to ensure the validity of the questionnaire created for the research study; it contributes to the credibility of research. In this study, pre-testing will be done through a pilot test and an expert panel review to ensure the internal reliability and validity of the questionnaire prior to its distribution.

According to Saunders et al. (2019), there are four different types of validity: face validity, content validity, construct validity, and predictive validity. In this study, face validity, content validity, and construct validity were used; these are covered in the sections that follow, along with how they were used.

4.9.5.1.1 Face validity

The level of face validity of a questionnaire is an informal, arbitrary measurement that experts use during a pilot study to assess whether the structure of the

questionnaire makes sense (Sürücü & Maslakçi, 2020). An expert panel and a pilot group evaluated the questionnaire statements for this study, giving feedback on how well-written and understandable each statement was. The expert panel reviewed the questionnaire's statements and provided feedback on whether they were essential and clear. Following the expert panel review, the pilot group re-examined the revised questionnaire and provided feedback on whether the questions could be clearly understood. This was done before the final questionnaire was administered to the aged users that would form the sample of the target population.

4.9.5.1.2 Content validity

Bollen (1989) defined content validity as a qualitative form of validity that is used to assess whether the survey questions are indicative of the study's research goals. The validity is compromised if there is a low representation (Sürücü & Maslakçi, 2020). According to Roberts et al. (2006), content validity offers the lowest level of validity.

According to Neuman (2014), the following three steps are included in assessing content validity:

- Specify the content of the definition of a construct;
- Ensure that all parts of the definition are sampled; and
- Develop a single or more indicators from the parts of the definition.

Content validity was examined during development of the questionnaire to ensure that the claims made in the questionnaire were supported by the information in the literature review. UTAUT2 was utilized to aid in the creation of the study's questionnaire to guarantee content validity. The statements for the questionnaire were created using ideas from both the theory and the reviewed literature. Additionally, content validity was ensured by having the expert panel review the questionnaire that was created and provide feedback on whether each statement was essential, not essential, clear, or unclear.

4.9.5.1.3 Construct validity

To determine and ensure that the questionnaire matches the construct to be measured, construct validity is used (Saunders et al., 2019). According to Mathison (2005), construct validity is the degree to which deductions can be made from

theoretical constructs. One method of establishing construct validity is through factor analysis (Mathison, 2005); this method that was adopted for this study.

Factor analysis has been briefly discussed under Data analysis in Section 4.9.4.

For this study, construct validity was firstly ensured by ensuring face and content validity; according to Du Plessis (2018), these perspectives supplement an instrument's construct validity. Second, construct validity was guaranteed using Exploratory Factor Analysis (EFA).

4.9.5.2 Reliability

According to Roberts et al. (2006), reliability is the measure to which a test instrument can consistently produce the same results when repeatedly tested in the same situation. If the same results can be obtained by using the same methods, multiple times within the same circumstances, then the measurement is reliable. A questionnaire can be considered reliable if similar results are produced after repeated administration of the questionnaire (Hair et al., 2009).

The validity of quantitative research depends on reliability, which is also closely related to the calibre of the study (Taherdoost, 2016). A quantitative study is deemed invalid if the measures used in the study are unreliable. According to Saunders et al. (2019), the reliability of the questionnaire refers to whether consistent results will be obtained at the various times and circumstances under which it is completed. According to Saunders et al. (2019), the consistency of the questionnaire responses should be examined. Cronbach's Alpha coefficients were used to assess the reliability of this study (Cronbach, 1951).

According to Gerber & Hall (2017), there is a set criterion to be used to interpret the Cronbach Alpha coefficient:

- Reliability is good for a value that is above 0.8;
- Reliability is acceptable for a value between 0.6 and 0.8; and
- Reliability is unacceptable for a value that is less than 0.6.

According to Gerber & Hall (2017), the Cronbach Alpha coefficient can be increased by the number of statements in a construct, and this should be noted when interpreting the coefficient.

4.10 Research ethics

Ethical considerations are an essential part of any research process (Israel & Hay, 2006). The appropriateness of a researcher's behaviour and the rights of those who are impacted by their work are both issues that fall under the purview of research ethics (Saunders et al., 2019). Ethical issues in research are concerned with the consent to conduct the research, the public, and the community, the willingness and participation of respondents, and the process used to analyse the data once it has been collected from respondents (Saunders et al., 2019). Researchers should take note of, and adhere to, ethical considerations for all types of research conducted and across all different fields, irrespective of the research design, approach, or sampling technique. The researcher must ensure that the study is morally justifiable and methodically reasonable (Saunders et al., 2019).

Bryman & Bell (2007) define the following guidelines for conducting research:

- The researcher should request consent from the participants before advancing with the study;
- The researcher must explain in clear terms the purpose and aim of the study, and ensure that this is understood by the respondent;
- The researcher should make sure that the information regarding the study's purpose is accurate and not misrepresented, exaggerated, or falsified;
- The study respondents should be free from danger, risk, or harm;
- The researcher should ensure that the respondents remain anonymous;
- The study respondents' dignity should be upheld and not infringed upon;
- The study respondents' right to privacy should be guaranteed;
- The data collected from the respondents should be kept confidential; and
- The representation of data collected from respondents should not be biased.

Based on the guidelines, and with consideration of the requirements of UNISA's policy on Research Ethics (2016), the next section discusses the ethical considerations for this study.

4.10.1 Study conduct

The study was conducted professionally, and all communication with respondents was formal, clear, and in English; which is one of the 11 official languages of South Africa and the language of administration which is spoken throughout the country.

4.10.2 Study inclusivity

The research was conducted in a manner that is respectful to the aged people of all genders, races, religions, and cultures. There was no segregation based on economic class or status, gender, race, religion, or culture.

4.10.3 Data integrity

The study was carried out by the institution's ethical mandate to report on the study's findings in detail and honestly, without falsifying or changing the data.

4.10.4 Respondent consent

Consent was requested from the respondents before the data was collected. This was done by providing a consent letter with the questionnaire for the respondents. A check box was provided on the questionnaire for the respondents to confirm their consent (see **Appendix D**).

4.10.5 Respondent sensitive data

With the Protection of Personal Information (POPIA) Act (2021) coming into effect, it is even more critical to protect the personal information of people, especially for aged users. For this study, no personally identifiable information or sensitive data for aged users was requested from the respondents as part of the research.

4.10.6 Respondent confidentiality

On completion of the questionnaire, no link could be made between respondents and responses provided. Respondents' confidentiality was protected. Only the researchers could access confidential information gathered from respondents.

4.10.7 Respondent participation

The respondents were made aware of the fact that participation in the study was entirely voluntary. In addition, it was communicated to the respondents that they could withdraw from completing the questionnaire without repercussions, and that this exercise was entirely voluntary.

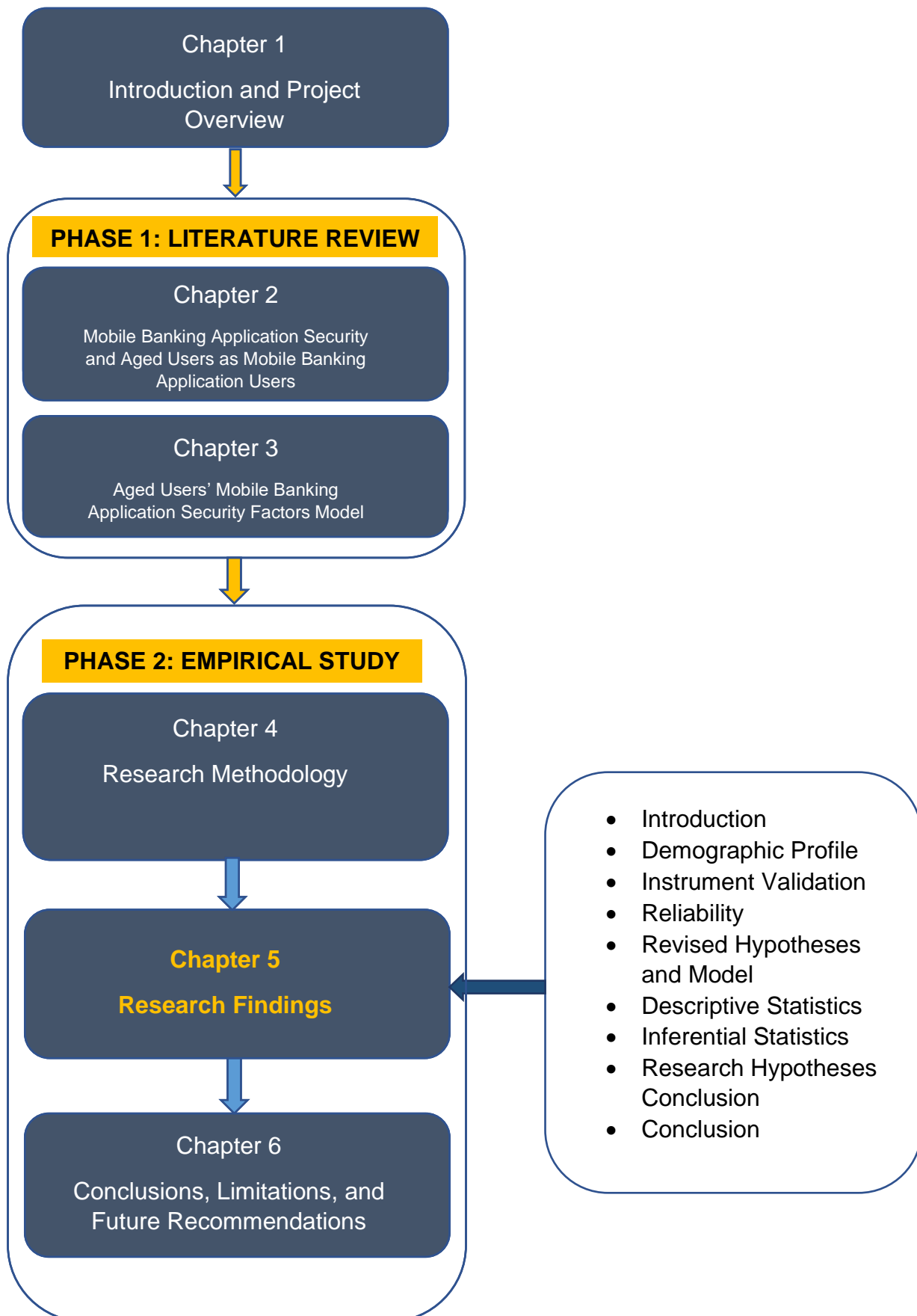
4.10.8 Research study approval and ethical clearance

An ethical clearance application was completed and submitted to the University of South Africa Research Ethics Committee to attain approval for the research to be conducted. This was submitted on the 20th of June 2023, and approval was obtained on the 28th of July 2023 from the College of Science, Engineering and Technology's School of Computing. The ethical clearance certificate is included in **Appendix A2**.

4.11 Conclusion

The research methodology used to achieve the research goals of this study is summarized in Chapter 4. The various stages of the research process were discussed, and the metaphor of an onion was used to describe the research methodology. The study's chosen research philosophy—the positivist paradigm—was discussed, and a deductive research methodology was used. For this quantitative, cross-sectional study, a survey research strategy was chosen. The chapter included information on how the questionnaire was created and subjected to pre-testing. The chapter's final section covered the study's ethical considerations presents the results and findings of the data collection process.

CHAPTER 5



RESEARCH FINDINGS

5.1 Introduction

Chapter 5 presents the findings of the empirical study and the statistical analysis of the data. This study proposed a conceptual Aged Users' Mobile Banking Application Security Factors Model in Chapter 3. The study included the collection of data from aged user respondents using a questionnaire, as per the methodology described in Chapter 4. The results of the data collection exercise are discussed in this chapter:

- The study respondents' demographic details;
- The responses to aged users' perceptions of the security of mobile banking applications questionnaire;
- The Exploratory Factor Analysis (EFA) results for the validity of the study research instrument;
- The updated hypotheses and proposed model with the new factor names;
- The Cronbach Alpha results for the internal reliability of the factors;
- The descriptive statistics for each factor; and
- The regression analysis results.

This chapter will address the following research objectives:

- To determine the reliability and validity of the questionnaire;
- To investigate the relationship between the factors that influence aged users' perception of the security of mobile banking applications; and
- To validate the Aged Users' Mobile Banking Application Security Factors Model.

5.2 Demographic profile

The study included 286 aged user respondents who completed the questionnaire. These users were from three selected aged user societies in South Africa, namely, a book club for aged users, a cooperative, and a church. All the aged user societies that participated in the study were distributed throughout South Africa.

The demographic profile section of the questionnaire comprised of questions relating to the demographic information on aged user respondents, namely, the aged users' age, level of education, experience in using mobile banking applications, and use of a proxy for banking.

5.2.1 Age distribution

Figure 5 – 1 illustrates the age distribution of respondents. Four age categories were considered in the range from 65 years to over 80 years. The largest group of respondents were aged between 65 and 70 years of age, constituting 54.2% of the study sample. The smallest group of respondents were over 80 years of age, constituting only 2.8% of the study sample.

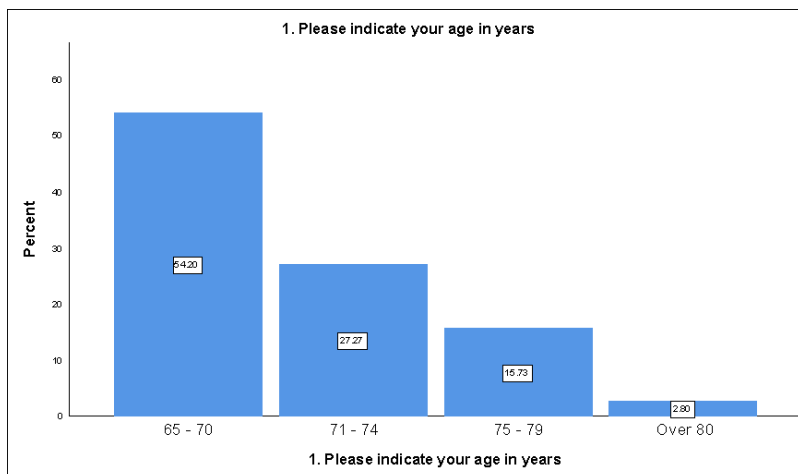


Figure 5 – 1: Age distribution (n=286)

5.2.2 Education distribution

Figure 5 – 2 illustrates the education distribution for the survey respondents. There were eight categories for respondents' highest level of education. All the respondents who captured their highest level of education had completed some level of education. The largest group of aged user respondents had a Diploma, constituting 24.5% of the study sample. The smallest group of respondents possessed a Postgraduate degree, constituting only 3.5% of the study sample. Of the total study sample, two users (0.7%) did not capture their highest level of education.

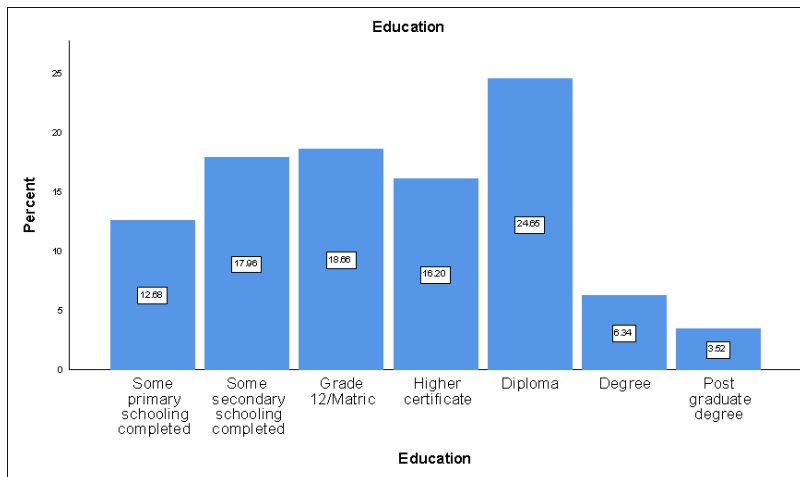


Figure 5 – 2: Education distribution (n=286)

5.2.3 Mobile banking application experience distribution

Figure 5 – 3 illustrates the distribution of the length of time or duration of experience with mobile banking applications for the survey respondents. Five categories applied. The largest group of aged user respondents have been using mobile banking applications for 3 to 5 years, constituting 47.9% of the study sample. This means that the users started making use of mobile banking applications between 2018 and 2020, which includes the time of the COVID-19 pandemic lockdown, that started in March 2020 in South Africa (Carlitz & Makhura, 2020). The smallest group of respondents had used mobile banking applications for less than six months, constituting only 2.1% of the study sample. Of the total study sample, two users (0.7%) did not capture the length of time using mobile banking applications.

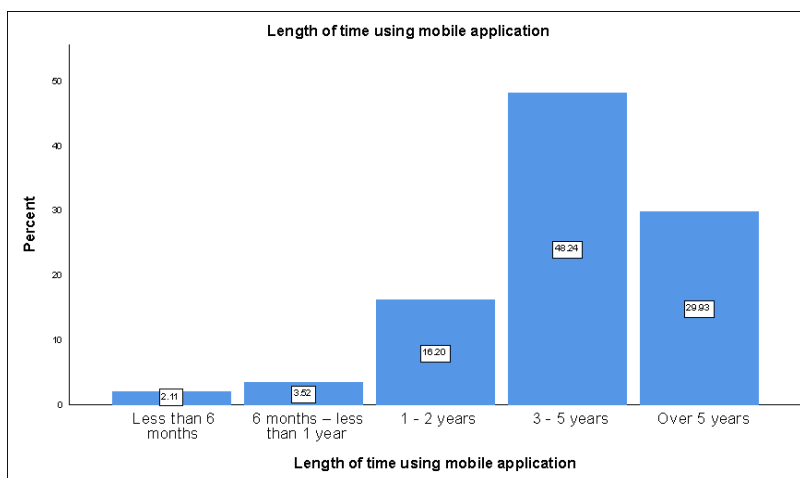


Figure 5 – 3: Mobile banking application duration distribution (n=286)

5.2.4 Proxy or assistance distribution

Figure 5 – 4 illustrates the presence of a proxy or someone authorized to assist and conduct banking on behalf of aged users on mobile banking applications. The aged user respondents had two options, either 'Yes' or 'No'. The largest group of respondents stated that they did not have anyone authorized to assist and conduct banking on their behalf on mobile banking applications, constituting 95.1% of the study sample. The smallest group of respondents did have assistance, constituting only 3.5% of the study sample. Of the total study sample, four users (1.4%) did not capture the presence or absence of someone authorized to assist and conduct banking on their behalf using the mobile banking application.



Figure 5 – 4: Mobile banking application proxy or assistance distribution (n=284)

5.2.5 Demographic profile summary

The data collected from the survey shows that the largest part of the sample was aged between 65 to 70 years (54.2%); possessing a Diploma (24.5%); had used a mobile banking application for 3 to 5 years (47.9%); and did not have proxies to assist and conduct banking on their behalf on mobile banking applications (95.1%).

5.3 Instrument validation

The validity of the questionnaire constructs was tested using EFA. The following guideline was used to determine the appropriate sample size for factor analysis (Gerber & Hall, 2017):

*Minimum number of respondents = Total number of questions in the questionnaire **

5

The study questionnaire consisted of 53 questions, excluding the demographic profile questions; therefore, a minimum of 265 respondents was required. A total of 286 respondents participated in the study, which was considered sufficient for the statistical validation of the data collection instrument.

A professional statistician was employed to assist with the statistical analysis of the data. The confidentiality agreement with the statistician is included in **Appendix F**. With the assistance of the professional statistician, the data were statistically analysed. The statistical analysis of the data was done using the SPSS Version 25 software package. The EFA statistical technique was used to examine construct validity to uncover hidden patterns in the data and to improve its capacity to be understood (Gerber & Hall, 2017). According to Gerber & Hall (2017), EFA is used to assess how well each questionnaire statement fits into the larger theoretical framework of the construct being measured, that is, the underlying relationships between the variables that are being measured (Gerber & Hall, 2017).

The Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity test (Sreejesh et al., 2014) were used to assess the suitability of the correlation matrices for factor analysis before conducting the EFA. According to Sreejesh et al. (2014), KMO values of greater than 0.8 and 0.9 indicate good and excellent sampling adequacy, respectively. According to Table 5 – 1, the KMO value of 0.94 demonstrated that the sample adequacy was excellent for carrying out EFA. Bartlett’s sphericity test revealed statistical significance ($p = 0.000$), as depicted in Table 5 – 1. Based on the results of Bartlett’s sphericity test, which required a probability of 0.05 or less, the variables were sufficiently correlated to perform EFA (Sreejesh et al., 2014). Table 5 – 1 shows the results of the Bartlett sphericity test.

Table 5 – 1: KMO and Bartlett’s Test, compiled from survey data

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.94
Bartlett’s Test of Sphericity	Approx. Chi-Square	12713.50
	df	1378
	Sig.	0.000

5.3.1 Determining the number of factors

The initial Eigenvalues and the cumulative percentage explained were used to identify the underlying factors of the variables (Gerber & Hall, 2017). The following conditions had to be met:

- The cumulative percentage explained had to be greater than 60%;
- The Eigenvalues had to be greater than 1;
- The statements must have loadings greater than 0.4; and
- Each factor should have at least three statements.

For this study, the Eigenvalues for eight factors were greater than 1, thereby suggesting that there could be eight factors that could be extracted with a cumulative Eigenvalue of 71.97%, which was greater than the required 60%.

Table 5 – 2: Eigenvalues for factors, compiled from survey data

Total Variance Explained				
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings
	Total	% of Variance	Cumulative %	Total
1	20.65	38.95	38.95	20.65
2	5.72	10.80	49.75	5.72
3	3.25	6.13	55.88	3.25
4	1.83	3.46	59.34	1.83
5	1.69	3.18	62.52	1.69
6	1.51	2.85	65.37	1.51
7	1.21	2.28	67.64	1.21
8	1.15	2.18	69.82	1.15

The factor loadings of the individual items were inspected (see **Appendix G**). According to Gerber & Hall (2017), items with factor loadings greater than 0.40 were considered, as they associate well with one another.

Following another review of the Eigenvalues in Table 5 – 2 and extracting the eight factors, a cumulative percentage of 69.82% for the eight factors was calculated.

Given that the cumulative percentage should be greater than 60%, this was adequate to proceed with the factor analysis.

A Principal Axis Factoring (PAF) extraction method was used, with a Direct Oblimin with the Kaiser Normalization rotation method; the rotation converged after 30 iterations. The makeup of the factors was determined by factor loadings (Gerber & Hall, 2017). The item loading cut-off was set at 0.4, as per Gerber & Hall's (2017) recommendation to keep items with loading values higher than 0.4.

According to Costello & Osborne (2005), items with factor loadings of more than 0.4 ought to be selected, whereas those with factor loadings lower than 0.4 ought to be disregarded. Items with factor loadings less than 0.4 might not be associated with other items, according to Costello & Osborne (2005).

According to Hair et al. (2019), items should be removed from factor analysis if the difference between the items with cross loadings, or the items with loading on more than one factor, is less than 0.2. Items with factor loadings below the established and accepted level of less than or equal to 0.4 (Hair et al., 2019) should also be deleted, as should items with larger cross-loadings, typically with a difference of more than 0.2. Table 5 – 3 shows in bold the questions that had a cross-loading on two factors. When there are cross-loadings on multiple factors, the largest loading has been retained for that factor after considering the theory underlying the factors.

The items highlighted in grey in Table 5 – 3 do not show any loading. This is because they had a factor loading that is not > 0.4 .

Table 5 – 3: Rotated pattern mix, compiled from survey data

Question	Factor							
	1	2	3	4	5	6	7	8
PS5 My interaction with mobile banking applications is secure.	0.73							
PS4 The mobile banking applications have strict security measures.	0.72							
PS2 My personal details on mobile banking applications are secure.	0.67							
PS3 My transaction details on mobile banking applications are secure.	0.67							
TT2 Mobile banking applications restrict unauthorised access.	0.66							
PS1 Mobile banking applications are secure.	0.53							
TT3 I can trust mobile banking applications to accurately process transactions.	0.51							
<i>PP4 My transaction information is protected when using mobile banking applications.</i>	0.47			-0.46				
<i>PP5 Mobile banking applications keep my private information protected.</i>	0.46			-0.45				
SI5 I have confidence in using mobile banking applications if my friends and family also use them.								
EE1 Learning how to use mobile banking applications is easy.		0.78						
EE3 Mobile banking applications are easy to use.		0.74						
EE2 My interactions with mobile banking applications are clear and understandable.		0.69						
EE4 It is easy for me to become skilful at using mobile banking applications.		0.65						
EE5 Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.		0.47						
FC2 I have the knowledge to use mobile banking applications.		0.43						
PE2 The use of mobile banking applications helps me complete banking tasks quickly.								

Question	Factor							
	1	2	3	4	5	6	7	8
FC3 Mobile banking applications are compatible with other technologies (such as mobile phones) I use.								
PE1 The use of mobile banking applications is useful in my daily life.								
PE3 The use of mobile banking applications increases my productivity.								
HB1 The use of mobile banking applications has become a habit for me.								
SI1 The people who are important to me think that I should use mobile banking applications.			0.84					
SI3 The people whose opinions that I value prefer that I use mobile banking applications.			0.83					
SI4 The people who are important to me support my use of mobile banking applications.			0.78					
SI2 The people who influence my behaviour think that I should use mobile banking applications.			0.74					
FC1 I have the resources necessary to use mobile banking applications.								
PR1 Using mobile banking applications does not put my privacy at risk.				-0.691				
PP2 Mobile banking applications provide adequate privacy protection.				-0.67				
PP1 My personal information is safe when using mobile banking applications.				-0.63				
PP3 Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.				-0.62				
PR4 There is little chance that I will lose my funds if I use mobile banking applications.				-0.61				
PR3 If I use mobile banking applications, criminals cannot attempt to take over my account.				-0.55				
PS6 There is nothing to worry about regarding the security of the mobile banking applications.				-0.49				
PR2 My funds are at no risk with the people I trust to help me use mobile banking applications.								
HB3 I must use mobile banking applications.								

Question	Factor							
	1	2	3	4	5	6	7	8
PV2 Mobile banking applications provide good value for money.					-0.69			
PV3 At the current price, the mobile banking applications provide good value.					-0.69			
PV1 Mobile banking applications are reasonably priced.					-0.63			
FC5 The financial institutions provide adequate support for using mobile banking applications.					-0.45			
FC4 I can get help from others when I have difficulties using mobile banking applications.					-0.45			
PR5 It is harmless for me to use mobile banking applications.						0.55		
UB2 I use mobile banking application for all my banking needs.						0.53		
BI2 I will always try to use mobile banking applications in my daily life.						0.40		
UB1 I regularly use mobile banking applications.								
TT1 I can trust mobile banking applications.								
HM2 Using a mobile banking application is enjoyable.							0.92	
HM1 Using a mobile banking application is fun.							0.90	
HM3 Using the mobile banking application is very exciting.							0.77	
HB2 I am addicted to using mobile banking applications.								
BI3 I plan to continue to use mobile banking applications frequently.								-0.85
BI1 I intend to continue using mobile banking applications in the future.								-0.72
UB3 I have increased my use of mobile banking applications over time.								-0.72
HB4 I have adequate experience to use mobile banking applications.								
Extraction Method: Principal Axis Factoring.								
Rotation Method: Oblimin with Kaiser Normalization.								
a. Rotation converged in 30 iterations.								

According to Hair et al. (2019), items should be removed from factor analysis if the difference between the items with cross loadings, or the items with loading on more than one factor, is less than 0.2. As indicated in bold in Table 5 – 3, two items with cross-loadings were identified:

- PP4 had a cross-loading on Factor 1 and Factor 4, with values of 0.47 and - 0.46, respectively. The difference between 0.47 and 0.46 is 0.01, therefore, this item was removed from the factor analysis.
- PP5 had a cross-loading on Factor 1 and Factor 4, with values of 0.46 and - 0.45 respectively. The difference between 0.46 and 0.45 is 0.01; therefore, this item was removed from the factor analysis. The questionnaire items and corresponding loadings obtained after the final PAF are listed in Table 5 – 4. The factor loadings are made simple and transparent by the rotating factor matrix. The resultant factors were renamed and labelled.

Table 5 – 4: Final factor names with factor loadings

Factor	Named:	Total number of items	Question	Factor Loading
1	Technological Security Perception	7	PS5	0.73
			PS4	0.72
			PS2	0.67
			PS3	0.67
			TT2	0.66
			PS1	0.53
			TT3	0.51
2	Expected Effort	6	EE1	0.78
			EE3	0.74
			EE2	0.69
			EE4	0.65
			EE5	0.47
			FC2	0.43
3	Societal Impact	4	SI1	0.84
			SI3	0.83
			SI4	0.78
			SI2	0.74
4	Privacy and Risk	7	PR1	-0.69

Factor	Named:	Total number of items	Question	Factor Loading
			PP2	-0.67
			PP1	-0.63
			PP3	-0.62
			PR4	-0.61
			PR3	-0.55
			PS6	-0.49
5	Tangible Benefits	5	PV2	-0.69
			PV3	-0.69
			PV1	-0.63
			FC5	-0.45
			FC4	-0.45
6	Risk Behaviour	3	PR5	0.55
			UB2	0.53
			BI2	0.40
7	Hedonistic Drive	3	HM2	0.92
			HM1	0.90
			HM3	0.77
8	Intent and Use behaviour	3	BI3	-0.85
			BI1	-0.72
			UB3	-0.72

All the factors make theoretical sense; they and represent the final factors that were used in the study.

5.4 Reliability

For this study, the reliability of the eight factors from the EFA was determined using Cronbach's Alpha coefficients (Cronbach, 1951). It is advantageous to attain a score above 0.7 to establish reliability (Esterhuizen & Martins, 2016). According to Gerber & Hall (2017), the Cronbach Alpha coefficient should be interpreted using a certain standard:

- Reliability is good for a value that is above 0.8;
- Reliability is acceptable for a value between 0.6 and 0.8; and
- Reliability is unacceptable for a value that is less than 0.6.

The Cronbach Alpha results for the eight factors are displayed in Table 5 – 5. The detailed statistics are included in **Appendix H**. Since all the Cronbach Alphas were higher than 0.7, all were considered to be acceptable.

Table 5 – 5: Cronbach Alpha coefficient values for the eight factors

Factor	Items	Number of items	Items omitted	Cronbach's Alpha	Reliability
Technological Security Perception	PS5, PS4, PS2, PS3, TT2, PS1, TT3	7	None	0.91	Good
Expected Effort	EE1, EE3, EE2, EE4, EE5, FC2	6	None	0.87	Good
Societal Impact	SI1, SI3, SI4, SI2	4	None	0.87	Good
Privacy and Risk	PR1, PP2, PP1, PP3, PR4, PR3, PS6	7	None	0.93	Good
Tangible Benefits	PV2, PV3, PV1, FC5, FC4	5	None	0.87	Good
Risk Behaviour	PR5, UB2, BI2	3	None	0.76	Acceptable
Hedonistic Drive	HM2, HM1, HM3	3	None	0.92	Good
Intent and Use Behaviour	BI3, BI1, UB3	3	None	0.88	Good

The eight factors' Cronbach Alpha was discovered to range from 0.76 to 0.93. This represented a high level of internal consistency.

5.5 Revised hypotheses and model

Following the finalization of the factors in Table 5 – 4, the postulated hypotheses from Section 3.3.3 and the proposed conceptual model from Section 3.3.4 were revised.

5.5.1 Final factors: revised hypotheses

The revised hypotheses were aligned with the new factor names, as follows:

H1: Expected Effort positively influences the Technological Security Perception of mobile banking applications by aged users.

H2: Societal Impact positively influences the Technological Security Perception of mobile banking applications by aged users.

H3: Privacy and Risk positively influence the Technological Security Perception of mobile banking applications by aged users.

H4: Tangible Benefits positively influence the Technological Security Perception of mobile banking applications by aged users.

H5: Hedonistic Drive positively influences the Technological Security Perception of mobile banking applications by aged users.

H6: Technological Security Perception positively influences Risk Behaviour by aged users to use mobile banking applications.

H7: Technological Security Perception positively influences Intent and Use Behaviour by aged users to use mobile banking applications.

5.5.2 Final factors: Revised conceptual model – Aged users' mobile banking application security factors model

Based on the postulated hypotheses in Section 5.4.1, the conceptual model that was previously proposed in Section 3.3.4 was updated, as per Figure 5 – 5:

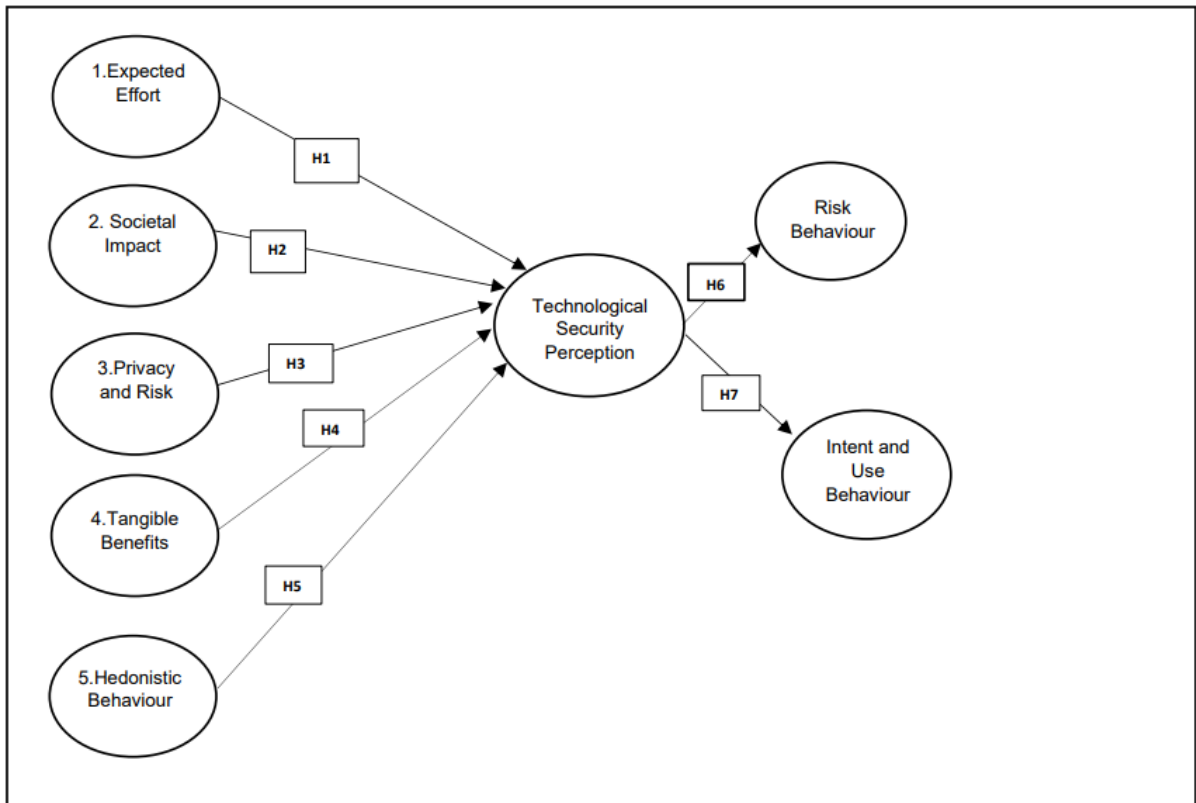


Figure 5 - 5: Final factors: Revised Conceptual Model – Aged users’ mobile banking application security factors model

5.6 Tests of normality

A test for normality was conducted to assess whether the data had a normal distribution. If the normality test is non-significant ($p > .05$), then the data is said to have a normal distribution. Field (2009) states that if the normality test returns a significant result ($p < .05$) then the data is said to not have a normal distribution.

The findings of the Shapiro-Wilk and Kolmogorov-Smirnov tests are shown in Table 5 – 6.

Table 5 – 6: Tests of Normality for the factors

Tests of Normality						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Technological Security Perception	0.223	278	0.000	0.846	278	0.000
Expected Effort	0.150	278	0.000	0.950	278	0.000
Societal Impact	0.177	278	0.000	0.830	278	0.000
Privacy and Risk	0.209	278	0.000	0.858	278	0.000
Tangible Benefits	0.210	278	0.000	0.791	278	0.000
Risk Behaviour	0.225	278	0.000	0.909	278	0.000
Hedonistic Drive	0.249	278	0.000	0.852	278	0.000
Intent and Use Behaviour	0.216	278	0.000	0.812	278	0.000
a. Lilliefors Significance Correction						

Based on the details from Table 5 – 6, the results from both tests of normality that were conducted illustrate that the data deviate from normality. However, Norman (2010) states that parametric tests can still be carried out on data that is not normally distributed when the sample set is large, as is the case for this study (n=278), with the outliers removed. Further, in large samples, it is easy for normality tests to be significant, even when deviations from normality are small.

The absence of symmetry in the normal distribution is known as skewness (Mishra et al., 2019), which is what was demonstrated in the box plots and histograms for the factors during the exploration of factor scores (see **Appendix G**). The absolute skewness was also inspected. If the skewness of the data is between -1 and 1, then the distribution is considered to be approximately normal. However, according to Mishra et al. (2019), this is not a reliable method for sample sizes that are small to moderate, as standard error decreases as the sample size increases.

A further way of identifying outliers is to calculate standardized z-scores per person (McKim, 2022).

Using -2 and 2 as the z-scores resulted in eight outliers and impacted three factors, namely Societal impact, Intent and Use Behaviour, and Tangible benefits.

This study adopted -2 and 2 as range, as it is within the acceptable scale. Any of the 286 users (n=286) that were found to have a Z-score of < -2 or > 2 were regarded as an outlier. The resulting sample, following removal of the outliers, had a sample size of 278 (n=278).

Descriptive statistics were used to describe the sample without the outliers (n=278).

5.7 Descriptive statistics

Descriptive statistics were used to outline and present the data in numerical and graphical form (Creswell & Creswell, 2018). This section discusses the mean values for the factors.

5.7.1 Means and standard deviation

The Likert scale only allowed a maximum of 5 responses: Strongly disagree (0), Disagree (1), Do not disagree or agree (2), Agree (3), and Strongly agree (4) – all the components had a maximum mean score of 4 and a minimum of 0. The mean and standard deviation values for the eight factors are displayed as descriptive statistics in Table 5 – 7. The factors have been sorted in descending order of mean value (M).

Table 5 – 7: Descriptive statistics per factor

Factor	N	Minimum	Maximum	Mean (M)	Std. Deviation
Tangible Benefits	278	1.00	4	3.52	.55
Societal Impact	278	.67	4	3.38	.58
Intent and Use Behaviour	278	.67	4	3.34	.61
Technological Security Perception	278	.00	4	3.29	.60
Privacy and Risk	278	.00	4	3.15	.65
Risk Behaviour	278	1.00	4	3.04	.59
Hedonistic Drive	278	.00	4	3.00	.89
Expected Effort	278	1.00	4	2.91	.61
Valid N (listwise)	278				

Figure 5 – 6 shows the mean values (M) for the factors, following removal of the outliers and as depicted in Table 5 – 7, in graphical form.

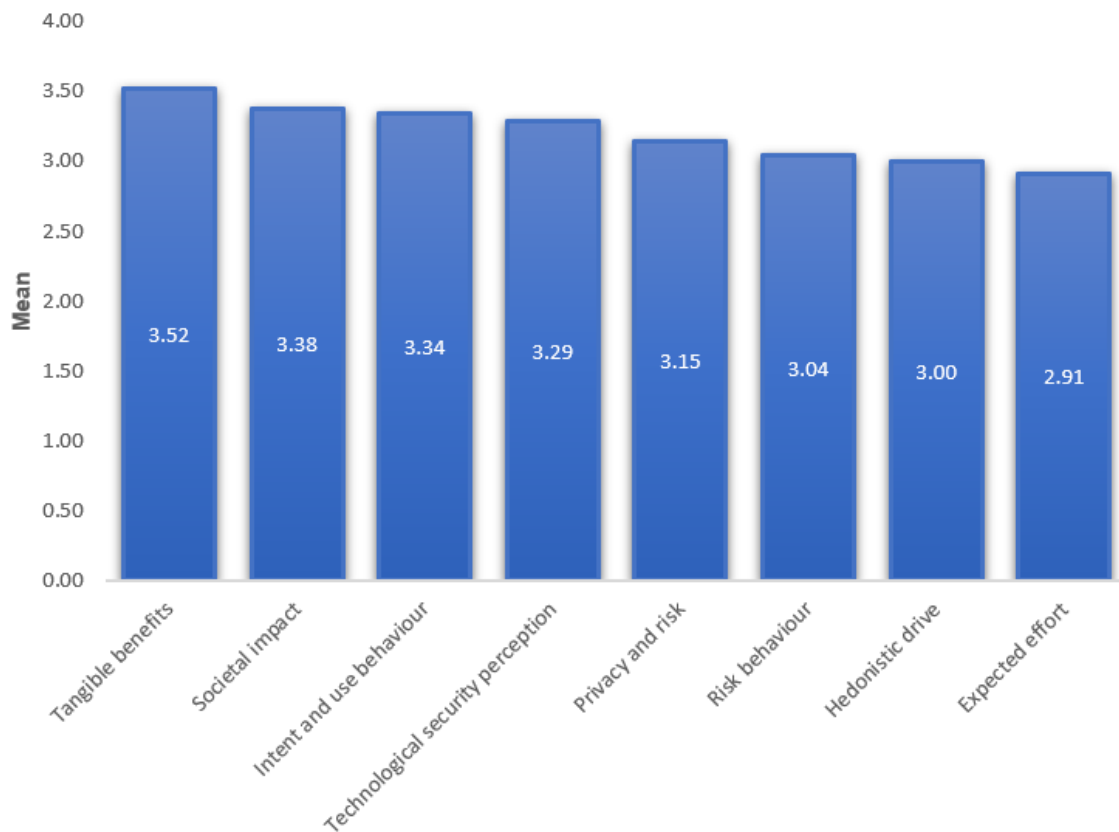


Figure 5 – 6: Descriptive statistics per factor

5.8 Inferential statistics

Inferential statistics allow the researcher to generalize the research results. Nicholas (2010) states that hypotheses can be tested using inferential statistics. According to Field (2009), it is possible to ascertain how different variables relate to one another by using inferential statistics. This analysis was therefore undertaken to derive more useful information from the data.

5.8.1 Structural Equation Modelling (SEM)

Structural equation modelling (SEM) was first used to attempt to validate the model (see **Appendix I** for results of the SEM).

Using the revised conceptual model in Section 5.4.2, the first SEM run yielded significant results (see Table 5 – 8).

Table 5 – 8: SEM Significance

Variable	Significance	Standardized coefficient
Technological Security Perception		
Expected Effort	0.000	0.14
Societal Impact	0.000	0.13
Privacy and Risk	0.000	0.78
<i>Tangible Benefits</i>	0.110	-0.07
<i>Hedonistic Drive</i>	0.724	-0.01
Cons	0.004	0.74
Risk Behaviour		
Technological Security Perception	0.000	0.60
Cons	0.000	1.85
Intent and Use Behaviour		
Risk Behaviour	0.000	0.65
Cons	0.000	2.10

According to the significance values in Table 5 – 8, tangible benefit and hedonistic drive were not significant predictors in the structural model, as $p > 0.05$.

These two variables were removed from the model, and SEM was conducted with the remaining variables. This yielded significant results for all the variables.

However, the fit indices were not acceptable, as per the SEM analysis results (see **Appendix I**).

Various modification indices were applied to improve model fit.

SEM was conducted again. The resultant model is displayed in Figure 5 – 7.

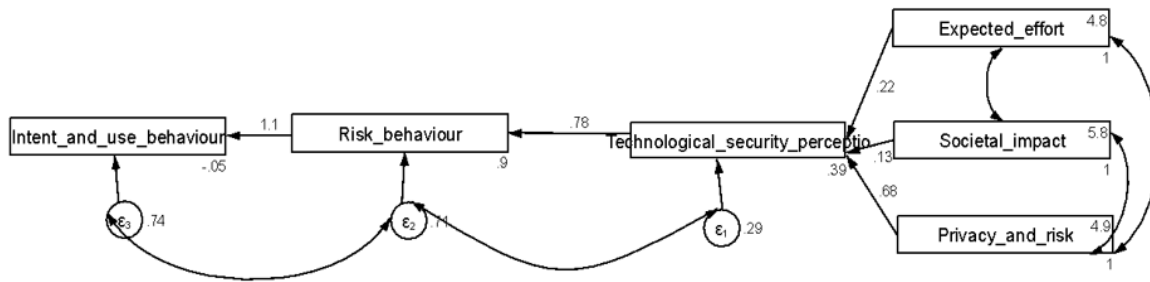


Figure 5 – 7: Resultant structural model

This model did not achieve adequate fit.

The next step in attempting to achieve a good fit was to break the model up and test it in segments. Therefore, Risk Behaviour and Intent, and Use Behaviour, were removed from the model to be tested separately. The resulting model is depicted in Figure 5 – 7.

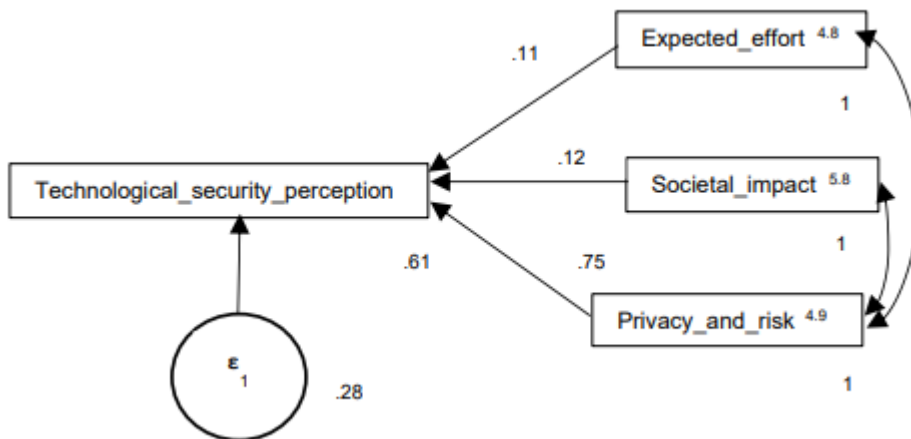


Figure 5 – 8: Derived structural model

This led to a saturated model and, while the model could be estimated, no fit indices could be calculated.

It was subsequently decided that the model be tested using multiple regression analysis, while using the approach of breaking down the model for ease of testing the variables.

5.8.2 Multiple regression analysis

Multiple regression analysis was conducted in three parts to identify the relationship between the variables:

- Technological Security Perception is considered a dependent variable, with five independent variables (expected effort, societal impact, privacy and risk, tangible benefits, and hedonistic drive);
- Risk Behaviour is considered a dependent variable, with technological security perception as an independent variable.
- Intent and Use Behaviour is considered a dependent variable, with technological security perception as an independent variable.

The results of the multiple regression analysis have been added to **Appendix J**.

5.8.4.1 Technological security perception dependent variable

One of the first assumptions of regression is the normality of residuals and the absence of multivariate outliers. This assumption was checked by looking at the histogram of residuals, as well as standardized residual values larger than an absolute value of 3. In the end, five multivariate outliers were removed, and the regression was performed on a dataset of 273. Results are reported below.

The model summary is presented in Table 5 – 9.

Table 5 – 9: Model summary – Technology security perception dependent variable

Model Summary ^b					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.87 ^a	0.75	0.75	0.28	1.92
a. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy, and risk, Expected effort, Tangible benefits					
b. Dependent Variable: Technological security perception					

According to the model summary, 75.1% of the variance in the dependent variable is explained by the independent variables – that is, the percentage that the

independent variables account for when it comes to the variation in the dependent variable.

Table 5 – 10 presents the results of the ANOVA table.

Table 5 – 10: ANOVA table – Technological security perception dependent variable

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	62.76	5	12.55	161.11	<.001 ^b
	Residual	20.80	267	0.08		
	Total	83.56	272			
a. Dependent Variable: Technological security perception						
b. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy, risk, Expected effort, Tangible benefits						

The data reported significant as per Table 5 – 10, as per the details in the ANOVA table $F(5, 267) = 161.11, p < 0.001$.

The coefficient results in Table 5 – 11 indicate whether the independent variables are significant predictors of the dependent variable. The coefficient table provides significance values, Beta coefficients, and B-coefficients.

The significance value should be $p < 0.05$ for the variable to be statistically significant. The variables that were not significant are marked in bold.

Table 5 – 11: Coefficients – Technological security perception dependent variable

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.47	0.13		3.47	0.00
	Expected effort	0.12	0.04	0.13	3.23	0.00
	Societal impact	0.12	0.03	0.12	3.65	0.00
	Privacy and risk	0.71	0.04	0.80	20.60	0.00

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
<i>Tangible benefits</i>	-0.04	0.05	-0.04	-0.77	0.44
<i>Hedonistic drive</i>	-0.01	0.02	-0.02	-0.48	0.63

The coefficients table provides data on the five independent variables, namely expected effort, societal impact, privacy and risk, tangible benefits, and hedonistic drive as per Table 5 – 11.

As depicted in Table 5 – 11, two variables, namely, tangible benefits ($p=0.44$) and hedonistic drive ($p=0.63$), are not significant as they $p > 0.05$ for both.

However, the rest of the variables for which $p < 0.05$, namely, expected effort, societal impact, and privacy and risk, are significant positive predictors of the dependent variable – Technological security perception.

The sign of the B-coefficients in Table 5 – 11 was also assessed. A positive sign indicated that, as the variable increased, so did the dependent variable. This applies to Expected effort (0.12), Societal impact (0.12), and Privacy and risk (0.71).

To compare the strength of the predictors, the Standardized Beta Coefficients were used. The largest value (0.80) for the independent variable Privacy and risk shows that it is the strongest predictor for the dependent variable, Technological security perception.

Following an assessment of the coefficients to determine whether the variables were independent, the following hypothesis statements, as per Section 5.4.1, could be verified:

H1: Expected Effort positively influences the Technological Security Perception of mobile banking applications by aged users.

The researcher had sufficient evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is rejected.

H2: Societal Impact positively influences the Technological Security Perception of mobile banking applications by aged users.

The researcher had sufficient evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is rejected.

H3: Privacy and Risk positively influences the Technological Security Perception of mobile banking applications by aged users.

The researcher had sufficient evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is rejected.

H4: Tangible Benefits positively influence the Technological Security Perception of mobile banking applications by aged users.

There was no evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is not rejected.

H5: Hedonistic Drive positively influences the Technological Security Perception of mobile banking applications by aged users.

There was no evidence to support this hypothesis based on the findings in this section (section 5.8.1). The null hypothesis is not rejected.

5.8.4.2 Risk behaviour dependent variable

The same process to identify multivariate outliers was conducted as for the Technological security perception; three outliers were removed, so that a sample size of n=275 remained.

The model summary is presented in Table 5 – 12.

Table 5 – 12: Model summary – Risk behaviour dependent variable

Model Summary ^b					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.66 ^a	0.43	0.43	0.43	1.92
a. Predictors: (Constant), Technological security perception					
b. Dependent Variable: Risk behaviour					

According to the model summary, 43% of the variance in the dependent variable is explained by the independent variables – that is, the percentage that the

independent variables account for when it comes to the variation in the dependent variable.

Table 5 – 13 presented the results of the ANOVA table.

Table 5 – 13: ANOVA table – Risk behaviour dependent variable

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	37.80	1	37.80	205.72	<.001 ^b
	Residual	50.16	273	0.18		
	Total	87.96	274			
a. Dependent Variable: Risk behaviour						
b. Predictors: (Constant), Technological security perception						

The analysis in Table 5 – 13 indicate that the data reported significant, as per the details in the ANOVA table $F(1, 273) = 205.72, p < 0.001$.

The multiple regression analysis that was conducted on the independent variable, Technological Security Perception, with the dependent variable Risk behaviour, produced the coefficients as summarised in Table 5 – 14.

As depicted in Table 5 – 14, Technological security perception was a significant positive predictor of risk behaviour ($p < 0.001$).

Table 5 – 14: Coefficients – Risk behaviour dependent variable

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.90	0.15		5.93	0.000
	Technological security perception	0.65	0.05	0.66	14.34	0.000
a. Dependent Variable: Risk behaviour						

Based on the coefficients presented in Table 5 – 14, the following hypothesis statements, as per Section 5.4.1, could be verified:

H6: Technological Security Perception positively influences Risk Behaviour by aged users in using mobile banking applications.

The researcher had sufficient evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is rejected.

5.8.4.3 Intent and Use Behaviour dependent variable

Regarding multivariate outliers, the same process as for risk behaviour was conducted; four outliers were removed, leaving a sample of size n=274.

The model summary is presented in Table 5 – 15.

Table 5 – 15: Model summary – Intent and Use Behaviour dependent variable

Model Summary ^b					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.66 ^a	0.43	0.43	0.42	1.90
a. Predictors: (Constant), Technological Security Perception					
b. Dependent Variable: Intent and Use Behaviour					

According to the model summary, 43% of the variance in the dependent variable is explained by the independent variable – that is, the percentage that the independent variables account for when it comes to the variation in the dependent variable.

Table 5 – 16 presented the results of the ANOVA table.

Table 5 – 16: ANOVA table – Intent and Use Behaviour dependent variable

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	35.98	1	35.98	206.33	<.001 ^b
	Residual	47.43	272	0.17		
	Total	83.41	273			
a. Dependent Variable: Intent and Use Behaviour						
b. Predictors: (Constant), Technological security perception						

The analysis in Table 5 – 16 indicate that the data reported significant, as per the details in the ANOVA table $F(1, 273) = 206.33, p < 0.001$.

The multiple regression analysis that was conducted on the independent variable, Technological Security Perception, with the dependent variable Intent and Use Behaviour, produced the coefficients outlined in Table 5 – 17.

As depicted in Table 5 – 17, Technological Security Perception was a significant positive predictor of Intent and Use Behaviour ($p < 0.001$).

Table 5 – 17: Coefficients – Intent and Use Behaviour dependent variable

Coefficients ^a					
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
1 (Constant)	1.223	0.152		8.066	0.000
Technological Security Perception	0.650	0.045	0.657	14.364	0.000

a. Dependent Variable: Intent and Use Behaviour

Based on the coefficients presented in Table 5 – 17, the following hypothesis statements, as per Section 5.4.1, could be verified:

H7: Technological Security Perception positively influences Intent and Use Behaviour by aged users to use mobile banking applications.

The researcher had sufficient evidence to support this hypothesis based on the findings in this section (Section 5.8.1). The null hypothesis is rejected.

5.9 Research hypotheses conclusion

Table 5 – 18 summarizes the research hypotheses, as per Section 5.8, and lists the conclusions regarding whether each hypothesis is supported, considering the findings of the empirical research.

Table 5 – 18: Research hypotheses conclusion

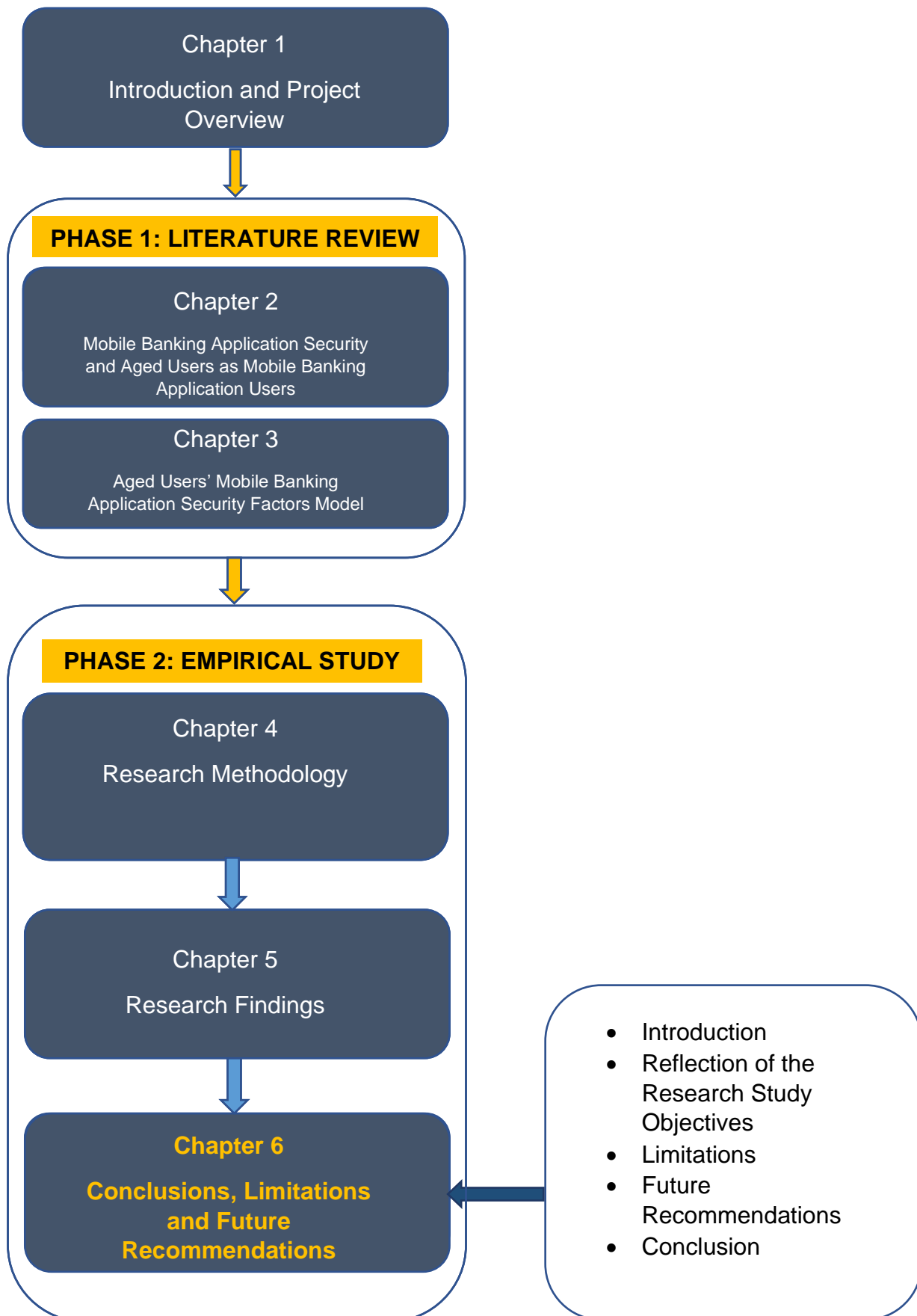
Research hypothesis	Hypothesis acceptance status
H1: Expected Effort positively influences the Technological Security Perception of mobile banking applications by aged users.	Supported
H2: Societal Impact positively influences the Technological Security Perception of mobile banking applications by aged users.	Supported
H3: Privacy and Risk positively influences the Technological Security Perception of mobile banking applications by aged users.	Supported
H4: Tangible Benefits positively influences the Technological Security Perception of mobile banking applications by aged users.	Not supported
H5: Hedonistic Drive positively influences the Technological Security Perception of mobile banking applications by aged users.	Not supported
H6: Technological Security Perception positively influences Risk Behaviour by aged users to use mobile banking applications.	Supported
H7: Technological Security Perception positively influences Intent and Use Behaviour by aged users to use mobile banking applications.	Supported

5.10 Conclusion

This research aims to create an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications by investigating the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa. This chapter addressed three of the research objectives regarding the reliability and validity of the questionnaire as research instrument.

The questionnaire was used to collect data from 286 aged user participants in South Africa, and EFA was used to test the validity of the research instrument. A total of eight factors were derived, namely, Technological Security Perception, Expected Effort, Societal Impact, Privacy and Risk, Tangible Benefits, Risk Behaviour, Hedonistic Drive, and Intent and Use Behaviour. The previously postulated hypotheses were revised based on the new factor names, and a new model was created. Cronbach's Alpha was used to assess the internal reliability of the factors. Structural Equation Modelling was done to test the model, together with multiple regression analysis to test and validate the hypotheses. Chapter 6 presents the conclusions, limitations, and recommendations for future work.

CHAPTER 6



CONCLUSIONS, LIMITATIONS, AND FUTURE RECOMMENDATIONS

6.1 Introduction

Chapter 6 presents a reflection on the study. It draws conclusions based on the literature review and the empirical study that was conducted on the factors that influence aged users' perception of the security of mobile banking applications in South Africa. These conclusions are presented and discussed with reference to the study objectives. The limitations identified for the literature review and the empirical study are also discussed. Recommendations are made that could inform the design of secure mobile banking applications, through the proposed Aged Users' Mobile Banking Application Security Factors Model.

This chapter addresses the following research objectives:

- To suggest recommendations for secure mobile banking applications for aged users, based on the Aged Users' Mobile Banking Application Security Factors Model.

6.2 Reflection of the research study objectives

This study aimed to create an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications, by investigating the factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa.

Data was collected by means of a questionnaire from willing and available aged users in South Africa who made use of mobile banking applications.

The aim of the study was addressed by answering the study research questions, where each research question was associated with one or more research objectives. The study was conducted in two phases, namely, a literature review for the development of the conceptual model of the security factors for aged users, and a regression analysis to validate the proposed model.

The research questions and objectives are outlined in Sections 1.4 and 1.5.2, respectively. Table 1 – 1 shows the link between the research questions and the associated objectives.

This section discusses the conclusions made concerning the research questions and the associated objectives.

6.2.1 Research questions

The main research question was answered through sub-questions, as was outlined in Section 1.4; these sub-questions will be discussed in this section.

6.2.1.1 a) What are the factors that influence aged users' perception of the security of mobile banking applications?

The research objectives linked to this research question are discussed, along with how the research question was answered in support of the research objectives.

6.2.1.1.1 To analyse literature for factors that influence the aged users' perception of the security of mobile banking applications

A scoping literature review was conducted, as reported in Chapter 3, and a list of factors on the security of mobile banking applications for the aged was identified (see Table 3.2.5). A total of 27 distinct factors were identified from the literature. The study adopted UTAUT2 to inform the proposed model as numerous industries, including mobile banking, have made extensive use of and validated UTAUT2 (Alalwan et al., 2017; Merhi et al., 2019; Aldiabat et al., 2019). However, Wechuli et al. (2017) identified that UTAUT2 lacks concepts essential to the use of technology; therefore, the study did not extend UTAUT2 but only used UTAUT2 to inform the research.

The 27 factors derived from the literature were mapped across existing UTAUT2 constructs, based on the definition of the constructs in the context of the study. Some of the factors could not be mapped to the existing constructs of UTAUT2. Therefore, four new additional constructs were developed. The final factor list included Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Hedonic Motivation, Price Value, Habit, Perceived Privacy, Technological Trust, Perceived Risk, and Perceived Security.

6.2.1.1.2 To develop the Aged Users' Mobile Banking Application Security Factors Model of the factors that influence aged users' perception of the security of mobile banking applications

The theoretical framework for the study was selected, and the study was informed by UTAUT2. Once the study constructs had been identified (see Section 3.3.2), the hypotheses were postulated based on the literature that had been reviewed. The hypotheses were developed to help address the main research question, and are included for each construct under Section 3.3.3. The identified constructs are Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions, Hedonic Motivation, Price Value, Habit, Perceived Privacy, Technological Trust, Perceived Risk, Perceived Security, Behavioural Intention, and Use Behaviour.

The following hypotheses were postulated:

H1: Performance Expectancy positively influences the Perceived Security of mobile banking applications by aged users.

H2: Effort Expectancy positively influences the Perceived Security of mobile banking applications by aged users.

H3: Social Influence positively influences the Perceived Security of mobile banking applications by aged users.

H4: Facilitating Conditions positively influences the Perceived Security of mobile banking.

H5: Hedonic Motivation positively influences the Perceived Security of mobile banking applications by aged users.

H6: Price Value positively influences the Perceived Security of mobile banking applications by aged users.

H7: Habit positively influences the Perceived Security of mobile banking applications by aged users.

H8: Perceived Privacy positively influences the Perceived Security of mobile banking applications by aged users.

H9: Technological Trust positively influences the Perceived Security of mobile banking applications by aged users.

H10: Perceived Risk positively influences the Perceived Security of mobile banking applications by aged users.

H11: Perceived Security positively influences Behavioural Intention by aged users to use mobile banking applications.

H12: Behavioural Intention to use mobile banking applications positively influences actual Use Behaviour of mobile banking applications.

The conceptual Aged Users' Mobile Banking Application Security Factors Model was proposed in Section 3.3.4.

6.2.1.1.3 To develop a questionnaire based on the Aged Users' Mobile Banking Application Security Factors Model

To be able to respond to the research sub-questions, the first step in the questionnaire design process was to develop the questionnaire statements from each of the chosen study constructs. The study questionnaire was developed in Chapter 3, and was informed by UTAUT2 as well as by literature. The statements for the questionnaire were created using statements and ideas from both the theory and the reviewed literature, as outlined in Section 3.3.3. UTAUT2 was utilized to aid in the creation of the study's questionnaire to guarantee content validity. Before administering the final questionnaire, pre-testing was done through an expert panel review and a pilot review to ensure the internal reliability and validity of the questionnaire (Saunders et al., 2019). The construct validity and reliability of the questionnaire were evaluated with an Exploratory Factor Analysis (EFA) (Mathison, 2005). The questionnaire was designed so that a summary of the study was given at the start to explain its goals and to inform the older user respondents about the confidentiality of the data gathered during the study (Rowley, 2014). The product was the close-ended questionnaire that made use of a 5-point Likert scale, which was shared with the aged users. The various gatekeepers presented aged users with an online survey link, while users who decided not to take the electronically delivered survey were given printed copies.

6.2.1.2 b) What is the relationship between the factors influencing aged users' perception of the security of mobile banking applications?

The research objectives linked to this research question are discussed, along with how the research question was answered using the research objectives.

6.2.1.2.1 To determine the reliability and validity of the questionnaire

The administration of the research instrument was presented in Chapter 4. Before the survey could commence, the University had to grant Ethical Research Clearance. Once this had been obtained, the research instrument (questionnaire) was administered in the form of an electronic and physical copies to three organizations in South Africa for aged user participants to complete. A participant information sheet and a consent request from the aged user participant to conduct the research were included. A total of 286 respondents completed the questionnaire during the three-week data collection period, and the data was used for statistical analysis. The final analysis was conducted on a data set of $n=278$ following the removal of outliers.

This statistical analysis was presented in Chapter 5. EFA was done to determine the validity of the questionnaire; this resulted in eight factors being yielded, namely:

i. Independent variables

- Technological Security Perception
- Expected Effort
- Societal Impact
- Privacy and Risk
- Tangible Benefits
- Hedonistic Drive

ii. Dependent variables

- Risk Behaviour
- Intent and Use Behaviour

Cronbach's Alpha was calculated to determine the reliability of the factors, all of which yielded good reliability, thereby indicating that the questionnaire had a high level of internal consistency.

6.2.1.2.2 To investigate the relationship between the factors that influence aged users' perception of the security of mobile banking applications

The hypotheses were revised in line with the eight new factors, as presented in Section 5.5.1. The revised hypotheses are:

H1: Expected Effort positively influences the Technological Security Perception of mobile banking applications by aged users.

H2: Societal Impact positively influences the Technological Security Perception of mobile banking applications by aged users.

H3: Privacy and Risk positively influences the Technological Security Perception of mobile banking applications by aged users.

H4: Tangible Benefits positively influences the Technological Security Perception of mobile banking applications by aged users.

H5: Hedonistic Drive positively influences the Technological Security Perception of mobile banking applications by aged users.

H6: Technological Security Perception positively influences Risk Behaviour by aged users to use mobile banking applications.

H7: Technological Security Perception positively influences Intent and Use Behaviour by aged users to use mobile banking applications.

To investigate the relationship between the factors, the study made use of multiple regression analysis. Achievement of this objective is documented in Section 5.8.1 of Chapter 5. Multiple regression analysis produced a Coefficient table that was used to compare the strength of the predictors.

As depicted in Section 5.8.1, expected effort, societal impact, and privacy and risk were significant positive predictors of the dependent variable – technological security perception. Privacy and risk showed that it is the strongest predictor for the dependent variable, technological security perception. Tangible Benefits and Hedonistic Drive were not significant.

Technological security perception was a significant positive predictor of Risk Behaviour.

Technological security perception was a significant positive predictor of Intent and Use Behaviour.

6.2.1.3 c) What are the factors that must be considered when designing secure mobile banking applications that are used by aged users in South Africa?

The research objectives linked to this research question are discussed, along with how the research question was answered using the research objectives.

6.2.1.3.1 To validate the Aged Users' Mobile Banking Application Security Factors Model

To validate the Aged Users' Mobile Banking Application Security Factors Model, the study made use of SEM, followed by multiple regression analysis. This process of achieving this objective was described in Section 5.8 of Chapter 5. Structural equation modelling (SEM) was first used to attempt to validate the model.

The first SEM run identified that tangible benefits and hedonistic drive were not significant predictors in the structural model. Modification indices were applied, and the model still did not achieve adequate fit. The model was tested in segments to try and achieve a good fit, which led to a saturated model.

It was then suggested that the model be validated using multiple regression analysis, by adopting the same segments for ease of testing. Using the coefficients results of the multiple regression analysis, the revised hypotheses for the study, as per Section 5.4.1 in Chapter 5, could be verified.

After conclusion of the revised research hypothesis in Chapter 5, Section 5.9, the final model is indicated in Figure 6 – 1.

A conceptual Aged Users' Mobile Banking Application Security Factors Model had been proposed in Chapter 3, Section 3.3.4, based on the literature reviewed.

Figure 6 – 1 depicts the final validated Aged Users' Mobile Banking Application Security Factors Model.

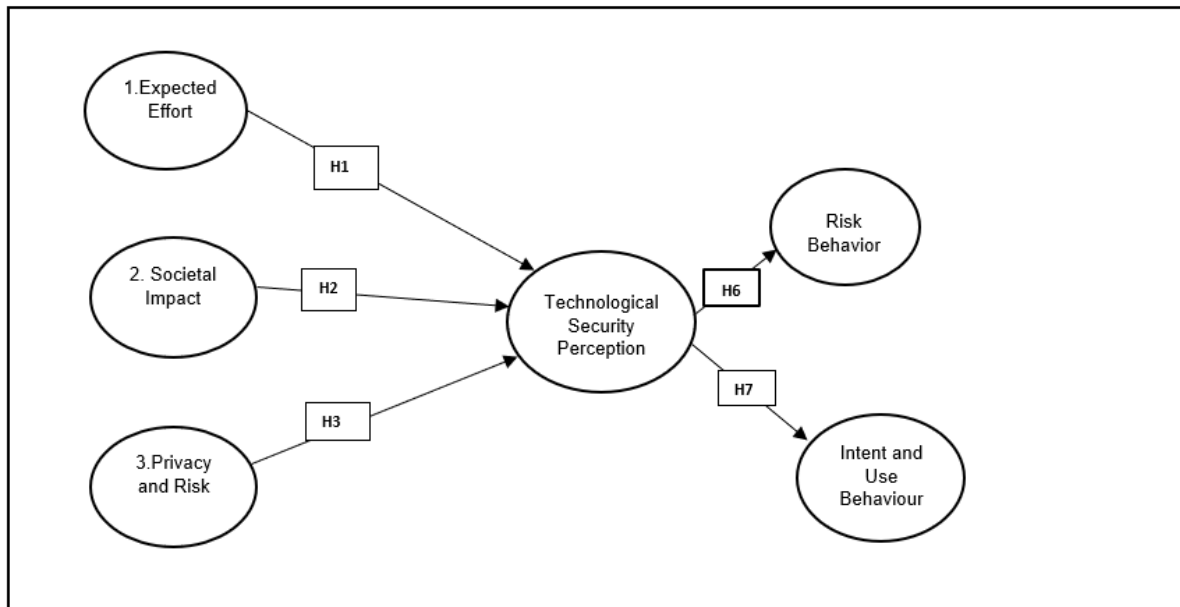


Figure 6 – 1: Final validated Aged Users' Mobile Banking Application Security Factors Model

6.2.1.3.2 To suggest recommendations for secure mobile banking applications for aged users, based on the Aged Users' Mobile Banking Application Security Factors Model

The recommendations for financial institutions have been discussed in detail in Section 6.4.1.

- Privacy and risk are the most likely factor to influence the technological security perception of aged users. This means that financial institutions should incorporate measures that provide improved privacy and minimize risk for aged users. This is the most important of the identified factors.
- Societal impact is the second most likely factor to influence the technological security perception of aged users. This means that financial institutions should direct marketing efforts for mobile banking applications to not just aged users, but also to social media and communities that support aged users.
- Expected effort is the third and least likely factor to influence the technological security perception of aged users. This means that financial institutions should design mobile banking applications that can recognize an aged user login, and simplify the view and available functions based on that. The aged user will still have the option to use the full mobile banking application view, but the simplified view will require less effort.

The consequences of the research findings are perceived to be important in guiding financial institutions to better design mobile banking applications that are secure and easy to use by aged users. This will result in aged users in South Africa becoming more digitally and socially included in banking trends.

6.3 Limitations

The following limitations were identified as they affect the generalizability of the findings of the study, and should be taken into consideration when the research findings are interpreted:

- There was limited research available within a South African context for the factors on the security of mobile banking applications for the aged. The list of factors used for the study was derived from 15 different countries, none of which included South Africa, as such highlighting the lack of research done within a South African context.
- The study was conducted with three organizations, with the data mostly collected through electronically administered questionnaires from a total of 286 respondents. A bigger sample size would have been more representative of aged users' perceptions of the factors that impact the security of mobile banking applications. In addition, it would have resulted in a reduced sampling error (Visser et al., 2013). The study sample is not representative of all aged users' perceptions of the factors that impact the security of mobile banking applications in South Africa. Therefore, the results from this study cannot be generalized to all aged users.
- The convenience sampling strategy used in this study resulted in limitations to the conclusions that could be made from the data. According to Hallam & Zanella (2017), convenience sampling is not known to be representative, and there may therefore be concerns regarding external validity.
- The study employed a cross-sectional time horizon design, which is not ideal for aged users' perceptions of the factors that impact the security of mobile banking applications, as they may change with time.
- The study adopted a quantitative research methodology to gather data on aged users' perceptions of the factors that impact the security of mobile banking applications. However, a qualitative method, using interviews as data

collection instrument, may have been used to gain a better grasp of the perceptions of aged users.

6.4 Future recommendations

Recommendations for future research have been made based on the findings from the research after the statistical analysis, the conclusions drawn, and the limitations identified.

6.4.1 Recommendations for financial institutions

The recommendations for financial institutions are:

- The results in Table 5 – 11 indicate that privacy and risk (Standardized Beta Coefficients=0.80) is the strongest predictor for the dependent variable, technological security perception. Johnson et al. (2020), who report that privacy and risk concerns were found to impede the adoption and usage of mobile banking technologies, support this. According to Cham et al. (2021), older users are more likely to use mobile banking applications and perceive the mobile banking experience as secure when there is less chance of privacy loss. This means that financial institutions should prioritize how personal information can be kept safe and not compromised for aged users of mobile banking applications, and how this is factored into the design of mobile banking applications. Aged users need to be aware, convinced of, and comfortable with the privacy of mobile banking applications. In addition, financial institutions should implement preventative risk measures to safeguard aged users and to protect against the potential loss that an aged user can suffer while trying to attain a specific desired outcome while using a mobile banking application. This can be achieved using a diligent authentication process when aged users have people or proxies to assist them with banking needs to minimize perceived risk. This is in line with Balcerzak et al. (2017), who state that applications for aged users should include security measures to support aged users' use of the mobile banking application. A diligent account access review process can also be implemented to review the use of, and access to, aged users' mobile banking applications, together with the authentication process to restrict unauthorized access. Financial institutions can also advise aged users that the data is

sensitive and can compromise the user's privacy or expose them to risk on the mobile banking applications through visible, simple, and better wording of such data on the mobile banking application.

- The results in Table 5 – 11 indicate that expected effort is the second strongest predictor (Standardized Beta Coefficients=0.13) for the dependent variable, technological security perception. Saukkonen et al. (2022) supports this, as they state that the required effort to use mobile banking applications is reduced if the mobile banking applications are simple, easy to access, and used securely without complexities for aged users. Financial institutions should design mobile banking applications that are easy to use and require minimal effort to use securely and effectively. The mobile banking application's interface should cater to aged users, as legibility challenges can be higher with the aged, which results in a cluttered interface that is difficult to navigate and requires more effort from aged users. This is in line with Sarcar et al. (2017), who suggest that mobile banking applications that are legible for aged users require less effort to use. Financial institutions should also simplify and make the authentication process more visible and easier to understand for aged users, as complex authentication mechanisms on mobile banking applications, especially when they do not cater to aged users' decline in cognitive ability, end up requiring that the aged user invests a significant amount of effort towards understanding the application. Iqbal et al. (2020) found that simplification of these complex mechanisms results in less effort and a secure mobile banking experience for aged users. Management of settings on mobile banking applications should also require minimal effort for aged users, such as enabling push notifications, or general management of security mechanisms on the mobile banking application. This can be achieved by building mobile banking applications that can identify a user's age and simplify the view for the aged user, with the option to switch to the mobile banking application's full view if required. The simplified view can offer the basic functions that the aged user conducts on the mobile banking application, and the reduced clutter and functions will require less effort to navigate.

- The results in Table 5 – 11 indicate that societal impact is the third strongest predictor (Standardized Beta Coefficients=0.12) for the dependent variable, technological security perception. This is supported by Latulipe et al. (2022) and Cham et al. (2021), who found that support by society plays an important role in influencing aged users' understanding of security and use of mobile banking applications. This means that financial institutions should publicize the use of mobile banking applications in a manner that targets not only the users of the mobile banking applications (i.e., aged users), but also the social network or community that are close or important to aged users. Aged users lean on the support of the people around them, and feedback from this community impacts the decisions that aged users make, particularly concerning the use of mobile banking applications. Financial institutions need to create awareness of the use and benefits of mobile banking applications through advertising that is inclusive and accessible, to cater to the social network and community of aged users.

6.4.2 Recommendations for future research

The recommendations for future research are:

- The study can be extended to include qualitative research to enhance the clarity of facts, as it investigates factors that have a significant influence on the perception of security for the use of mobile banking applications by aged users in South Africa. According to Creswell & Creswell (2018), qualitative research allows for a better understanding of how users feel about a phenomenon, and this can be achieved using interviews. The study can also adopt a mixed methods approach, making use of both quantitative and qualitative approaches to leverage their respective advantages and strong points.
- The survey can be conducted for a bigger sample across South Africa, with the questionnaire further validated.
- The impact of moderating factors such as age, education, and experience in using a mobile banking application, and the use of a proxy can be measured against the security factors to assess how each of the moderators would modify the relationship between the variables. According to the literature that was reviewed, these characteristics have an impact on aged users'

perceptions of the factors that impact the security of mobile banking applications, and would provide further insights and understanding of the data collected from aged users.

6.5 Conclusion

This chapter reflected on the study, through conclusions drawn from the literature reviewed and from the empirical study conducted on the factors that influence aged users' perception of the security of mobile banking applications in South Africa.

The chapter presented the limitations of the study. It outlined practical recommendations for financial institutions and pointed to areas for future research. The chapter also provided the final and validated Aged Users' Mobile Banking Application Security Factors Model, which could inform the design of secure mobile banking applications for aged users.

LIST OF REFERENCES

- Afshan, S. and Sharif, A. (2016). Acceptance of mobile banking framework in Pakistan. *Telematics and Informatics*, 33(2), pp.370–387.
<https://doi.org/10.1016/j.tele.2015.09.005>.
- Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes*, 50(2), pp.179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T).
- Alalwan, A.A., Dwivedi, Y.K., and Rana, N.P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, 37(3), pp.99–110.
- Aldiabat, K., Al-Gasaymeh, A., and K.Rashid, A.S. (2019). The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry. *International Journal of Interactive Mobile Technologies (IJIM)*, 13(02), p.37.
<https://doi.org/10.3991/ijim.v13i02.9262>.
- Al-Jabri, I.M. and Sohail, M.S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research*, 13(4), pp.379–391.
- Altawalbeh, S.M., Alkhateeb, F.M., and Attarabeen, O.F. (2019). Ethical issues in consenting older adults: academic researchers and community perspectives. *Journal of Pharmaceutical Health Services Research*, 11(1), pp.25–32.
<https://doi.org/10.1111/jphs.12327>.
- Amin, A., Ul Haq, I. and Nazir, M. (2017). Two factor authentication. *International Journal of Computer Science and Mobile Computing*, [online] 6(7), pp.5–8. Available at: <<https://ijcsmc.com/docs/papers/July2017/V6I7201707.pdf>> [Accessed 25 Jan. 2023].
- Anastasi, A. and Urbina, S. (2010). *Psychological testing*. New Delhi: Phi Learning Private Limited.

Apau, R. and Koranteng, F.N. (2019). Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behaviour. *International Journal of Cyber Criminology*, 13(2), pp.228–254. <https://doi.org/10.5281/zenodo.3697886>.

Arksey, H. and O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), pp.19–32. <https://doi.org/10.1080/1364557032000119616>.

Asp, E., Manzel, K., Koestner, B., Cole, C., Denburg, N., and Tranel, D. (2012). A Neuropsychological Test of Belief and Doubt: Damage to Ventromedial Prefrontal Cortex Increases Credulity for Misleading Advertising, *Frontiers in Neuroscience*, 9(6), pp.1–9.

Assensoh-Kodua, A., Migiro, S., and Mutambara, E. (2016). Mobile banking in South Africa: A systematic review of the literature. *Dut.ac.za*. [online] Available at: <<http://ir.dut.ac.za/handle/10321/2275>> [Accessed 12 September 2022].

Babbie, E. R. (2021). *The practice of social research*, 15th ed. S.L.: Cengage Learning, AU.

Balcerzak, B., Kopec, W., Nielek, R., Kruk, S., Warpechowski, K., Wasik, M., & Węgrzyn, M. (2017, September). Press F1 for help: participatory design for dealing with on-line and real life security of older adults. In *2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)* (Vol. 1, pp. 240-243). IEEE; Lviv, Ukraine. <https://doi.org/10.1109/stc-csit.2017.8098778>.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall

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

Baumann, F. (2021). The Next Frontier—Human Development and the Anthropocene: UNDP Human Development Report 2020. *Environment: Science and Policy for Sustainable Development*, [online] 63(3), pp.34–40. <https://doi.org/10.1080/00139157.2021.1898908>.

Bhatiasevi, V. (2016). An extended UTAUT model to explain the adoption of mobile banking. *Information Development*, 32(4), pp.799–814.

Bhattacharyya, D., Ranjan, R., Alisherov, F., and Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3), pp.13–28.

Bollen, K.A. (1989). The Consequences of Measurement Error. *Structural Equations with Latent Variables*. pp.151–178. <https://doi.org/10.1002/9781118619179.ch5>.

Brocklehurst, H. and Laurenson, M. (2008). A concept analysis examining the vulnerability of older people. *British Journal of Nursing*, 17(21), pp.1354–1357.

Bryman, A. (2016). *Social Research Methods*. 5th ed. Oxford: Oxford University Press.

Bryman, A. and Bell, E. (2007). *Business research methods*. 2nd ed. Oxford, Oxford University Press; New York: Oxford University Press.

Carlitz, R.D. and Makhura, M.N. (2020). Life Under Lockdown: Illustrating Tradeoffs in South Africa's Response to COVID-19. *World Development*, p.105168. <https://doi.org/10.1016/j.worlddev.2020.105168>.

Carter, W. and Zheng, D. (2015). *The Evolution of Cybersecurity Requirements for the U.S. Financial Industry*. [online] Available at: <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf> [Accessed 18 Jun. 2022].

Cham, T.-H., Cheah, J.-H., Cheng, B.-L., and Lim, X.-J. (2021). I Am too old for this! Barriers contributing to the non-adoption of mobile payment. *International Journal of Bank Marketing*, 40(5), pp.1017–1050. <https://doi.org/10.1108/ijbm-06-2021-0283>.

Chanajitt, R., Viriyasitavat, W., and Choo, K.-K.R. (2016). Forensic analysis and security assessment of Android m-banking apps. *Australian Journal of Forensic Sciences*, 50(1), pp.3–19. <https://doi.org/10.1080/00450618.2016.1182589>.

Chatterji, S., Byles, J., Cutler, D., Seeman, T., and Verdes, E. (2015). Health, functioning, and disability in older adults—present status and future implications. *The Lancet*, 385(9967), pp.563–575. [https://doi.org/10.1016/s0140-6736\(14\)61462-8](https://doi.org/10.1016/s0140-6736(14)61462-8).

Chen, L. and Holsapple, C.W. (2013). E-business adoption research: State of the art. *Journal of Electronic Commerce Research*, 14(3), p.261.

Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., ... & Xu, L. (2020, June). An empirical assessment of security risks of global android banking apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 1310-1322); New York, United States. <https://doi.org/10.1145/3377811.3380417>.

Chen, S., Su, T., Fan, L., Meng, G., Xue, M., Liu, Y., & Xu, L. (2018, October). Are mobile banking apps secure? what can be improved? In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 797-802); Lake Buena Vista, Florida. <https://doi.org/10.1145/3236024.3275523>.

Chigada, J.M. and Hirschfelder, B. (2017). Mobile banking in South Africa: A review and directions for future research. *SA Journal of Information Management*, 19(1). <https://doi.org/10.4102/sajim.v19i1.789>.

Chigori, D., Viljoen, K., Ford, M., and Cilliers, L. (2020). Mobile phone banking: A comparative analysis of e-service quality and customer loyalty of banking applications and Unstructured Supplementary Service Data services. *Journal of Economic and Financial Sciences*, 13(1), p.11. <https://doi.org/10.4102/jef.v13i1.471>.

Chirani, I., & Ghofrani, Y. R. (2010, April). Designing a model for explanation of the internet banking acceptance rate. In *2010 2nd IEEE International Conference on Information Management and Engineering* (pp. 627-633). IEEE. <https://doi.org/10.1109/icime.2010.5478241>.

Cohen, L., Manion, L., and Morrison, K. (2011). *Research Methods in Education* (7th Edition). London: Routledge.

Collis, J. and Hussey, R. (2003). *Business Research: a practical guide for undergraduate and postgraduate students*. New York: Palgrave Macmillan.

Constantin, L. (2014). *Security analysis of mobile banking apps reveals significant weaknesses*. [online] Available at: <<https://www.pcworld.com/article/443298/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html>> [Accessed 23 Dec. 2022].

Consumer Protection Act (2014). Consumer Protection Act | South African Government. [online] Wwww.gov.za. Available at: <<https://www.gov.za/documents/consumer-protection-act>> [Accessed 14 Jan. 2023].

Copyright Act 98 of 1978 (2015). Copyright Act 98 of 1978 | South African Government. [online] Available at: <<https://www.gov.za/documents/copyright-act-16-apr-2015-0942>> [Accessed 14 Jan. 2023].

Costello, A. B. and Osborne, J. W. (2005). Best Practices in Exploratory Factor Analysis : Four Recommendations for Getting the Most From Your Analysis. *Practical Assessment, Research, and Evaluation*, 10(7), pp.1–9.

Creswell, J.W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. London: Sage Publications Ltd.

Creswell, J.W. and Creswell, J.D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, California: Sage Publications, Inc.

Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), pp.297–334. <https://doi.org/10.1007/bf02310555>.

Dasgupta, D., Roy, A., and Nag, A. (2017). Multi-Factor Authentication. *Infosys Science Foundation Series*, pp.185–233. https://doi.org/10.1007/978-3-319-58808-7_5.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), pp.319–340. <https://doi.org/10.2307/249008>.

Davis, F.D., Bagozzi, R.P., and Warshaw, P.R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace 1. *Journal Of Applied Social Psychology*, 22(14), pp.1111–1132.

Dawson, C. (2002). *Practical research methods: a user-friendly guide to mastering research*. Oxford, United Kingdom: Comwell Press.

De Vos, A.S., Delport, C.S.L., Fouche, C. and Strydom, H., 2011. *Research at grass roots: A primer for the social science and human professions*. Van Schaik Publishers.

De, D., Kishore, K., Jaswal, V., and Kulkarni, V. (2021). Practical guidelines to develop and evaluate a questionnaire. *Indian Dermatology Online Journal*, 12(2), p.266. https://doi.org/10.4103/idoj.idoj_674_20.

DeLiema, M. (2017). Elder Fraud and Financial Exploitation: Application of Routine Activity Theory. *The Gerontologist*, 58(4), pp.706–718. <https://doi.org/10.1093/geront/gnw258>.

Du Plessis, M. (2018). *Constructing and validating a measuring instrument for coping with occupational stress* (University of South Africa). [online] Available at: <<<https://uir.unisa.ac.za/handle/10500/25387>> [Accessed 18 Sep. 2022].

Electronic Communications and Transactions Act (2010). Electronic Communications and Transactions Act | South African Government. [online] Available at: <<https://www.gov.za/documents/electronic-communications-and-transactions-act>> [Accessed 14 Jan. 2023].

Elena, T., Ekaterine, G., & Gyuzal, K. (2018, December). Development of Innovative Banking Products and Technologies for People with Disabilities. In *4th International Conference on Economics, Management, Law and Education (EMLE 2018)* (pp. 29-33). Atlantis Press; Moscow, Russia. <https://doi.org/10.2991/emle-18.2018.6>.

Esmaeili, A., Haghgoo, I., Davidavičienė, V., and Meidutė-Kavaliauskienė, I. (2021). Customer loyalty in mobile banking: Evaluation of perceived risk, relative advantages, and usability factors. *Engineering Economics*, 32(1), pp.70–81.

Esterhuizen, W. and Martins, N. (2016). The factor structure of a safety leadership assessment tool for the mining industry. *Journal of Contemporary Management*, 13(1), pp.1–26.

Etikan, I., Musa, S.A., and Alkassim, R.S., (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), pp.1–4.

Featherman, M.S. and Pavlou, P.A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), pp.451–474.

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.). London: Sage.

Financial Intelligence Centre Act 38 of 2001 | South African Government. [online] Available at: <<https://www.gov.za/documents/financial-intelligence-centre-act>> [Accessed 31 May 2022].

Fishbein, M. and Ajzen, I. (1977). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co.

Fisher, F.M. (1980). Multiple Regression in Legal Proceedings. *Columbia Law Review*, 80(4), p.702. <https://doi.org/10.2307/1122137>

Følstad, A. (2017). Users' design feedback in usability evaluation: a literature review. *Human-centric Computing and Information Sciences*, 7(1), pp.1-19.

Friemel, T.N. (2014). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media and Society*, 18(2), pp.313–331. <https://doi.org/10.1177/1461444814538648>.

Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., & Egelman, S. (2019). Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 21-40).

FSCA Financial Sector Outlook Study (2022). FCSA. [online] Available at: <<https://www.fsca.co.za/Documents/FSCA%20Financial%20Sector%20Outlook%20Study%202022.pdf>> [Accessed 23 May. 2022].

Galliers, R.D. (1985). In search of a paradigm for information systems research. In E. Mumford, R. Hirschheim, C. Fitzgerald and T. Wood-Harper (Eds.), *Research methods in information systems* (pp. 281-297). Amsterdam: North-Holland.

Garg, K., Garg, A.D., and Ledwaba, K.S. (2014). Customers perceptions of mobile banking using the technology acceptance model for selected banking outlets in Gauteng, South Africa. *International Journal of Computers and Technology*, 13(1), pp.4096–4109. <https://doi.org/10.24297/ijct.v13i1.2927>.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, 28(6), pp.725–737. [https://doi.org/10.1016/s0305-0483\(00\)00021-9](https://doi.org/10.1016/s0305-0483(00)00021-9).

Gefen, D., Straub, D., and Boudreau, M.C. (2000). Structural equation modelling and regression: Guidelines for research practice. *Communications of the Association For Information Systems*, 4(1), p.7.

Gerber, H. and Hall, R. (2017). Quantitative research design. In *Data Acquisition – 1 Day*, pp.30–56. Pretoria: HR Statistics (Pty) Ltd.

Goddard, W. and Melville, S. (2004). *Research methodology: An introduction*. Juta and Company Ltd.

Grant, M.J. and Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal*, 26(2), pp.91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>.

Grix, J. (2004). *The Foundations of Research*. New York, NY: Palgrave Macmillan.

Gupta, K.P., Manrai, R. and Goel, U. (2019). Factors influencing adoption of payments banks by Indian customers: extending UTAUT with perceived credibility. *Journal of Asia Business Studies*, 13(2), pp.173–195. <https://doi.org/10.1108/jabs-07-2017-0111>.

Hair, J.F., Black, W.C. and Babin, B.J. (2019). *Multivariate data analysis*. Andover, Hampshire, United Kingdom: Cengage Learning Emea.

Hald, A. (2005). *A history of probability and statistics and their applications before 1750*. Hoboken, N.J.: Wiley-Interscience.

Harris, M.A., Patten, K. and Regan, E.A. (2013). *The Need for BYOD Mobile Device Security Awareness and Training*. [online] Semantic Scholar. Available at: <<https://api.semanticscholar.org/CorpusID:14741532>> [Accessed 31 May. 2023].

He, W., Tian, X., Shen, J. and Li, Y. (2015). Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology. [online] Semantic Scholar. Available at: <<https://api.semanticscholar.org/CorpusID:2759626>> [Accessed 30 Apr. 2023].

Hilton, C.E. (2015). The importance of pretesting questionnaires: a field research example of cognitive pretesting the Exercise referral Quality of Life Scale (ER-QLS). *International Journal of Social Research Methodology*, 20(1), pp.21–34. <https://doi.org/10.1080/13645579.2015.1091640>.

Hoyt, W.T., Warbasse, R.E., and Chu, E.Y. (2006). Construct validation in counselling psychology research. *The Counseling Psychologist*, 34(6), pp.769–805.

IBM (2021). *What are push notifications?* [online] Available at: <<https://www.ibm.com/cloud/learn/push-notifications>>. [Accessed 11 Dec. 2022].

IBM (2022). *What is encryption? Data encryption defined*. [online] www.ibm.com. Available at: <<https://www.ibm.com/topics/encryption>>. [Accessed 28 Dec. 2022].

International Monetary Fund. (2022). *World Economic Outlook Database April 2022 – WEO Groups and Aggregates Information*. [online] Available at: <<https://www.imf.org/external/pubs/ft/weo/2022/01/weodata/groups.htm>> [Accessed 18 July. 2022].

Iqbal, S., Irfan, M., Ahsan, K., Hussain, M.A., Awais, M., Shiraz, M., et al. (2020). A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication

Factor. *IEEE Access*, 8, pp.177405–177423.

<https://doi.org/10.1109/access.2020.3025429>.

Israel, M. and Hay, I. (2006). *Research ethics for social scientists*. London: Sage.

Jayachandran, A. (2019). E-Banking or Branch Banking? Preference of Senior Citizens in Kerala (2019). *The IUP Journal of Bank Management*, Vol. XVIII, No. 2, May 2019, pp.19–29.

Jin, X., Kuang, E., & Fan, M. (2021). "Too old to bank digitally?": A Survey of Banking Practices and Challenges Among Older Adults in China. In *Designing Interactive Systems Conference 2021* (pp. 802-814). New York, United States.

Johnson, J. and Finn, K. (2017). *Designing user interfaces for an aging population : towards universal design*. Cambridge: Morgan Kaufmann.

Johnson, J. A. (2018). Designing technology for an aging population. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-2). Montreal, Canada. <https://doi.org/10.1145/3491101.3503745>.

Johnson, V.L., Woolridge, R.W., Wang, W., and Bell, J.R. (2020). The impact of perceived privacy, accuracy and security on the adoption of mobile self-checkout systems. *Journal of Innovation Economics Management*, (1), pp.221–247.

Kim, Y. J., Chun, J. U., and Song, J. (2009). Investigating the role of attitude in technology acceptance from an attitude strength perspective. *International Journal of Information Management*, 29(1), 67–77.

<https://doi.org/10.1016/j.ijinfomgt.2008.01.011>

Klímová, B., Poullová, P., Šimonová, I., Pražák, P., and Cierniak-Emerych, A. (2018). Internet use by the older adults in the Czech Republic. *E+M Ekonomie a Management*, 21(3), pp.220–232. <https://doi.org/10.15240/tul/001/2018-3-014>.

Koenaite, M., Chuchu, T., and de Villiers, M.V. (2019). The impact of mobile banking on the adoption of banking products and services in South Africa, using the technology acceptance model. *Journal of Business and Retail Management Research*, 13(03). <https://doi.org/10.24052/jbrmr/v13is03/art-09>.

Koenaite, M., Maziriri, E., and Chuchu, T. (2021). Attitudes Towards Utilising Mobile Banking Applications Among Generation Z Consumers in South Africa. *Journal of Business and Management Review*, 2(6), pp.417–438.

<https://doi.org/10.47153/jbmr26.1452021>.

Koosha A. (2018). *Understanding Adoption of Mobile Wallets : On Aged Population* Master of Science Thesis, KTH Industrial Engineering and Management. (TRITA-ITM-EX). [online] Available from: <<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-231107>> [Accessed 25 Jan. 2023]

Kumar, R. (2011). *Research Methodology: a step-by-step guide for beginners* (3rd ed.). London: Sage Publications.

Latulipe, C., Dsouza, R., & Cumbers, M. (2022, April). Unofficial Proxies: How Close Others Help Older Adults with Banking. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-13); New Orleans, Los Angeles.

<https://doi.org/10.1145/3491102.3501845>

Law, E.L.-C. and Abrahão, S. (2014). Interplay between User Experience (UX) evaluation and system development. *International Journal of Human-Computer Studies*, 72(6), pp.523–525. <https://doi.org/10.1016/j.ijhcs.2014.03.003>.

Lee, J.-H., Poliakoff, E., and Spence, C. (2009). The Effect of Multimodal Feedback Presented via a Touch Screen on the Performance of Older Adults. *Haptic and Audio Interaction Design*, pp.128–135. https://doi.org/10.1007/978-3-642-04076-4_14.

Leedy, P.D. and Ormrod, J.E. (2019). *Practical Research: Planning and Design*. 12th ed. New York: Pearson Education, Inc.

Lin, W.R., Lin, C-Y., and Ding, Y-H. (2020). Factors affecting the behavioural intention to adopt mobile payment: An empirical study in Taiwan. *Mathematics*, 8(10), p.1851.

Malhotra, N. K. (2010). *Marketing Research: An Applied Orientation* (6th ed.). London: Pearson Education.

- Manikandan, S. (2011). Measures of central tendency: Median and mode. *J Pharmacol Pharmacother*, 2(3), pp.214–215.
- Mattila, M., Karjaluoto, H., and Pento, T. (2003). Internet banking adoption among mature customers: early majority or laggards? *Journal of Services Marketing*, 17(5), pp.514–528. <https://doi.org/10.1108/08876040310486294>.
- McKim, C. (2022). Z-Score. Routledge. <https://doi.org/10.4324/9780367198459-reprw155-1>.
- Mendel, T., & Toch, E. (2019). My mom was getting this popup: Understanding motivations and processes in helping older relatives with mobile security and privacy. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(4), 1-20; London, United Kingdom. <https://doi.org/10.1145/3369821>.
- Mendenhall, W., Sincich, T., and Boudreau, N.S. (2003). *A second course in statistics: regression analysis* (Vol. 6). Upper Saddle River, NJ: Prentice Hall.
- Merhi, M., Hone, K., and Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, 59, p.101151.
- Mesquita, A. (Ed.). (2012). *User perception and influencing factors of technology in everyday life*. IGI Global.
- Mishra, P., Pandey, C.M., Singh, U., Gupta, A., Sahu, C., and Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. *Annals of Cardiac Anaesthesia*, 22(1), p.67.
- Mohd Thas Thaker, H., Mohd Thas Thaker, M.A., Khaliq, A., Pitchay, A.A., and Hussain, H.I. (2021). Behavioural intention and adoption of internet banking among clients of Islamic banks in Malaysia: An analysis using UTAUT2. *Journal of Islamic Marketing*, 13(5), pp.1171–97.
- Montesdioca, G.P.Z. and Maçada, A.C.G. (2015). Measuring user satisfaction with information security practices. *Computers and Security*, 48, pp.267–280.

Montgomery, D.C., Peck, E.A., and Vining, G.G. (2021). *Introduction to linear regression analysis*. Hoboken, NJ: John Wiley & Sons.

Morrison, B., Coventry, L., and Briggs, P. (2021). How do Older Adults feel about engaging with Cyber-Security? *Human Behaviour and Emerging Technologies*, 3(5), pp.1033–1049. <https://doi.org/10.1002/hbe2.291>.

Mouton, J. (2001.) *How to succeed in your master's and doctoral studies: A South African guide and resource book*. Pretoria: Van Schaik.

Msweli, N.T. (2020). *Factors influencing the adoption of mobile banking technology by the elderly in South Africa*. [online] repository.up.ac.za. Available at: <<http://hdl.handle.net/2263/75466>> [Accessed 11 Jul. 2022]

Msweli, N.T. and Mawela, T. (2020). Enablers and Barriers for Mobile Commerce and Banking Services Among the Elderly in Developing Countries: A Systematic Review. *Responsible Design, Implementation and Use of Information and Communication Technology*, pp.319–330.

Negahban, A. and Chung, C.H. (2014). Discovering determinants of users' perception of mobile device functionality fit. *Computers in Human Behaviour*, 35, pp.75–84.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. Relevance of Social Research. (7th ed., Vol. 8). England: Pearson Education Limited. <https://doi.org/10.2307/3211488>

Nguyen, T. T., Nguyen, D. C., Schilling, M., Wang, G., & Backes, M. (2021, May). Measuring user perception for detecting unexpected access to sensitive resource in mobile apps. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (pp. 578-592); Hong Kong, China. <https://doi.org/10.1145/3433210.3437511>.

Nicholson, S., Sniehotta, F.F., van Wijck, F., Greig, C.A., Johnston, M., McMurdo, M.E.T., Dennis, M., and Mead, G.E. (2012). A Systematic Review of Perceived Barriers and Motivators to Physical Activity after Stroke. *International Journal of Stroke*, 8(5), pp.357–364.

Norman, D. (2019). *I wrote the book on user-friendly design. What I see today horrifies me.* [online] Fast Company. Available at: <<https://www.fastcompany.com/90338379/i-wrote-the-book-on-user-friendly-design-what-i-see-today-horrifies-me>> [Accessed 15 Jul. 2022].

Norman, G. (2010). Likert scales, levels of measurement and the 'laws' of statistics. *Advances in Health Sciences Education*, 15(5), pp.625–632. <https://doi.org/10.1007/s10459-010-9222-y>.

O'Brien, H. (2016). Theoretical Perspectives on User Engagement. *Why Engagement Matters*, pp.1–26. https://doi.org/10.1007/978-3-319-27446-1_1.

O'Brien, H. and Cairns, P. eds., (2016). *Why Engagement Matters*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-27446-1>.

O'Brien, H.L. and Toms, E.G. (2009). The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology*, 61(1), pp.50–69.

O'Brien, H.L., Cairns, P. and Hall, M. (2018). A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies*, 112, pp.28–39. <https://doi.org/10.1016/j.ijhcs.2018.01.004>.

O'Rourke, N, and Hatcher, L. (2013). *A Step-By-Step Approach to Using SAS for Factor Analysis and Structural Equation Modeling*, Cary, North Carolina: Sas.

Oates, B.J. (2006). *Researching information systems and computing*. Los Angeles: Sage, Imp.

OECD (2020), *Financial Consumer Protection and Ageing Populations*. [online] Available at: <<https://www.oecd.org/finance/Financial-consumer-protection-and-ageing-populations.pdf>> [Accessed 25 May 2022].

Okem, A.E. (ed). (2016). *Theoretical and Empirical Studies on Cooperatives*. Springer briefs in geography. <https://doi.org/10.1007/978-3-319-34216-0>.

Older Persons Act 13 of 2006. (2006). [online] Available at: <https://www.justice.gov.za/legislation/acts/2006-013_olderpersons.pdf> [Accessed 12 July 2022].

Osho, O., Mohammed, U.L., Nimzing, N.N., Uduimoh, A.A., and Misra, S. (2019). Forensic Analysis of Mobile Banking Apps. *Computational Science and Its Applications – ICCSA 2019*, pp.613–626. https://doi.org/10.1007/978-3-030-24308-1_49.

OWASP (2022). *OWASP foundation, the open source foundation for application security*. [online] owasp.org. Available at: <<https://owasp.org/>>. [Accessed 12 Dec. 2022].

Paek, H.-J. and Hove, T. (2017). Risk Perceptions and Risk Characteristics. *Oxford Research Encyclopedia of Communication*. <https://doi.org/10.1093/acrefore/9780190228613.013.283>.

Panja, B., Fattaleh, D., Mercado, M., Robinson, A. and Meharia, P., 2013, May. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In *2013 international conference on collaboration technologies and systems (CTS)* (pp. 397-403). IEEE; Montreal, Canada.

Patton, M.Q. (2002). *Qualitative research and evaluation methods*. London: Sage.

PCI Security Standards Council (2019). *Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. [online] [Pcisecuritystandards.org](https://www.pcisecuritystandards.org). Available at: <<https://www.pcisecuritystandards.org/>> [Accessed 11 Dec 2022].

Peruma, A., Palmerino, J., and Krutz, D.E. (2018). Investigating user perception and comprehension of Android permission models. *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, pp.56-66; Gothenburg, Sweden. <https://doi.org/10.1145/3197231.3197246>.

Pieterse, H. (2008). *An Evaluation of Mature Consumer Needs in the banking Sector*, M A Dissertation in Psychology, UNISA, 2008.

Police recorded crime statistics Republic of South Africa . (2022). [online] Available at:
<https://www.saps.gov.za/services/downloads/third_quarter_presentation_2021_2022.pdf> [Accessed 11 Jun. 2022].

Poston, H. (2021). *Top threat modeling frameworks: STRIDE, OWASP Top 10, MITRE ATT&CK framework and more | Infosec*. [online] Available at:
<<https://resources.infosecinstitute.com/topics/management-compliance-auditing/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/>> [Accessed 19 Jun. 2022].

Pratama, R.R.D. and Renny, R., 2022. The role of behavioural intentions to use mobile banking: application of the UTAUT2 method with security, trust and risk factors. *Dinasti International Journal of Management Science*, 3(4), pp.728–741.

Protection of Personal Information Act (POPI Act). [online] Available at:
<<https://popia.co.za/>> [Accessed 22 May. 2022].

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

Ralston, M., Schatz, E., Menken, J., Gómez-Olivé, F., and Tollman, S. (2015). Who Benefits—Or Does not—From South Africa’s Old Age Pension? Evidence from Characteristics of Rural Pensioners and Non-Pensioners. *International Journal of Environmental Research and Public Health*, 13(1), p.85.

Ramnath, N. (2018). *Factors affecting the adoption of mobile banking among rural South Africans*, Doctoral dissertation, University of Pretoria.

Raut, S., Prabhu, S.R., and Agrawal, A.K. (2021, May). Ensuring Smartphone Security Through Real-Time Log Analysis. In *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021)*; Trichy, India.

Rehman, A.A. and Alharthi, K. (2016). An introduction to research paradigms. *International Journal of Educational Investigations*, 3(8), pp.51–59.

Rescorla, E. and Schiffman, A. (1999). The Secure Hypertext Transfer Protocol. <https://doi.org/10.17487/RFC2660>.

Reserve Bank of South Africa (2022). SA registered banks and representative offices. [online] Available at: <<https://www.resbank.co.za/en/home/what-we-do/Prudentialregulation/sa-registered-banks-and-representative-offices>> [Accessed 11 Jun. 2022].

Roberts, P., Priest, H., and Traynor, M. (2006). Reliability and validity in research. *Nursing Standard*, 20(44), pp.41–45. <https://doi.org/10.7748/ns2006.07.20.44.41.c6560>.

Robinson, S., Arbenz, G., Birta, L.G., Tolk, A., and Wagner, G. (2015). Conceptual modeling: Definition, purpose and benefits. *2015 Winter Simulation Conference (WSC)*, pp. 2812-2826.

Robinson, S., Arbez, G., Birta, L. G., Tolk, A., & Wagner, G. (2015, December). Conceptual modeling: Definition, purpose and benefits. In *2015 Winter Simulation Conference (WSC)* (pp. 2812-2826). IEEE; Huntington Beach, California. <https://doi.org/10.1109/wsc.2015.7408386>.

Robson, C. (2002). *Real world research: a resource for social scientists and practitioner-researchers*. Oxford: Blackwell Publishing.

Rogers, E.M. (1995). Diffusion of Innovations: modifications of a model for telecommunications. In *Die diffusion von innovationen in der telekommunikation*, pp.25–38. Springer, Berlin, Heidelberg.

Rogers, W.A., Gilbert, D.K., and Cabrera, E.F. (1997). An analysis of automatic teller machine usage by older adults: A structured interview approach. *Applied Ergonomics*, 28(3), pp.173–180. [https://doi.org/10.1016/s0003-6870\(96\)00076-2](https://doi.org/10.1016/s0003-6870(96)00076-2).

Rogozhkina, N.U. (2022). Cybersecurity in banking. *libeldoc.bsuir.by*. [online] Available at: <<https://libeldoc.bsuir.by/handle/123456789/48436>> [Accessed 11 Aug. 2022].

Rowley, J. (2014). Designing and using research questionnaires. *Management Research Review*, 37(3), pp.308–330.

Samaradiwakara, G.D.M.N. and Gunawardena, C.G. (2014). Comparison of existing technology acceptance theories and models to suggest a well improved theory/model. *International Technical Sciences Journal*, 1(1), pp.21–36.

Sangeetha, S. and Sumathi, M. (2018). Scale-based secured sensitive data storage for banking services in cloud. *International Journal of Electronic Business*, 14(2), p.171. <https://doi.org/10.1504/ijeb.2018.10016227>.

Sarcar, S., Jokinen, J., Oulasvirta, A., Silpasuwanchai, C., Wang, Z., & Ren, X. (2016). Towards ability-based optimization for aging users. In *Proceedings of the International Symposium on Interactive Technology and Ageing Populations* (pp. 77-86); Kochi, Japan. <https://doi.org/10.1145/2996267.2996275>.

Sarcar, S., Munteanu, C., Jokinen, J. P., Oulasvirta, A., Silpasuwanchai, C., Charness, N., ... & Ren, X. (2017). Designing mobile interactions for the ageing populations. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 506-509); Denver, Colorado. <https://doi.org/10.1145/3027063.3027074>.

Saukkonen, P., Kainiemi, E., Virtanen, L., Kaihlanen, A.-M., Koskinen, S., Sainio, P., Koponen, P., Kehusmaa, S., and Heponiemi, T. (2022). Non-use of Digital Services Among Older Adults During the Second Wave of COVID-19 Pandemic in Finland: Population-Based Survey Study. *Human Aspects of IT for the Aged Population. Design, Interaction and Technology Acceptance*, pp.596–613. https://doi.org/10.1007/978-3-031-05581-2_41.

Saunders, M., Lewis, P., and Thornhill, A. (2019). *Research methods for business students*. 8th ed. United Kingdom: Pearson.

Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9), pp.9–16.

Seifert, A. and Schelling, H.R. (2018). Seniors Online: Attitudes Toward the Internet and Coping With Everyday Life. *Journal of Applied Gerontology*, 37(1), pp.99–109. <https://doi.org/10.1177/0733464816669805>.

Shitkova, M., Holler, J., Heide, T., Clever, N. and Becker, J. (2015). Towards Usability Guidelines for Mobile Websites and Applications. *Wirtschaftsinformatik und Angewandte Informatik*, pp.1603–1617.

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

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

Soodan, V. and Rana, A. (2020). Modeling customer' intention to use e-wallet in a developing nation: Extending UTAUT2 with security, privacy and savings. *Journal of Electronic Commerce in Organizations (JECO)*, 18(1), pp.89–114.

South African Government (2017). *Old age pension | South African Government*. [online] Available at: <<https://www.gov.za/services/social-benefits-retirement-and-old-age/old-age-pension>> [Accessed 22 May. 2022].

Sreejesh, S., Mohapatra, S. and Anusree, M.R. (2014). *Business Research Methods*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-00539-3>.

Statista. (2022). *Smartphone users in South Africa 2014-2022*. [online] Available at: <<https://www.statista.com/statistics/488376/forecast-of-smartphone-users-in-south-africa/#:~:text=Jan%2018%2C%202023%20Today%20about%2020%20to%2022>> [Accessed 26 May. 2022]

Statistics South Africa (2016). *StatsSA | StatsSA*. [online] Available at: <<http://cs2016.statssa.gov.za/>> [Accessed 22 May. 2022].

- Statistics South Africa (2020). *Statistics South Africa*. [online] Available at: <<https://www.statssa.gov.za/?m=2020>> [Accessed 22 May. 2022]
- Sun, H. and Zhang, P. (2006). The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies*, 64(2), pp.53–78. <https://doi.org/10.1016/j.ijhcs.2005.04.013>.
- Sürücü, I. and Maslakçı, A. (2020). Validity and reliability in quantitative research. *Business and Management Studies: An International Journal*, 8(3), pp.2694–2726.
- Tabachnick, B.G., Fidell, L.S., and Ullman, J.B. (2013). *Using Multivariate Statistics*, pp.497–516. Boston, MA: Pearson.
- Tahar, A., Riyadh, H.A., Sofyani, H., and Purnomo, W.E. (2020). Perceived Ease of Use, Perceived Usefulness, Perceived Security and Intention to Use E-Filing: The Role of Technology Readiness. *The Journal of Asian Finance, Economics and Business*, 7(9), pp.537–547. <https://doi.org/10.13106/jafeb.2020.vol7.no9.537>.
- Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *International Journal of Academic Research in Management*, 5(3), pp.28–36. Taherdoost, H., Sahibuddin, S., and Jalaliyoon, N. (2014). Exploratory Factor Analysis; Concepts and Theory. *Hal.science*, [online] 27, p.375. Available at: <<https://hal.science/hal-02557344>> [Accessed 25 Jan. 2023].
- Taylor, S. and Todd, P.A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), pp.144–176.
- Thakkar, J.J. (2020). Procedural Steps in Structural Equation Modelling. *Structural Equation Modelling*, pp.29–34. https://doi.org/10.1007/978-981-15-3793-6_3.
- The Banking Association South Africa (BASA). (2021). *Do not Take the Bait: OBS Warns*. [online] Available at: <<https://www.banking.org.za/news/protect-your-livelihood-do-not-take-the-bait-a-warning-from-the-obs/>> [Accessed 4 May 2022].

- Thompson, R.L., Higgins, C.A., and Howell, J.M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly*, 15(1), pp.125–143.
- Titus, R.M., Heinzelmann, F., and Boyle, J.M. (1995). *Victimization of Persons by Fraud*. *Crime and Delinquency*, 41(1), pp.54–72.
- Tiwari, P., Garg, V., Singhal, A., & Puri, N. (2020). Mobile Banking a Myth or Misconception. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 781-786). IEEE; Noida, India.
- Tricco, A.C., Lillie, E., Zarin, W., O'Brien, K.K., Colquhoun, H., Levac, D., Moher, D., et al. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Annals of Internal Medicine*, 169(7), p.467. <https://doi.org/10.7326/m18-0850>.
- Ubam, E., Hipiny, I., and Ujir, H. (2021). *User Interface/User Experience (UI/UX) Analysis amp; Design of Mobile Banking App for Senior Citizens: A Case Study in Sarawak, Malaysia*. IEEE Xplore. <https://doi.org/10.1109/ICEEI52609.2021.9611136>.
- United Nations Development Programme. (2021). UNDP Annual Report 2021. [online] Available at: <<https://www.undp.org/publications/undp-annual-report-2021#>> [Accessed 31 Jan. 2023].
- United Nations, Department of Economic and Social Affairs, Population Division (2015). *World Population Ageing 2015 (ST/ESA/SER.A/390)*.
- Vally, N.T. (2016). Insecurity in South African Social Security: An Examination of Social Grant Deductions, Cancellations, and Waiting. *Journal of Southern African Studies*, 42(5), pp.965–982. <https://doi.org/10.1080/03057070.2016.1223748>.
- Van Boekel, L.C., Peek, S.T., and Luijckx, K.G. (2017). Diversity in Older Adults' Use of the Internet: Identifying Subgroups Through Latent Class Analysis. *Journal of Medical Internet Research*, 19(5), pp.180. <https://doi.org/10.2196/jmir.6853>.
- Van Wyk, J. and Mason, K.A. (2001). Investigating Vulnerability and Reporting Behaviour for Consumer Fraud Victimization. *Journal of Contemporary Criminal Justice*, 17(4), pp.328–345. <https://doi.org/10.1177/1043986201017004003>.

Veitch, A. (2016). *Mobile Applications and the Law – Schindlers Attorneys*. [online] Available at: <https://www.schindlers.co.za/2016/mobile-applications-and-the-law/>. [Accessed 13 Dec. 2022].

Venkatesh, V. and Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. *Journal of Global Information Technology Management*, 13(1), pp.5–27.

Venkatesh, V., Brown, S.A., and Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), pp.21–54.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), pp.425–478.

Venkatesh, V., Thong, J.Y., and Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), pp.157–178.

Vidal, E. (2019, October). Digital literacy program: reducing the digital gap of the elderly: experiences and lessons learned. In *2019 International Conference on Inclusive Technologies and Education (CONTIE)* (pp. 117-1173). IEEE; San Jose del Cabo, Mexico.

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, 10(1), pp.69–80.

Wang, J. and Wang, X. (2019). *Structural equation modeling: Applications using Mplus*. Hoboken, NJ: John Wiley & Sons.

Wechuli, N.A., Franklin, W., and Jotham, W. (2017). User Perceived Secure Mobile Banking Service Provision Framework. *International Journal of Computer Engineering and Information Technology*, 10(10), pp.225–232.

Westin, A.F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), p.166.

- Weston, R. and Gore Jr, P.A. (2006). A brief guide to structural equation modelling. *The counselling psychologist*, 34(5), pp.719–751.
- White, A. (2013). *Six Main Rules Of Safe Mobile Banking. Where, When And How?* [online] Available at: <<https://www.jammer-store.com/six-main-rules-of-safe-mobile-banking.html>> [Accessed 23 Dec. 2022].
- Wilson, R.S., Beckett, L.A., Barnes, L.L., Schneider, J.A., Bach, J., Evans, D.A., and Bennett, D.A. (2002). Individual differences in rates of change in cognitive abilities of older persons. *Psychology and Aging*, 17(2), pp.179–193.
- Wong, C.Y., Ibrahim, R., Hamid, T.A. and Mansor, E.I. (2018). Usability and design issues of smartphone user interface and mobile apps for older adults. In *User Science and Engineering: 5th International Conference, i-USEr 2018, August 28–30, 2018, Proceedings 5* (pp. 93-104); Puchong, Malaysia.
- World Health Organisation (WHO). (2015). *WHO | World report on ageing and health 2015*. [online] Available at: <<http://www.who.int/ageing/events/world-report-2015-launch/en/>> [Accessed 11 Dec. 2022].
- World Health Organisation (WHO). (2020). *GHO | By category | Life expectancy and Healthy life expectancy - Data by country*. [online] Available at: <<https://apps.who.int/gho/data/view.main.SDG2016LEXv?lang=en>> [Accessed 11 May. 2022].
- World Health Organization (WHO). (2020). Global Health Observatory Data Repository. Geneva: WHO; 2020. *GHO | By category | Life expectancy and Healthy life expectancy - Data by WHO region*. [online] Available at: <<https://apps.who.int/gho/data/view.main.SDG2016LEXREGv?lang=en>> [Accessed 12 May. 2022].
- Yong, A. G. and Pearce, S. (2013). A beginner' s guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology*, 9(2), pp.79–94.


Yousafzai, S. and Yani-de-Soriano, M. (2012). Understanding customer-specific factors underpinning internet banking adoption. *International Journal of Bank Marketing*, 30(1), pp.60–81. <https://doi.org/10.1108/02652321211195703>.

Zhuang, M., Toms, E.G. and Demartini, G. (2016). The relationship between user perception and user behaviour in interactive information retrieval evaluation. In *Advances in Information Retrieval: 38th European Conference on IR Research, ECIR 2016, March 20–23, 2016. Proceedings 38* (pp.293-305); Padua, Italy.

INDEX OF APPENDICES

Appendix A: Ethical clearance approval

A1: Non-human participant ethical clearance



School of Computing_CSET_SOC

Date: 02/03/2023

Dear: Miss Rumbidzai Goronga

Decision: Ethics Approval from 02/03/2023 to 02/03/2026

NHREC Registration #: (if applicable)
Ref #: 0641
Name: Miss Rumbidzai Goronga
Student #: 48286885
Staff #:

Researcher:

South Africa
48286885@mylife. 5099

Supervisor: Prof Adele da Veiga dveiga@unisa.ac.za

Co-Supervisor: Professor Hugo Lotriet lotrihh@unisa.ac.za

AGED USERS' MOBILE BANKING APPLICATION SECURITY FACTORS MODEL TO GUIDE THE DESIGN OF MOBILE BANKING APPLICATIONS BASED ON THE PERCEPTION OF AGED USERS IN GAUTENG, SOUTH AFRICA

Qualification: MSc Computing

Thank you for the application for research ethics clearance by the School of Computing_CSET_SOC for the above mentioned research study Ethics approval is granted for three years .

The **negligible risk application** was **reviewed** by School of Computing_CSET_SOC on 02/03/2023 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the School of Computing_CSET_SOC .
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the

Page 1 of 2

Committee in writing, accompanied by a progress report.

5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date (02/03/2023). Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.
8. **Recommendation:** Consider removing: "... and will be a quantitative study." This seems to refer to the main study which is not covered by this application, unless the scoping literature review is regarded as quantitative too.

Additional Conditions

1. Disclosure of data to third parties is prohibited without explicit consent from Unisa.
2. De-identified data must be safely stored on password protected PCs.
3. Care should be taken by the researcher when publishing the results to protect the confidentiality and privacy of the university.
4. Adherence to the National Statement on Ethical Research and Publication practices, principle 7 referring to Social awareness, must be ensured: "Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible." Unisa will not be liable for any failure to comply with this principle.

Note

The reference number 0641 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Kind regards,



D Danie Bisschoff
Chair of School of Computing_CSET_SOC

E-mail:



Executive Dean / By delegation from the Executive Dean of School of Computing_CSET_SOC

E-mail:

A2: Human participant ethical clearance

College of Science, Engineering and Technology_ School of Computing_ERC

Date: 26/07/2023

Dear: Miss Rumbidzai Goronga

**Decision: Ethics Approval from
26/07/2023 to 26/07/2026.**

NHREC Registration # : (if applicable)

Ref #: 1026

Name: Miss Rumbidzai Goronga

Student #: 48286885

Staff #:

Researcher: Miss Rumbidzai Goronga

Supervisor: Prof Adele da Veiga

Co-Supervisor: Professor Hugo Lotriet

Mobile banking applications security factors model for aged users in South Africa

Qualification: MSc Computing

Thank you for the application for research ethics clearance by the College of Science, Engineering and Technology_ School of Computing_ERC for the above mentioned research study Ethics approval is granted for three years.

The **low risk application** was **reviewed** by College of Science, Engineering and Technology_ School of Computing_ERC on 26/07/2023 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology_ School of Computing_ERC.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.

5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date (26/07/2026). Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.

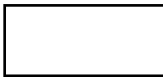
Additional Conditions


1. Disclosure of data to third parties is prohibited without explicit consent from Unisa.
2. De-identified data must be safely stored on password protected PCs.
3. Care should be taken by the researcher when publishing the results to protect the confidentiality and privacy of the university.
4. Adherence to the National Statement on Ethical Research and Publication practices, principle 7 referring to Social awareness, must be ensured: "Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible." Unisa will not be liable for any failure to comply with this principle.

Note


The reference number 1026 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Kind regards,



Dr. Danie Bisschoff
Chair of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: 



Executive Dean / By delegation from the Executive Dean of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: 

Appendix B: Participant information sheet

B1: Expert panel participant information sheet



PARTICIPANT INFORMATION SHEET – EXPERT PANEL

Ethics clearance reference number: 1026

1 August 2023

Title: Mobile banking applications security factors model for aged users in South Africa.

Dear Prospective Participant

My name is Rumbidzai Goronga, and I am doing research with Professor A. Da Veiga, an Associate Professor in the Department of Computing and Professor H. Lotriet, a Professor in the Department of Computing towards an MSc in Computing at the University of South Africa. We are inviting you to participate in a study entitled "Mobile banking applications security factors model for aged users in South Africa".

WHAT IS THE PURPOSE OF THE STUDY?

This study is expected to collect important information that could assist us to develop an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications.

WHY AM I BEING INVITED TO PARTICIPATE?

You are invited to participate in the evaluation of the questionnaire for the study as an **expert panel member**. For this study, we envisage 5-10 experts to participate. The expert panel members have been invited because of their Academic and Information Security expertise. The expert panel review will assist in reviewing the questionnaire and providing recommendations where required.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The study involves a survey whereby the participant must complete a questionnaire. Demographics, and mobile banking application security perception type of questions will be asked. No personal identifiable information of the expert panel will be collected.

The expert panel is invited to review the questionnaire prior to the pilot group reviewing the questionnaire, and subsequently the final survey being sent to the aged users.

The expected review time for the expert panel is 1-2 weeks. During this time the expert panel will be given an opportunity to review the questionnaire and provide input. The expected timeframe for the expert panel to complete the questionnaire is approximately 15 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the 'send' button based on the anonymous nature of the survey.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the understanding of perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa from a research perspective. It is anticipated that the information gained from this survey will help us to develop an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not foresee that you will experience any negative consequences by completing the survey. The survey is anonymous and no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Your name will not be recorded anywhere, and no-one will be able to connect you to the responses or input you provide. Your responses will be given a random unique identifier, or a pseudonym and we will refer to you in this way in the data, any publications or other research reporting methods such as conference proceedings.

By completing this survey, the anonymous information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings. A report on the study may be submitted for publication but individual participants will not be identifiable in the report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at Unisa for future research or academic purposes; electronic information will be stored on a password-protected computer. Future use of the stored data will be subject to further research ethics review and approval, if applicable. Hard copies will be shredded, and data will be deleted permanently from the survey application database files and hard drive of the computer through the use of a relevant software application.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the understanding of perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

If you would like to be informed of the final research findings, please contact Rumbidzai Goronga on or email . The findings are accessible for a period of 5 years.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact Rumbidzai Goronga on or email .

Should you have concerns about the way in which the research has been conducted, you may contact Professor A. da Veiga on or email: . Contact the research ethics chairperson of the School of Computing Research Ethics Committee on email: if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.
Thank you.

Rumbidzai Goronga



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



PARTICIPANT INFORMATION SHEET – PILOT GROUP

Ethics clearance reference number: 1026

1 August 2023

Title: Mobile banking applications security factors model for aged users in South Africa.

Dear Prospective Participant

My name is Rumbidzai Goronga, and I am doing research with Professor A. Da Veiga, an Associate Professor in the Department of Computing and Professor H. Lotriet, a Professor in the Department of Computing towards an MSc in Computing at the University of South Africa. We are inviting you to participate in a study entitled "Mobile banking applications security factors model for aged users in South Africa".

WHAT IS THE PURPOSE OF THE STUDY?

This study is expected to collect important information that could assist us to develop an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications.

WHY AM I BEING INVITED TO PARTICIPATE?

You are invited to participate in a pilot survey. Users that are over 65 years of age and make use of mobile banking applications will take part in the pilot survey and are invited based on availability. A group of 10-15 aged users will take part in the pilot survey.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the pilot group participant must complete a questionnaire. Demographics, and mobile banking application security perception type of questions will be asked. No personal identifiable information of the pilot group will be collected.



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The expected timeframe for the pilot group participant to complete the questionnaire is approximately 15 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the 'send' button based on the anonymous nature of the survey.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the understanding of perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa from a research perspective. It is anticipated that the information gained from this survey will help us to develop an Aged Users' Mobile Banking Application Security Factors Model that could inform the design of secure mobile banking applications.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not foresee that you will experience any negative consequences by completing the survey. The survey is anonymous and no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

Your name will not be recorded anywhere, and no-one will be able to connect you to the responses or input you provide. Your responses will be given a random unique identifier, or a pseudonym and we will refer to you in this way in the data, any publications or other research reporting methods such as conference proceedings.



University of South Africa
Pretter Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

By completing this survey, the anonymous information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings. A report on the study may be submitted for publication but individual participants will not be identifiable in the report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at Unisa for future research or academic purposes; electronic information will be stored on a password-protected computer. Future use of the stored data will be subject to further research ethics review and approval, if applicable. Hard copies will be shredded, and data will be deleted permanently from the survey application database files and hard drive of the computer through the use of a relevant software application.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the understanding of perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Rumbidzai Goronga on or email . The findings are accessible for a period of 5 years.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact Rumbidzai Goronga on or email .



University of South Africa
Pretter Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Should you have concerns about the way in which the research has been conducted, you may contact Professor A. da Veiga on or email: . Contact the research ethics chairperson of the School of Computing Research Ethics Committee on email: if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.
Thank you.

Rumbidzai Goronga



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix C: Consent letter

C1: Expert panel consent letter



CONSENT TO PARTICIPATE IN THIS STUDY EXPERT PANEL

Title: Mobile banking applications security factors model for aged users in South Africa

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the processing of my feedback for the review of the questionnaire as part of the expert panel.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Researcher's Name & Surname: **Rumbidzai Goronga**

Researcher's signature _____ Date.....



University of South Africa
Pretia Street, Midrand Ridge, City of Tshwane
PO Box 392 UNISA, 0203 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

C2: Pilot group consent letter



**CONSENT TO PARTICIPATE IN THIS STUDY
PILOT GROUP**

Title: Mobile banking applications security factors model for aged users in South Africa

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the processing of my answers in completing the questionnaire as part of the pilot group.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Researcher's Name & Surname: Rumbidzai Goronga

Researcher's signature _____ Date.....



University of South Africa
Pretia Street, Maitland Road, City of Tlokweng
PO Box 392 UNISA, 0033 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix D: Questionnaires

D1: Expert panel questionnaire

**AGED USERS' PERCEPTIONS OF THE SECURITY OF MOBILE BANKING
APPLICATIONS QUESTIONNAIRE
FOR EXPERT PANEL**

Dear expert panel member

You are invited to participate in a survey conducted by Rumbidzai Goronga under the supervision of Prof A. da Veiga (School of Computing) and Prof. H. Lotriet (School of Computing) towards obtaining an MSc degree in Computing at the University of South Africa.

This survey has been designed to investigate the perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa. By completing this survey, you agree that the information you provide may be used for research purposes as well as for dissemination through peer-reviewed publications and conference proceedings. It is envisaged that the information we gain from this survey will help us to develop a security factors model that will help financial institutions in better designing mobile banking applications that are secure and easy to use for aged users. You are, however, under no obligation to complete the survey and may withdraw from the study at any time prior to submitting it. The survey has been developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, we will not be able to extract your information from the study once you have clicked the 'send' button. If you choose to participate in this survey, it will take no more than 15 minutes of your time. Although you as an individual will not benefit from your participation, it is envisioned that the findings of this study will improve the understanding of the perception of the factors that influence the security of mobile banking applications by aged users in South Africa from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. As researchers we undertake to keep any information provided herein confidential, not to let it go out of our possession, and to report on the findings from the perspective of the participating group (and not from that of an individual).

The records will be kept for five years for audit purposes, after which it will be permanently destroyed, and electronic versions will be deleted permanently from the hard drive of the computer. Furthermore, you will not be reimbursed or receive any incentives for your participation in the survey.

The research has been reviewed and approved by the School of Computing Research Ethics Committee, Reference Number: 1026. The primary researcher, Rumbidzai Goronga, can be contacted during office hours on . The study leader, Dr A. Da Veiga, is available during office hours on . Should you have any

questions regarding the ethical aspects of the study, you may contact the chairperson of the School of Computing Research Ethics Committee at [REDACTED]. Alternatively, you can report any serious unethical behaviour on the University's toll-free hotline 0800 86 96 93.

You now make your decision on whether to participate by continuing to the next page. **You are still free to withdraw from the study at any time prior to starting or completing the study.**

Please make sure that you have read the participant information sheet and signed the consent form prior to completing the questionnaire.

Information and definition section

Your participation in this very important survey is sincerely appreciated. The questionnaire consists of three sections, namely Section A where information about the expert panel is requested, Section B with 5 demographic questions, and Section C with **53** questions on the aged users' perceptions of the factors that influence the security of mobile banking applications.

The questionnaire comprises 12 elements:

1. Performance expectancy – This is the degree to which the mobile banking application is perceived to be of good use.
2. Effort expectancy – This is the degree to which the mobile banking application is perceived to be easy to use.
3. Social influence – This is the degree to which a user perceives the mobile banking application to be appreciated by the social network or community that are close or important to that user.
4. Facilitating conditions – This is the degree to which a user believes to possess the resources to support the use of the mobile banking application.
5. Hedonic motivation – This is the degree to which the mobile banking application is perceived to provide pleasure, enjoyment, and amusement.
6. Price value – This is the user's reasoning between the monetary cost of using the mobile banking application and the perceived benefits realized by using the mobile banking application.
7. Habit – This is the manner in which people perform as time passes, and behaviour changes due to learning or using the mobile banking application.
8. Perceived privacy – This is the degree to which a user's personal information is safe and protected from potential compromise.

9. Perceived risk – This is the potential loss that a user can suffer while trying to attain a specific desired outcome, using the mobile banking application.
10. Technological trust – This is the trust that the users have in the mobile banking applications to conduct banking transactions.
11. Perceived security – This is the degree of trust that the mobile banking application can securely transit sensitive information without any breaches.
12. Behavioural intention – This is a user's readiness or motivation to performs a certain behaviour.
13. Use behaviour – This is a measure of the actual frequency of use of a mobile banking application by a user.

Please find the questionnaire on the next page. Completion is expected to take no more than 15 minutes.

Section A: Expert panel information

We require some background information about the experts involved in reviewing the questionnaire and would appreciate if you would complete the questions below.

- i. What is your field of expertise (e.g. academic, information security, audit, technology, legal)?

- ii. What is your current job title?

- iii. What experience do you have in information security?

- iv. How many years' experience do you have in information security?

- v. What is your highest educational qualification?

The survey is conducted to determine the aged users' perceptions of the factors that influence the security of mobile banking applications.

Section B: Demographic Profile

We require some background information and would appreciate if you can please complete the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Indicate with a cross (X) as to whether you believe the item is essential to include or not, and whether it is clear or not.

Demographic Profile								
1. Please indicate your age	65 - 70		71-74		75-79		80+	
2. Please indicate your highest level of education	No schooling	Some primary schooling completed	Some secondary schooling completed	Grade 12/Matric	Higher certificate	Diploma	Degree	Post graduate degree
3. Please indicate your experience using a mobile banking application	Less than 6 months	6 months - less than 1 year		1 - 2 years	3 - 5 years		Over 5 years	
4. Please indicate all challenges related to using a mobile device as applicable to you	Difficulty remembering		Difficulty concentrating		Visual challenges			

Demographic Profile		
5. Please indicate if you have someone authorized to conduct banking on your behalf	Yes	
	No	

Expert panel feedback for demographic section:

Section C: Perceptions of the factors that influence the security of mobile banking applications

The following questions relate to the aged users' perceptions of the factors that influence the security of mobile banking applications. You are requested to select 2 answers.

Please rate the items below by indicating whether you believe the item is essential to include or not, and whether it is clear or not.

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
Performance expectancy									
1.	The use of mobile banking applications is useful in my daily life.								
2.	The use of mobile banking applications helps me complete banking tasks quickly.								
3.	The use of mobile banking applications increases my productivity.								
Effort expectancy									

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
4.	Learning how to use mobile banking applications is easy.								
5.	My interactions with mobile banking applications are clear and understandable.								
6.	Mobile banking applications are easy to use.								
7.	It is easy for me to become skilful at using mobile banking applications.								
8.	Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.								
Social influence									

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
9.	The people who are important to me think that I should use mobile banking applications.								
10.	The people who influence my behaviour think that I should use mobile banking applications.								
11.	The people whose opinions that I value prefer that I use mobile banking applications.								
12.	The people who are important to me support my use of mobile banking applications.								
13.	I have confidence in using mobile banking applications if my friends and family also use them.								

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
Facilitating conditions									
14.	I have the resources necessary to use mobile banking applications.								
15.	I have the knowledge to use mobile banking applications.								
16.	Mobile banking applications are compatible with other technologies (such as mobile phones) I use.								
17.	I can get help from others when I have difficulties using mobile banking applications.								
18.	There is sufficient support offered by the financial								

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
	institutions for using mobile banking applications.								
Hedonic motivation									
19.									
	Using a mobile banking application is fun.								
20.									
	Using a mobile banking application is enjoyable.								
21.									
	Using the mobile banking application is very exciting.								
Price value									
22.									
	Mobile banking applications are reasonably priced.								
23.									
	Mobile banking applications provide good value for money.								

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
24.									
	At the current price, the mobile banking applications provide good value.								
Habit									
25.									
	The use of mobile banking applications has become a habit for me.								
26.									
	I am addicted to using mobile banking applications.								
27.									
	I must use mobile banking applications.								
28.									
	I have adequate experience to use mobile banking applications.								
Perceived privacy									

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here				
		Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
29.	My personal information is safe when using mobile banking applications.									
30.	Mobile banking applications offer sufficient privacy protection measures.									
31.	Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.									
32.	My transaction information is protected when using mobile banking applications.									
33.	Mobile banking applications keep my private information protected.									

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here				
		Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
Perceived risk										
34.	Using mobile banking applications does not put my privacy at risk.									
35.	People trusted to assist me with using mobile banking applications do not pose a risk to my funds.									
36.	Criminals cannot try and take control of my account if I use mobile banking applications.									
37.	The chances of losing my money if my use mobile banking applications are low.									
38.	It is harmless for me to use mobile banking applications.									

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
Technological trust									
39.	I can trust mobile banking applications.								
40.	Mobile banking applications restrict unauthorised access.								
41.	I can trust mobile banking applications to accurately process transactions.								
Perceived security									
42.	Mobile banking applications are secure.								
43.	My user data on mobile banking applications is secure.								
44.	My transaction details on mobile banking applications are secure.								

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
45.	The mobile banking applications have diligent security controls.								
46.	My interaction on mobile banking applications is secure.								
47.	There is nothing to worry about regarding the security of the mobile banking applications.								
Behavioural intention									
48.	I intend to continue using mobile banking applications in the future.								
49.	I will always try to use mobile banking applications in my daily life.								
50.	I plan to continue to use mobile banking applications frequently.								

Perceptions of the factors that influence the security of mobile banking applications						Expert panel – select 2 answers here			
	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Essential	Not essential	Item is clear	Item is unclear
Use behaviour									
51.	I regularly use mobile banking applications.								
52.	I use mobile banking application for all my banking needs.								
53.	I have increased my use of mobile banking applications over time.								

D2: Pilot group questionnaire

AGED USERS' PERCEPTIONS OF THE FACTORS INFLUENCING THE SECURITY OF MOBILE BANKING APPLICATIONS QUESTIONNAIRE FOR PILOT GROUP

Dear pilot group member

You are invited to participate in a survey conducted by Rumbidzai Goronga under the supervision of Prof A. da Veiga (School of Computing) and Prof. H. Lotriet (School of Computing) towards obtaining an MSc degree in Computing at the University of South Africa.

This survey has been designed to investigate the perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa. By completing this survey, you agree that the information you provide may be used for research purposes as well as for dissemination through peer-reviewed publications and conference proceedings. It is envisaged that the information we gain from this survey will help us to develop a security factors model that will help financial institutions in better designing mobile banking applications that are secure and easy to use for aged users. You are, however, under no obligation to complete the survey and may withdraw from the study at any time prior to submitting it. The survey has been developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, we will not be able to extract your information from the study once you have clicked the 'send' button. If you choose to participate in this survey, it will take no more than 15 minutes of your time. Although you as an individual will not benefit from your participation, it is envisioned that the findings of this study will improve the understanding of the perceptions of the factors that influence the security of mobile banking applications by aged users in South Africa from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. As researchers we undertake to keep any information provided herein confidential, not to let it go out of our possession, and to report on the findings from the perspective of the participating group (and not from that of an individual).

The records will be kept for five years for audit purposes, after which it will be permanently destroyed, and electronic versions will be deleted permanently from the hard drive of the computer. Furthermore, you will not be reimbursed or receive any incentives for your participation in the survey.

The research has been reviewed and approved by the School of Computing Research Ethics Committee. The primary researcher, Rumbidzai Goronga, can be contacted during office hours on . The study leader, Dr A. Da Veiga, is available during office hours on . Should you have any questions regarding the ethical

aspects of the study, you may contact the chairperson of the School of Computing Research Ethics Committee at . Alternatively, you can report any serious unethical behaviour on the University's toll-free hotline 0800 86 96 93.

You now make your decision on whether to participate by continuing to the next page. **You are still free to withdraw from the study at any time prior to starting or completing the study.**

Please make sure that you have read the participant information sheet and signed the consent form prior to completing the questionnaire.

Information section

Your participation in this very important survey is sincerely appreciated. The questionnaire consists of two sections, namely Section A with 5 demographic questions, and Section B with **53** questions on the perceptions of the factors that influence the security of mobile banking applications.

Please find the questionnaire on the next page. Completion is expected to take no more than 15 minutes.

Section A: Demographic Profile

We require some background information and would appreciate if you can please complete the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Indicate with a cross (X) as to whether you believe the item is essential to include or not, and whether it is clear or not.

Demographic Profile								
1. Please indicate your age in years	65 - 70		71 - 74		75 - 79		Over 80	
2. Please indicate your highest level of education	No schooling	Some primary schooling completed	Some secondary schooling completed	Grade 12/Matric	Higher certificate	Diploma	Degree	Post graduate degree
3. Please indicate how long you have been using a mobile banking application	Less than 6 months		6 months – less than 1 year		1 - 2 years	3 - 5 years	Over 5 years	
4. Please indicate all challenges related to	I have difficulty remembering when using a mobile banking application		I have difficulty concentrating when using a mobile banking application		I have visual challenges when using a mobile banking application			

Demographic Profile		
using a mobile device as applicable to you		
5. Please indicate if you have someone authorized to conduct banking on your behalf	Yes	No

Section B: Perceptions of the factors influencing the security of mobile banking applications

The following questions relate to your perceptions of the factors influencing the security of mobile banking applications. Please rate the items below by indicating your level of agreement with one of the five options next to each of the statements.

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
1.	The use of mobile banking applications is useful in my daily life.					
2.	The use of mobile banking applications helps me complete banking tasks quickly.					
3.	The use of mobile banking applications increases my productivity.					
4.	Learning how to use mobile banking applications is easy.					
5.	My interactions with mobile banking applications are clear and understandable.					
6.	Mobile banking applications are easy to use.					
7.	It is easy for me to become skilful at using mobile banking applications.					
8.	Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.					
9.	The people who are important to me think that I should use mobile banking applications.					
10.	The people who influence my behaviour think that I should use mobile banking applications.					

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
11.	The people whose opinions that I value prefer that I use mobile banking applications.					
12.	The people who are important to me support my use of mobile banking applications.					
13.	I have confidence in using mobile banking applications if my friends and family also use them.					
14.	I have the resources necessary to use mobile banking applications.					
15.	I have the knowledge to use mobile banking applications.					
16.	Mobile banking applications are compatible with other technologies (such as mobile phones) I use.					
17.	I can get help from others when I have difficulties using mobile banking applications.					
18.	The financial institutions provide adequate support for using mobile banking applications.					
19.	Using a mobile banking application is fun.					
20.	Using a mobile banking application is enjoyable.					
21.	Using the mobile banking application is very exciting.					
22.	Mobile banking applications are reasonably priced.					
23.	Mobile banking applications provide good value for money.					

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
24.	At the current price, the mobile banking applications provide good value.					
25.	The use of mobile banking applications has become a habit for me.					
26.	I am addicted to using mobile banking applications.					
27.	I must use mobile banking applications.					
28.	I have adequate experience to use mobile banking applications.					
29.	My personal information is safe when using mobile banking applications.					
30.	Mobile banking applications provide adequate privacy protection.					
31.	Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.					
32.	My transaction information is protected when using mobile banking applications.					
33.	Mobile banking applications keep my private information protected.					
34.	Using mobile banking applications does not put my privacy at risk.					
35.	My funds are at no risk with the people I trust to help me use mobile banking applications.					
36.	If I use mobile banking applications, criminals cannot attempt to take over my account.					
37.	There is little chance that I will lose my funds if I use mobile banking applications.					

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
38.	It is harmless for me to use mobile banking applications.					
39.	I can trust mobile banking applications.					
40.	Mobile banking applications restrict unauthorised access.					
41.	I can trust mobile banking applications to accurately process transactions.					
42.	Mobile banking applications are secure.					
43.	My personal details on mobile banking applications are secure.					
44.	My transaction details on mobile banking applications are secure.					
45.	The mobile banking applications have strict security measures.					
46.	My interaction on mobile banking applications is secure.					
47.	There is nothing to worry about regarding the security of the mobile banking applications.					
48.	I intend to continue using mobile banking applications in the future.					
49.	I will always try to use mobile banking applications in my daily life.					
50.	I plan to continue to use mobile banking applications frequently.					
51.	I regularly use mobile banking applications.					
52.	I use mobile banking application for all my banking needs.					
53.	I have increased my use of mobile banking applications over time.					

D3: Aged users' questionnaire (electronically administered)

AGED USERS' PERCEPTIONS OF THE SECURITY OF MOBILE BANKING APPLICATIONS

Dear prospective participant

You are invited to participate in a survey conducted by Rumbidzai Goronga under the supervision of Prof A. da Veiga (School of Computing) and Prof. H. Lotriet (School of Computing) towards obtaining an MSc degree in Computing at the University of South Africa.

The survey you have received has been designed to study the perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa. You were selected to participate in this survey because you are at least 65 years of age, reside in South Africa and make use of mobile banking applications. You will not be eligible to complete the survey if you are younger than 65 years of age, do not reside in South Africa and do not make use of mobile banking applications. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a security factors model that will help financial institutions in better designing mobile banking applications that are secure and easy to use for aged users. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the understanding of the perception of the factors that influence the security of mobile banking applications by aged users in South Africa from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. The researcher undertakes to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for a minimum period of five years for audit purposes where after it will be permanently destroyed, hard copies will be shredded, and electronic versions will be permanently deleted from the hard drive of the computer. You will not be reimbursed or receive any incentives for your participation in the survey.

The research has been reviewed and approved by the School of Computing Research Ethics Committee. The primary researcher, Rumbidzai Goronga, can be contacted during office hours on [REDACTED]. The study leader, Dr A. Da Veiga, is available during office hours on [REDACTED]. Should you have any questions regarding the ethical aspects of the study, you may contact the chairperson of the School of Computing Research Ethics Committee at [REDACTED]. Alternatively, you can report any serious unethical behavior on the University's toll-free hotline 0800 86 96 93.

You are deciding whether to participate by continuing to the next page (or by indicating your consent by clicking on the 'box' below). By completing the survey, you imply that you have consented to participate in this research. You are free to withdraw from the study at any time prior to clicking the send button.

[Sign in to Google](#) to save your progress. [Learn more](#)

* Indicates required question

Do you agree and consent to participate? *

Yes

Next



Page 1 of 4

Clear form

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

AGED USERS' PERCEPTIONS OF THE SECURITY OF MOBILE BANKING APPLICATIONS

[Sign in to Google](#) to save your progress. [Learn more](#)

Information section

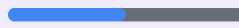
Your participation in this very important survey is sincerely appreciated. The questionnaire consists of two sections:

- Section A where demographic information is requested
- Section B with 53 questions on your perceptions of the factors that influence the security of mobile banking applications.

Please find the questionnaire on the next page. Completion is expected to take no more than 15 minutes.

[Back](#)

[Next](#)



Page 2 of 4

[Clear form](#)

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

AGED USERS' PERCEPTIONS OF THE SECURITY OF MOBILE BANKING APPLICATIONS

[Sign in to Google](#) to save your progress. [Learn more](#)

Section A: Demographic Profile

We require some background information and would appreciate if you can please complete the questions below.

Instructions

Please provide one response to each item in the questionnaire

1. Please indicate your age in years

- 65 - 70
- 71 - 74
- 75 - 79
- Over 80

2. Please indicate your highest level of education

- No schooling
- Some primary schooling completed
- Some secondary schooling completed
- Grade 12/Matric
- Higher certificate
- Diploma
- Degree
- Post graduate degree

3. Please indicate how long you have been using a mobile banking application

- Less than 6 months
- 6 months – less than 1 year
- 1 - 2 years
- 3 - 5 years
- Over 5 years

4. Please indicate all challenges related to using a mobile device as applicable to you

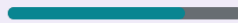
- I have difficulty remembering when using a mobile banking application
- I have difficulty concentrating when using a mobile banking application
- I have visual challenges when using a mobile banking application

5. Please indicate if you have someone authorized to help you and conduct banking on your behalf

- Yes
- No

[Back](#)

[Next](#)



Page 3 of 4

[Clear form](#)

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

AGED USERS' PERCEPTIONS OF THE SECURITY OF MOBILE BANKING APPLICATIONS

[Sign in to Google](#) to save your progress. [Learn more](#)

Section B: Perceptions of the factors influencing the security of mobile banking applications

The following questions relate to your perceptions of the factors influencing the security of mobile banking applications.

Please rate the items below by indicating your level of agreement with one of the five options next to each of the statements.

	Strongly disagree	Disagree	Agree	Strongly agree	Not applicable
The use of mobile banking applications is useful in my daily life.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of mobile banking applications helps me complete banking tasks quickly.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of mobile banking applications increases my productivity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Learning how to use mobile banking applications is easy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My interactions with mobile banking applications are clear and understandable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Mobile banking applications are easy to use.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy for me to become skilful at using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The people who are important to me think that I should use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The people who influence my behaviour think that I should use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The people whose opinions that I value prefer that I use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The people who are important to me support my use of mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have confidence in using mobile banking applications if my friends and family also use them.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I have the resources necessary to use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have the knowledge to use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications are compatible with other technologies (such as mobile phones) I use.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can get help from others when I have difficulties using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The financial institutions provide adequate support for using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using a mobile banking application is fun.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Using a mobile banking application is enjoyable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the mobile banking application is very exciting.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications are reasonably priced.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications provide good value for money.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
At the current price, the mobile banking applications provide good value.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of mobile banking applications has become a habit for me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am addicted to using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I must use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have adequate experience to use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

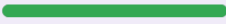
My personal information is safe when using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications provide adequate privacy protection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My transaction information is protected when using mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications keep my private information protected.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using mobile banking applications does not put my privacy at risk.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My funds are at no risk with the people I trust to help me use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If I use mobile banking applications, criminals cannot attempt to take over my account.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

There is little chance that I will lose my funds if I use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is harmless for me to use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can trust mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications restrict unauthorised access.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can trust mobile banking applications to accurately process transactions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile banking applications are secure.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My personal details on mobile banking applications are secure.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My transaction details on mobile banking applications are secure.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The mobile banking applications have strict security measures.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

My interaction on mobile banking applications is secure.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
There is nothing to worry about regarding the security of the mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I intend to continue using mobile banking applications in the future.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I will always try to use mobile banking applications in my daily life.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I plan to continue to use mobile banking applications frequently.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I regularly use mobile banking applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use mobile banking application for all my banking needs.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have increased my use of mobile banking applications over time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[Back](#)

[Submit](#)



Page 4 of 4

[Clear form](#)

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

D4: Aged users' questionnaire (printed)

AGED USERS' PERCEPTIONS OF THE FACTORS INFLUENCING THE SECURITY OF MOBILE BANKING APPLICATIONS QUESTIONNAIRE

Dear prospective participant

You are invited to participate in a survey conducted by Rumbidzai Goronga under the supervision of Prof A. da Veiga (School of Computing) and Prof. H. Lotriet (School of Computing) towards obtaining an MSc degree in Computing at the University of South Africa.

This survey has been designed to investigate the perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa. By completing this survey, you agree that the information you provide may be used for research purposes as well as for dissemination through peer-reviewed publications and conference proceedings. It is envisaged that the information we gain from this survey will help us to develop a security factors model that will help financial institutions in better designing mobile banking applications that are secure and easy to use for aged users. You are, however, under no obligation to complete the survey and may withdraw from the study at any time prior to submitting it. The survey has been developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, we will not be able to extract your information from the study once you have clicked the 'send' button. If you choose to participate in this survey, it will take no more than 15 minutes of your time. Although you as an individual will not benefit from your participation, it is envisioned that the findings of this study will improve the understanding of the perceptions of the factors that influence the security of mobile banking applications by aged users in South Africa from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. As researchers we undertake to keep any information provided herein confidential, not to let it go out of our possession, and to report on the findings from the perspective of the participating group (and not from that of an individual).

The records will be kept for five years for audit purposes, after which it will be permanently destroyed, and electronic versions will be deleted permanently from the hard drive of the computer. Furthermore, you will not be reimbursed or receive any incentives for your participation in the survey.

The research will be reviewed and approved by the School of Computing Research Ethics Committee. The primary researcher, Rumbidzai Goronga, can be contacted during office hours on . The study leader, Dr A. Da Veiga, is available during office hours on . Should you have any questions regarding the ethical aspects of the study, you may contact the chairperson of the School of Computing Research Ethics

Committee at . Alternatively, you can report any serious unethical behaviour on the University's toll-free hotline 0800 86 96 93.

You now make your decision on whether to participate by continuing to the next page. **You are still free to withdraw from the study at any time prior to starting or completing the study.**

I consent to the above and wish to proceed with the survey.

Information section

Your participation in this very important survey is sincerely appreciated. The questionnaire consists of two sections: Section A where demographic information is requested, and Section B with **53** questions on your perceptions of the factors that influence the security of mobile banking applications.

Please find the questionnaire on the next page. Completion is expected to take no more than 15 minutes.

Section A: Demographic Profile

We require some background information and would appreciate if you can please complete the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Indicate with a cross (X) for your selection

Demographic Profile								
1. Please indicate your age in years	65 - 70		71 - 74		75 - 79		Over 80	
2. Please indicate your highest level of education	No schooling	Some primary schooling completed	Some secondary schooling completed	Grade 12/Matric	Higher certificate	Diploma	Degree	Post graduate degree
3. Please indicate how long you have been using a mobile banking application	Less than 6 months		6 months – less than 1 year		1 - 2 years	3 - 5 years		Over 5 years
4. Please indicate all challenges related to	I have difficulty remembering when using a mobile banking application		I have difficulty concentrating when using a mobile banking application		I have visual challenges when using a mobile banking application			

Demographic Profile	
using a mobile device as applicable to you	
5. Please indicate if you have someone authorized to help you and conduct banking on your behalf	Yes
	No

Section B: Perceptions of the factors influencing the security of mobile banking applications

The following questions relate to your perceptions of the factors influencing the security of mobile banking applications. Please rate the items below by indicating your level of agreement with one of the five options next to each of the statements.

Perceptions of the factors influencing the security of mobile banking applications	Strongly disagree	Disagree	Neutral	Agree	Strong Agree
1. The use of mobile banking applications is useful in my daily life.					
2. The use of mobile banking applications helps me complete banking tasks quickly.					
3. The use of mobile banking applications increases my productivity.					
4. Learning how to use mobile banking applications is easy.					
5. My interactions with mobile banking applications are clear and understandable.					
6. Mobile banking applications are easy to use.					
7. It is easy for me to become skilful at using mobile banking applications.					
8. Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.					
9. The people who are important to me think that I should use mobile banking applications.					
10. The people who influence my behaviour think that I should use mobile banking applications.					

Perceptions of the factors influencing the security of mobile banking applications	Strongly disagree	Disagree	Neutral	Agree	Strong Agree
11. The people whose opinions that I value prefer that I use mobile banking applications.					
12. The people who are important to me support my use of mobile banking applications.					
13. I have confidence in using mobile banking applications if my friends and family also use them.					
14. I have the resources necessary to use mobile banking applications.					
15. I have the knowledge to use mobile banking applications.					
16. Mobile banking applications are compatible with other technologies (such as mobile phones) I use.					
17. I can get help from others when I have difficulties using mobile banking applications.					
18. The financial institutions provide adequate support for using mobile banking applications.					
19. Using a mobile banking application is fun.					
20. Using a mobile banking application is enjoyable.					
21. Using the mobile banking application is very exciting.					
22. Mobile banking applications are reasonably priced.					
23. Mobile banking applications provide good value for money.					

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
24.	At the current price, the mobile banking applications provide good value.					
25.	The use of mobile banking applications has become a habit for me.					
26.	I am addicted to using mobile banking applications.					
27.	I must use mobile banking applications.					
28.	I have adequate experience to use mobile banking applications.					
29.	My personal information is safe when using mobile banking applications.					
30.	Mobile banking applications provide adequate privacy protection.					
31.	Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.					
32.	My transaction information is protected when using mobile banking applications.					
33.	Mobile banking applications keep my private information protected.					
34.	Using mobile banking applications does not put my privacy at risk.					
35.	My funds are at no risk with the people I trust to help me use mobile banking applications.					
36.	If I use mobile banking applications, criminals cannot attempt to take over my account.					
37.	There is little chance that I will lose my funds if I use mobile banking applications.					

Perceptions of the factors influencing the security of mobile banking applications		Strongly disagree	Disagree	Neutral	Agree	Strong Agree
38.	It is harmless for me to use mobile banking applications.					
39.	I can trust mobile banking applications.					
40.	Mobile banking applications restrict unauthorised access.					
41.	I can trust mobile banking applications to accurately process transactions.					
42.	Mobile banking applications are secure.					
43.	My personal details on mobile banking applications are secure.					
44.	My transaction details on mobile banking applications are secure.					
45.	The mobile banking applications have strict security measures.					
46.	My interaction on mobile banking applications is secure.					
47.	There is nothing to worry about regarding the security of the mobile banking applications.					
48.	I intend to continue using mobile banking applications in the future.					
49.	I will always try to use mobile banking applications in my daily life.					
50.	I plan to continue to use mobile banking applications frequently.					
51.	I regularly use mobile banking applications.					
52.	I use mobile banking application for all my banking needs.					
53.	I have increased my use of mobile banking applications over time.					

Appendix E: Anonymous cover letter



Ethical Clearance #: 1026

COVER LETTER TO A SURVEY – HARDCOPY HANDOUT

Mobile banking applications security factors model for aged users in South Africa

Dear prospective participant

You are invited to participate in a survey conducted by Rumbidzai Goronga under the supervision of Prof A. da Veiga (School of Computing) and Prof. H. Lotriet (School of Computing) towards obtaining an MSc degree in Computing at the University of South Africa.

The survey you have received has been designed to study the perceptions of aged users on the factors that influence the security of mobile banking applications in South Africa. You were selected to participate in this survey because you are at least 65 years of age, reside in South Africa and make use of mobile banking applications. You will not be eligible to complete the survey if you are younger than 65 years of age, do not reside in South Africa and do not make use of mobile banking applications. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a security factors model that will help financial institutions in better designing mobile banking applications that are secure and easy to use for aged users. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the understanding of the perception of the factors that influence the security of mobile banking applications by aged users in South Africa from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. The researcher undertakes to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The records will be kept for a minimum period of five years for audit purposes where after it will be permanently destroyed, hard copies will be shredded, and electronic versions will be permanently deleted from the hard drive of the computer. You will not be reimbursed or receive any incentives for your participation in the survey.

The research has been reviewed and approved by the School of Computing Research Ethics Committee. The primary researcher, Rumbidzai Goronga, can be contacted during office hours on . The study leader, Dr A. Da Veiga, is available during office hours on . Should you have any questions regarding the ethical aspects of the study, you may contact the chairperson of the School of Computing Research Ethics Committee at . Alternatively, you can report any serious unethical behaviour on the University's toll-free hotline 0800 86 96 93.

You are deciding whether to participate by collecting a survey questionnaire print out. By completing the survey, you imply that you have consented to participate in this research. You are free to withdraw from the study at any time prior to clicking the completing the survey.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Gatekeeper to keep signed cover letter separate from complete questionnaire when collecting the signed forms and questionnaires.



Appendix F: Statistician's confidentiality agreement

1



UNISA RESEARCH ETHICS 3rd Party Confidentiality Agreement (Transcriber, Co-coder, Statistician and/or Fieldworkers)

A. INSTRUCTIONS

Please read through the entirety of this form carefully before signing.

After completing the required fields, please sign the form. After this form has been signed by the transcriber, co-coder, statistician or fieldworker, it should be given to the principal researcher for submission to the relevant UNISA Research Ethics Committee.

The transcriber, co-coder, statistician and/or fieldworker should keep a copy of the *Confidentiality Agreement* for their records.

B. CONFIDENTIALITY OF A RESEARCH STUDY

Confidentiality is the treatment and maintenance of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure (the informed consent documentation) without permission. Confidential information relating to human participants in a research study may include, but is not limited to the personal information listed below:

- a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;
- d) the biometric information of the person;
- e) the personal opinions, views or preferences of the person;
- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person; and
- h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Form adapted from the confidentiality agreement developed by the University of St Thomas IRB, retrieved from <https://www.stthomas.edu>

As a third party you will have access to research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) that include confidential information. Participants have revealed information to the researcher(s) since they have been assured by the researcher(s) that every effort will be made to maintain their privacy throughout the study. That is why it is of the utmost importance to maintain confidentiality when conducting your duties as a transcriber, statistician, co-coder and/or fieldworker during the research study. *Below is a list of expectations you will be required to adhere to in your role as a third party in this study. Review these expectations carefully before signing this form.*

C. THIRD PARTY EXPECTATIONS

To maintain confidentiality, I agree to:

1. Keep all research information that I collect or that is shared with me confidential by not discussing or sharing this information verbally or in any format with anyone other than the principal researcher of this study;
2. Ensure the security of research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) while it is in my possession. This includes:
 - Keeping all data and/or transcript documents and digitized interviews on a password protected computer with password-protected files;
 - Closing any programs and documents when temporarily away from the computer;
 - Keeping any printed transcripts or data in a secure location such as a locked file cabinet;
 - Permanently deleting any digital communication containing the data.
3. Not make copies of research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) unless specifically instructed to do so by the principal researcher;
4. Give all research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) and research participant information, back to the principal researcher upon completion of my duties as a transcriber;
5. After discussing it with the principal researcher, erase or destroy all research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) that cannot be returned to the principal researcher upon completion of my duties in this study.

Name of 3rd party involved in research activities: **Dr Liezel Korf**

Research activity responsible for (transcribing interviews, co-coding of data, statistical analysis, collecting data, etc.): **Statistical Analysis**

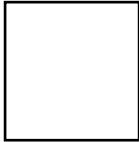
Title of Research Study: **Mobile banking applications security factors model for aged users in South Africa**

Name of Principal Researcher: **Rumbidzai Goronga**

By signing this form, I acknowledge that I have reviewed, understand, and agree to adhere to the expectations described above. I agree to maintain confidentiality while performing my duties as acquired

Form adapted from the confidentiality agreement developed by the University of St Thomas IRB, retrieved from <https://www.stthomas.edu>

by the principal researcher. I recognise that failure to comply with these expectations may result in legal action.



14 June 2023

Signature of 3rd party

Date

Dr Liezel Korf

Print Name

Appendix G: Factor loadings

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	20.645	38.953	38.953	20.645	38.953	38.953
2	5.724	10.799	49.752	5.724	10.799	49.752
3	3.247	6.127	55.879	3.247	6.127	55.879
4	1.833	3.458	59.337	1.833	3.458	59.337
5	1.687	3.183	62.519	1.687	3.183	62.519
6	1.509	2.848	65.368	1.509	2.848	65.368
7	1.206	2.276	67.643	1.206	2.276	67.643
8	1.154	2.177	69.820	1.154	2.177	69.820
9	1.141	2.152	71.972	1.141	2.152	71.972
10	0.922	1.740	73.712			
11	0.790	1.491	75.203			
12	0.729	1.375	76.578			
13	0.694	1.310	77.887			
14	0.673	1.270	79.157			
15	0.649	1.224	80.381			
16	0.607	1.146	81.527			
17	0.577	1.089	82.617			
18	0.541	1.020	83.637			
19	0.518	0.978	84.615			
20	0.475	0.896	85.511			
21	0.467	0.881	86.392			
22	0.457	0.862	87.254			
23	0.424	0.799	88.053			
24	0.410	0.774	88.827			
25	0.381	0.719	89.547			
26	0.375	0.707	90.253			
27	0.338	0.639	90.892			
28	0.326	0.615	91.507			
29	0.319	0.602	92.109			
30	0.294	0.555	92.664			
31	0.291	0.549	93.213			
32	0.263	0.495	93.708			
33	0.260	0.491	94.199			
34	0.251	0.473	94.672			
35	0.237	0.447	95.119			
36	0.229	0.432	95.551			
37	0.209	0.394	95.945			
38	0.207	0.390	96.335			
39	0.197	0.372	96.706			
40	0.186	0.351	97.058			
41	0.174	0.329	97.387			
42	0.170	0.320	97.707			
43	0.160	0.302	98.009			

44	0.146	0.276	98.285			
45	0.143	0.270	98.556			
46	0.123	0.231	98.787			
47	0.118	0.223	99.010			
48	0.109	0.205	99.216			
49	0.099	0.186	99.402			
50	0.094	0.177	99.578			
51	0.080	0.152	99.730			
52	0.074	0.140	99.870			
53	0.069	0.130	100.000			
Extraction Method: Principal Component Analysis.						

Appendix H: Reliability statistics

Scale: Technological security perception

Case Processing Summary

		N	%
Cases	Valid	284	99.3
	Excluded ^a	2	0.7
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.911	0.912	4

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.722	0.628	0.852	0.223	1.355	0.007	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PS4 The mobile banking applications have strict security measures.	9.71	4.268	0.799	0.689	0.886

PS5 My interaction on mobile banking applications is secure.	9.80	4.128	0.766	0.664	0.896
PP4 My transaction information is protected when using mobile banking applications.	9.77	3.859	0.841	0.769	0.870
PP5 Mobile banking applications keep my private information protected.	9.82	3.934	0.794	0.733	0.887

Scale: Expected effort

Case Processing Summary

		N	%
Cases	Valid	286	100.0
	Excluded ^a	0	0.0
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.873	0.875	5

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.583	0.441	0.671	0.231	1.523	0.007	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
EE1 Learning how to use mobile banking applications is easy.	11.79	5.965	0.708	0.523	0.844
EE2 My interactions with mobile banking applications are clear and understandable.	11.40	5.862	0.762	0.582	0.830
EE3 Mobile banking applications are easy to use.	11.79	6.028	0.719	0.556	0.841
EE4 It is easy for me to become skilful at using mobile banking applications.	11.61	6.133	0.750	0.573	0.835
EE5 Elements on the mobile banking application (such as screen display) make it easy to use mobile banking applications.	11.61	6.260	0.576	0.354	0.877

Scale: Societal impact

Case Processing Summary

		N	%
Cases	Valid	283	99.0
	Excluded ^a	3	1.0
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.868	0.872	4

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.629	0.557	0.779	0.222	1.399	0.006	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
SI1 The people who are important to me think that I should use mobile banking applications.	10.08	4.794	0.676	0.458	0.849
SI2 The people who influence my behaviour think that I should use mobile banking applications.	10.22	4.255	0.665	0.453	0.859
SI3 The people whose opinions that I value prefer that I use mobile banking applications.	9.94	4.387	0.804	0.677	0.800
SI4 The people who are important to me support my use of mobile banking applications.	9.95	4.221	0.754	0.633	0.817

Scale: Privacy and risk

Case Processing Summary

		N	%
Cases	Valid	286	100.0
	Excluded ^a	0	0.0
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.927	0.928	7

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.649	0.502	0.808	0.306	1.609	0.008	7

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PR1 Using mobile banking applications does not put my privacy at risk.	18.83	16.783	0.794	0.654	0.913
PP1 My personal information is safe when using mobile banking applications.	18.63	17.708	0.773	0.702	0.916

PP2 Mobile banking applications provide adequate privacy protection.	18.59	17.541	0.778	0.715	0.915
PP3 Unauthorised people will not be able to view the details I input while transacting on the mobile banking application.	18.69	17.028	0.817	0.716	0.911
PR4 There is little chance that I will lose my funds if I use mobile banking applications.	18.62	16.329	0.829	0.723	0.910
PR3 If I use mobile banking applications, criminals cannot attempt to take over my account.	18.85	16.388	0.766	0.660	0.917
PS6 There is nothing to worry about regarding the security of the mobile banking applications.	18.88	17.771	0.647	0.436	0.927

Scale: Tangible benefits

Case Processing Summary

		N	%
Cases	Valid	285	99.7
	Excluded ^a	1	0.3
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
------------------	--	------------

0.870

0.879

5

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.592	0.408	0.843	0.434	2.064	0.022	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PV1 Mobile banking applications are reasonably priced.	13.87	6.740	0.764	0.672	0.824
PV2 Mobile banking applications provide good value for money.	13.72	7.011	0.832	0.785	0.810
PV3 At the current price, the mobile banking applications provide good value.	13.72	7.555	0.802	0.730	0.824
FC4 I can get help from others when I have difficulties using mobile banking applications.	13.89	7.508	0.622	0.398	0.860
FC5 The financial institutions provide adequate support for using mobile banking applications.	14.22	7.523	0.522	0.291	0.890

Scale: Risk behaviour

Case Processing Summary

		N	%
Cases	Valid	285	99.7
	Excluded ^a	1	0.3
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.763	0.770	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.527	0.507	0.545	0.038	1.075	0.000	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PR5 It is harmless for me to use mobile banking applications.	6.01	2.017	0.599	0.363	0.687
UB2 I use mobile banking application for all my banking needs.	6.07	1.576	0.590	0.348	0.703

BI2 I will always try to use mobile banking applications in my daily life.	6.00	1.824	0.616	0.383	0.659
--	------	-------	-------	-------	-------

Scale: Hedonistic drive

Case Processing Summary

		N	%
Cases	Valid	286	100.0
	Excluded ^a	0	0.0
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.919	0.921	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.796	0.743	0.836	0.093	1.125	0.002	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
HM1 Using a mobile banking application is fun.	5.95	3.671	0.828	0.713	0.890

HM2 Using a mobile banking application is enjoyable.	5.90	3.561	0.880	0.777	0.850
HM3 Using the mobile banking application is very exciting.	6.02	3.315	0.809	0.668	0.911

Scale: Intent and use behaviour

Case Processing Summary

		N	%
Cases	Valid	286	100.0
	Excluded ^a	0	0.0
	Total	286	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.880	0.879	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.709	0.664	0.760	0.096	1.145	0.002	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted

B11 I intend to continue using mobile banking applications in the future.	6.64	2.028	0.773	0.612	0.824
B13 I plan to continue to use mobile banking applications frequently.	6.72	2.000	0.802	0.647	0.798
UB3 I have increased my use of mobile banking applications over time.	6.42	2.174	0.728	0.532	0.864

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,763	0,77	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0,527	0,507	0,545	0,038	1,075	0	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PR5 It is harmless for me to use mobile banking applications.	6,01	2,017	0,599	0,363	0,687
UB2 I use mobile banking application for all my banking needs.	6,07	1,576	0,59	0,348	0,703
BI2 I will always try to use mobile banking applications in my daily life.	6	1,824	0,616	0,383	0,659

Scale: Hedonistic drive

Case Processing Summary

		N	%
Cases	Valid	286	100
	Excluded ^a	0	0
	Total	286	100

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,919	0,921	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0,796	0,743	0,836	0,093	1,125	0,002	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
HM1 Using a mobile banking application is fun.	5,95	3,671	0,828	0,713	0,89
HM2 Using a mobile banking application is enjoyable.	5,9	3,561	0,88	0,777	0,85
HM3 Using the mobile banking application is very exciting.	6,02	3,315	0,809	0,668	0,911

Scale: Intent and Use Behaviour

Case Processing Summary

		N	%
Cases	Valid	286	100
	Excluded ^a	0	0
	Total	286	100

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0,88	0,879	3

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0,709	0,664	0,76	0,096	1,145	0,002	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
BI1 I intend to continue using mobile banking applications in the future.	6,64	2,028	0,773	0,612	0,824
BI3 I plan to continue to use mobile banking applications frequently.	6,72	2	0,802	0,647	0,798
UB3 I have increased my use of mobile banking applications over time.	6,42	2,174	0,728	0,532	0,864

Appendix I: Structured Equation Modelling (SEM)

	OIM	Standardized		z	P> z	[95%	Conf.
		Coef.	Std. Err.				
Technological_security_perception							
Expected_effort		0.142838	0.041026	3.48	0.000	0.062429	0.223247
Societal_impact		0.134265	0.034404	3.9	0.000	0.066834	0.201696
Privacy_and_risk		0.779079	0.029659	26.27	0.000	0.720949	0.837209
Tangible_benefits		-0.0729	0.045583	-1.6	0.110	-0.16224	0.016443
Hedonistic_drive		-0.01438	0.040705	-0.35	0.724	-0.09416	0.065402
_cons		0.74162	0.260593	2.85	0.004	0.230868	1.252371
Risk_behaviour							
Technological_security_perce~o		0.60467	0.03619	16.71	0.000	0.533738	0.675602
_cons		1.849624	0.323277	5.72	0.000	1.216013	2.483235
Intent_and_use_behaviour							
Risk_behaviour		0.654694	0.034012	19.25	0.000	0.588031	0.721356
_cons		2.098378	0.306308	6.85	0.000	1.498025	2.69873

Tangible_benefits removed, Hedonistic_drive removed

Standardized	OIM	Coef.	Std.	Err.	z	P> z	[95%
Technological_security_perception							
Expected_effort		0.109829	0.034534	3.18	0.001	0.042144	0.177514
Societal_impact		0.118217	0.03345	3.53	0	0.052656	0.183779
Privacy_and_risk		0.751349	0.025991	28.91	0	0.700407	0.80229
_cons		0.614915	0.248112	2.48	0.013	0.128625	1.101205
Risk_behaviour							
Technological_security_perception		0.60467	0.036208	16.7	0	0.533704	0.675636
_cons		1.849624	0.323283	5.72	0	1.216001	2.483247
Intent_and_use_behaviour							
Risk_behaviour		0.654694	0.034015	19.25	0	0.588026	0.721361
_cons		2.098378	0.306309	6.85	0	1.498022	2.698733

Modification indices applied

	Standardized		Coef.	Std.	Err.	z	P> z	[95%
Structural								
	Technological_security_perception							
	Expected_effort		0.228143	0.032332	7.06	0	0.164773	0.291512
	Societal_impact		0.13468	0.029546	4.56	0	0.076772	0.192588
	Privacy_and_risk		0.667838	0.032394	20.62	0	0.604348	0.731329

	Standardized		Coef.	Std.	Err.	z	P> z	[95%
	_cons		0.354255	0.234366	1.51	0.131	-0.1051	0.813604
	Risk_behaviour							
	Technological_security_perce~o		0.773764	0.039833	19.43	0	0.695694	0.851835
	_cons		0.922968	0.350172	2.64	0.008	0.236643	1.609293
	Intent_and_use_behaviour							
	Risk_behaviour		1.085925	0.055952	19.41	0	0.976262	1.195589
	_cons		-0.12819	0.418682	-0.31	0.759	-0.94879	0.692412
	mean(Expected_effort)	4.817566	0.212932	22.62	0	4.400228	5.234904	
	mean(Societal_impact)	5.831283	0.25447	22.92	0	5.33253	6.330035	
	mean(Privacy_and_risk)	4.853564	0.214397	22.64	0	4.433354	5.273774	
	var(e.Technological_security_p~o)	0.294549	0.030459	0.240511	0.360728			
	var(e.Risk_behaviour)	0.662968	0.051863	0.568728	0.772823			
	var(e.Intent_and_use_behaviour)	0.757337	0.096167	0.590477	0.971348			
	var(Expected_effort)	1	.	.	.			
	var(Societal_impact)	1	.	.	.			
	var(Privacy_and_risk)	1	.	.	.			
	cov(e.Technological_security_p~o,							
	e.Risk_behaviour)	-0.38265	0.062652	-6.11	0	-0.50545	-0.25986	

	Standardized		Coef.	Std.	Err.	z	P> z	[95%
	cov(e.Technological_security_p~o,							
REMOVED	e.Intent_and_use_behaviour)	-0.12489	0.059981	-2.08	0.037	-0.24244	-0.00733	
	cov(e.Risk_behaviour,							
	e.Intent_and_use_behaviour)	-0.54417	0.060944	-8.93	0	-0.66362	-0.42473	
CANNOT BE REMOVED - IMPLIED BY MODEL	cov(Expected_effort,							
	Societal_impact)	0.133447	0.058908	2.27	0.023	0.01799	0.248905	
	cov(Expected_effort,							
	Privacy_and_risk)	0.400538	0.050354	7.95	0	0.301846	0.49923	
	cov(Societal_impact,							
	Privacy_and_risk)	0.327984	0.053524	6.13	0	0.223078	0.432889	

Non-significant paths removed

Standardized	OIM	Coef.	Std.	Err.	z	P> z	[95%
Technological_security_perception							
Expected_effort		0.222552	0.032639	6.82	0	0.158581	0.286523
Societal_impact		0.12657	0.029497	4.29	0	0.068756	0.184384
Privacy_and_risk		0.676143	0.032035	21.11	0	0.613356	0.73893
_cons		0.388176	0.235053	1.65	0.099	-0.07252	0.848871
Risk_behaviour							

Standardized	OIM	Coef.	Std.	Err.	z	P> z	[95%
Technological_security_perception		0.778023	0.039732	19.58	0	0.70015	0.855895
_cons		0.899632	0.359021	2.51	0.012	0.195964	1.6033
Intent_and_use_behaviour							
Risk_behaviour		1.070778	0.055358	19.34	0	0.962278	1.179277
_cons		-0.04998	0.414918	-0.12	0.904	-0.8632	0.763246

Appendix J: Multiple regression analysis

Regression

Notes

Input	N of Rows in Working Data File	278
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.

Descriptive Statistics

	Mean	Std. Deviation	N
Technological security perception	3.2866	0.60081	278
Expected effort	2.9137	0.60589	278
Societal impact	3.3801	0.58069	278
Privacy and risk	3.1465	0.64945	278
Tangible_benefits	3.5180	0.55215	278
Hedonistic drive	2.9976	0.88848	278

Correlations

		Technological security perception	Expected effort	Societal impact	Privacy and risk	Tangible_benefits	Hedonistic drive
Pearson Correlation	Technological security perception	1.000	0.427	0.379	0.834	0.492	0.285
	Expected effort	0.427	1.000	0.133	0.401	0.522	0.570
	Societal impact	0.379	0.133	1.000	0.328	0.375	0.152
	Privacy and risk	0.834	0.401	0.328	1.000	0.574	0.302
	Tangible_benefits	0.492	0.522	0.375	0.574	1.000	0.522
	Hedonistic drive	0.285	0.570	0.152	0.302	0.522	1.000

		Technological security perception	Expected effort	Societal impact	Privacy and risk	Tangible benefits	Hedonistic drive
Sig. (1-tailed)	Technological security perception		0.000	0.000	0.000	0.000	0.000
	Expected effort	0.000		0.013	0.000	0.000	0.000
	Societal impact	0.000	0.013		0.000	0.000	0.006
	Privacy and risk	0.000	0.000	0.000		0.000	0.000
	Tangible_benefits	0.000	0.000	0.000	0.000		0.000
	Hedonistic drive	0.000	0.000	0.006	0.000	0.000	
N	Technological security perception	278	278	278	278	278	278
	Expected effort	278	278	278	278	278	278
	Societal impact	278	278	278	278	278	278
	Privacy and risk	278	278	278	278	278	278
	Tangible_benefits	278	278	278	278	278	278
	Hedonistic drive	278	278	278	278	278	278

Variables Entered/Removed^a

Model	Variables Entered	Variables Removed	Method
1	Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits ^b		Enter
a. Dependent Variable: Technological security perception			
b. All requested variables entered.			

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.850 ^a	0.722	0.717	0.31984	1.588
a. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits					
b. Dependent Variable: Technological security perception					

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	72.165	5	14.433	141.093	<.001 ^b
	Residual	27.824	272	0.102		
	Total	99.989	277			
a. Dependent Variable: Technological security perception						
b. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits						

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	0.445	0.149		2.985	0.003		
	Expected effort	0.142	0.041	0.143	3.420	0.001	0.587	1.705
	Societal impact	0.139	0.036	0.134	3.827	0.000	0.831	1.203
	Privacy and risk	0.721	0.037	0.779	19.438	0.000	0.637	1.570
	Tangible_benefits	-0.079	0.050	-0.073	-1.580	0.115	0.480	2.082
	Hedonistic drive	-0.010	0.028	-0.014	-0.349	0.727	0.604	1.656
a. Dependent Variable: Technological security perception								

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions					
				(Constant)	Expected effort	Societal impact	Privacy and risk	Tangible benefits	Hedonistic drive
1	1	5.872	1.000	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.059	9.999	0.02	0.02	0.07	0.03	0.00	0.54
	3	0.026	15.137	0.03	0.14	0.30	0.40	0.00	0.14
	4	0.021	16.533	0.07	0.56	0.01	0.36	0.00	0.21
	5	0.013	21.633	0.63	0.27	0.61	0.00	0.05	0.01
	6	0.009	25.100	0.24	0.01	0.01	0.20	0.95	0.10

a. Dependent Variable: Technological security perception

Casewise Diagnostics^a

b	Std. Residual	Technological security perception	Predicted Value	Residual
59	4.790	3.00	1.4680	1.53201
63	-3.025	0.00	0.9675	-0.96749
214	-4.311	1.50	2.8788	-1.37880

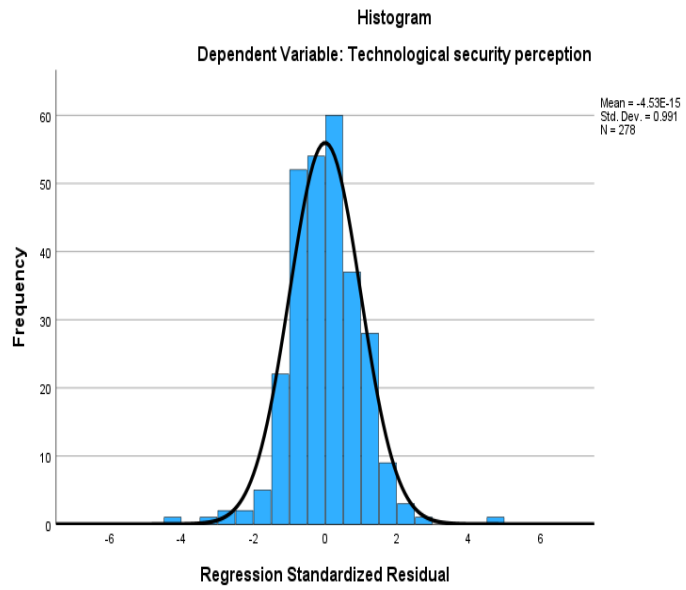
a. Dependent Variable: Technological security perception

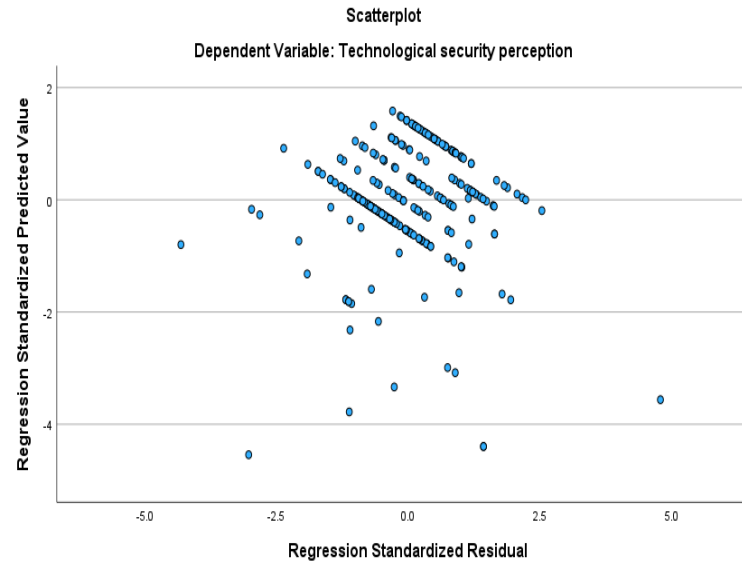
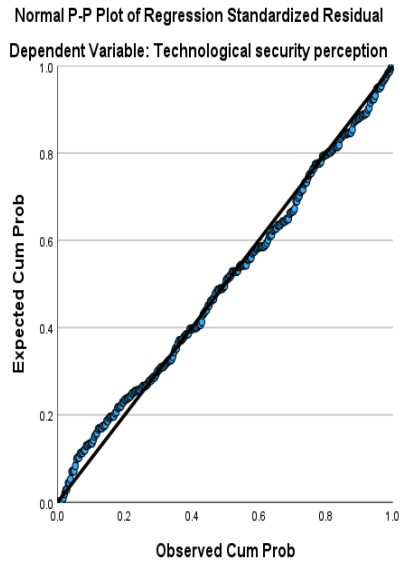
Residuals Statistics^a

	b	Maximum	Mean	Std. Deviation	N
Predicted Value	0.9675	4.0938	3.2866	0.51042	278
Residual	-1.37880	1.53201	0.00000	0.31694	278
Std. Predicted Value	-4.544	1.581	0.000	1.000	278
Std. Residual	-4.311	4.790	0.000	0.991	278

a. Dependent Variable: Technological security perception

Charts





Regression 3 outliers removed

Notes

Input	N of Rows in Working Data File	275
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.

Descriptive Statistics

	Mean	Std. Deviation	N
Technological security perception	3.3061	0.55962	275
Expected effort	2.9207	0.60434	275

Societal impact	3.3870	0.56455	275
Privacy and risk	3.1668	0.61562	275
Tangible_benefits	3.5185	0.55374	275
Hedonistic drive	2.9988	0.89311	275

Correlations

		Technological security perception	Expected effort	Societal impact	Privacy and risk	Tangible_benefits	Hedonistic drive
Pearson Correlation	Technological security perception	1.000	0.417	0.345	0.846	0.529	0.303
	Expected effort	0.417	1.000	0.112	0.386	0.524	0.574
	Societal impact	0.345	0.112	1.000	0.295	0.376	0.159
	Privacy and risk	0.846	0.386	0.295	1.000	0.597	0.319
	Tangible_benefits	0.529	0.524	0.376	0.597	1.000	0.524
	Hedonistic drive	0.303	0.574	0.159	0.319	0.524	1.000
Sig. (1-tailed)	Technological security perception		0.000	0.000	0.000	0.000	0.000
	Expected effort	0.000		0.032	0.000	0.000	0.000
	Societal impact	0.000	0.032		0.000	0.000	0.004
	Privacy and risk	0.000	0.000	0.000		0.000	0.000
	Tangible_benefits	0.000	0.000	0.000	0.000		0.000
	Hedonistic drive	0.000	0.000	0.004	0.000	0.000	
N	Technological security perception	275	275	275	275	275	275
	Expected effort	275	275	275	275	275	275
	Societal impact	275	275	275	275	275	275
	Privacy and risk	275	275	275	275	275	275
	Tangible_benefits	275	275	275	275	275	275
	Hedonistic drive	275	275	275	275	275	275

Variables Entered/Removed^a

Model	Variables Entered	Variables Removed	Method
1	Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits ^b		Enter
a. Dependent Variable: Technological security perception			
b. All requested variables entered.			

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.858 ^a	0.737	0.732	0.28964	0.008
a. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits					
b. Dependent Variable: Technological security perception					

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	63.242	5	12.648	150.766	<.001 ^b
	Residual	22.568	269	0.084		
	Total	85.809	274			
a. Dependent Variable: Technological security perception						
b. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits						

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	0.474	0.139		3.412	0.001		
	Expected effort	0.124	0.038	0.134	3.288	0.001	0.588	1.702
	Societal impact	0.116	0.034	0.117	3.414	0.001	0.838	1.193
	Privacy and risk	0.723	0.036	0.795	20.163	0.000	0.628	1.592
	Tangible_benefits	-0.049	0.047	-0.049	-1.051	0.294	0.458	2.186
	Hedonistic drive	-0.013	0.025	-0.021	-0.516	0.606	0.601	1.664

a. Dependent Variable: Technological security perception

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions					
				(Constant)	Expected effort	Societal impact	Privacy and risk	Tangible_benefits	Hedonistic drive
1	1	5.876	1.000	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.059	10.019	0.02	0.02	0.06	0.02	0.00	0.54
	3	0.025	15.460	0.01	0.27	0.33	0.21	0.00	0.24
	4	0.021	16.786	0.07	0.46	0.01	0.49	0.01	0.11
	5	0.012	22.596	0.82	0.22	0.55	0.01	0.00	0.03
	6	0.009	25.589	0.08	0.03	0.05	0.28	0.99	0.08

a. Dependent Variable: Technological security perception

Casewise Diagnostics^a

Case Number	Std. Residual	Technological security perception	Predicted Value	Residual
3	-3.297	2.25	3.2049	-0.95494
4	-3.138	2.25	3.1590	-0.90905

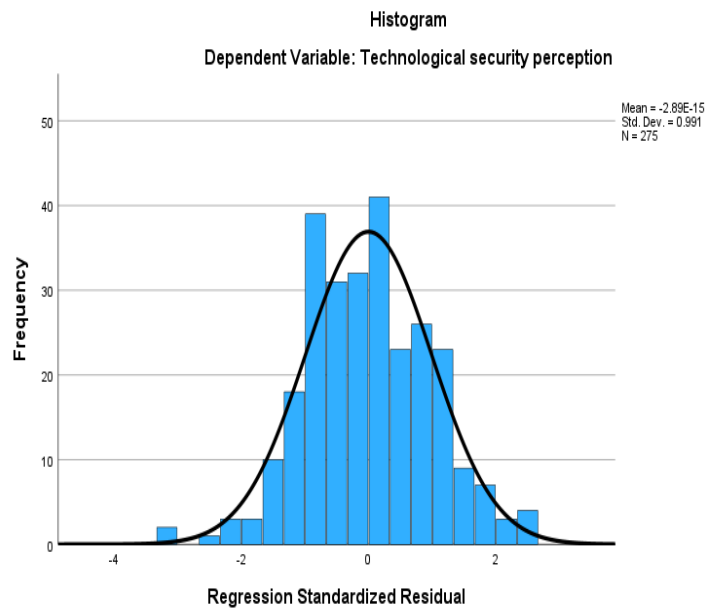
a. Dependent Variable: Technological security perception

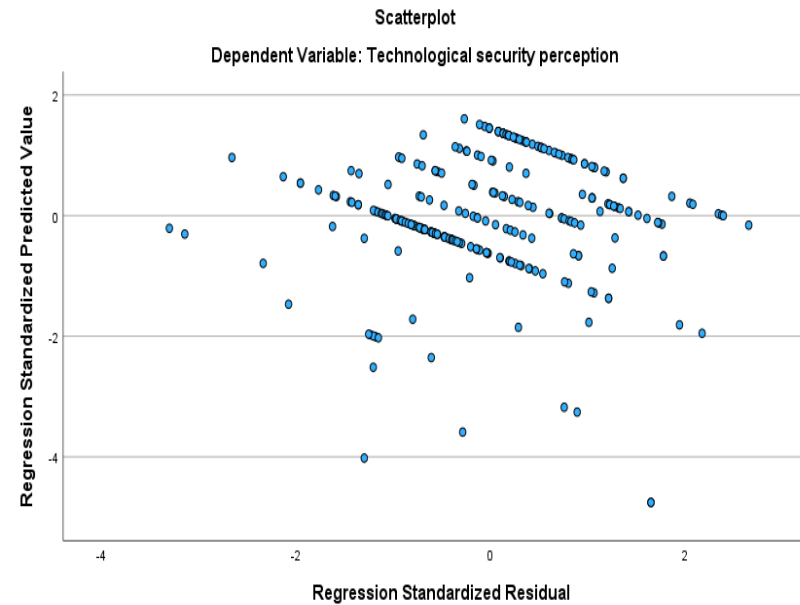
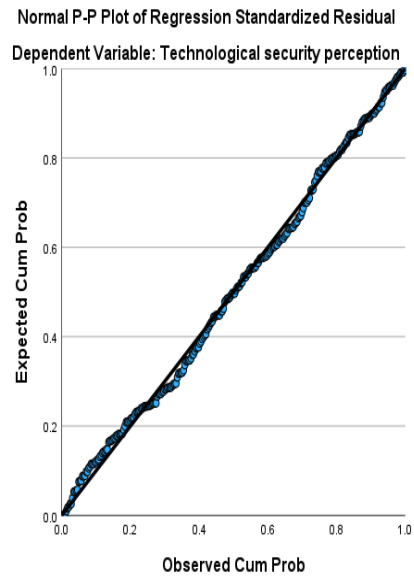
Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.0211	4.0767	3.3061	0.48043	275
Residual	-0.95494	0.77022	0.00000	0.28699	275
Std. Predicted Value	-4.756	1.604	0.000	1.000	275
Std. Residual	-3.297	2.659	0.000	0.991	275

a. Dependent Variable: Technological security perception

Charts





Regression 5 outliers removed

Notes

Input	N of Rows in Working Data File	273
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.

Descriptive Statistics

	Mean	Std. Deviation	N
Technological security perception	3.3138	0.55427	273

Expected effort	2.9216	0.60623	273
Societal impact	3.3852	0.56615	273
Privacy and risk	3.1680	0.61771	273
Tangible_benefits	3.5165	0.55498	273
Hedonistic drive	2.9976	0.89525	273

Correlations

		Technological security perception	Expected effort	Societal impact	Privacy and risk	Tangible_benefits	Hedonistic drive
Pearson Correlation	Technological security perception	1.000	0.420	0.356	0.854	0.544	0.310
	Expected effort	0.420	1.000	0.112	0.386	0.525	0.574
	Societal impact	0.356	0.112	1.000	0.297	0.375	0.158
	Privacy and risk	0.854	0.386	0.297	1.000	0.599	0.320
	Tangible_benefits	0.544	0.525	0.375	0.599	1.000	0.523
	Hedonistic drive	0.310	0.574	0.158	0.320	0.523	1.000
Sig. (1-tailed)	Technological security perception		0.000	0.000	0.000	0.000	0.000
	Expected effort	0.000		0.032	0.000	0.000	0.000
	Societal impact	0.000	0.032		0.000	0.000	0.005
	Privacy and risk	0.000	0.000	0.000		0.000	0.000
	Tangible_benefits	0.000	0.000	0.000	0.000		0.000
	Hedonistic drive	0.000	0.000	0.005	0.000	0.000	
N	Technological security perception	273	273	273	273	273	273
	Expected effort	273	273	273	273	273	273
	Societal impact	273	273	273	273	273	273
	Privacy and risk	273	273	273	273	273	273
	Tangible_benefits	273	273	273	273	273	273

	Hedonistic drive	273	273	273	273	273	273
--	------------------	-----	-----	-----	-----	-----	-----

Variables Entered/Removed^a

Model	Variables Entered	Variables Removed	Method
1	Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits ^b		Enter

a. Dependent Variable: Technological security perception

b. All requested variables entered.

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.867 ^a	0.751	0.746	0.27913	1.922

a. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits

b. Dependent Variable: Technological security perception

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	62.760	5	12.552	161.107	<.001 ^b
	Residual	20.802	267	0.078		
	Total	83.562	272			

a. Dependent Variable: Technological security perception

b. Predictors: (Constant), Hedonistic drive, Societal impact, Privacy and risk, Expected effort, Tangible_benefits

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	0.465	0.134		3.472	0.001		
	Expected effort	0.117	0.036	0.129	3.225	0.001	0.587	1.703
	Societal impact	0.119	0.033	0.122	3.651	0.000	0.839	1.191
	Privacy and risk	0.713	0.035	0.795	20.600	0.000	0.626	1.597
	Tangible_benefits	-0.035	0.045	-0.035	-0.772	0.441	0.457	2.189
	Hedonistic drive	-0.012	0.024	-0.019	-0.481	0.631	0.602	1.662

a. Dependent Variable: Technological security perception

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions					
				(Constant)	Expected effort	Societal impact	Privacy and risk	Tangible_benefits	Hedonistic drive
1	1	5.875	1.000	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.059	9.990	0.02	0.02	0.07	0.02	0.00	0.54
	3	0.025	15.431	0.01	0.27	0.33	0.21	0.00	0.24
	4	0.021	16.730	0.07	0.46	0.01	0.49	0.01	0.11
	5	0.012	22.515	0.82	0.22	0.55	0.01	0.00	0.03
	6	0.009	25.548	0.08	0.03	0.04	0.28	0.99	0.07

a. Dependent Variable: Technological security perception

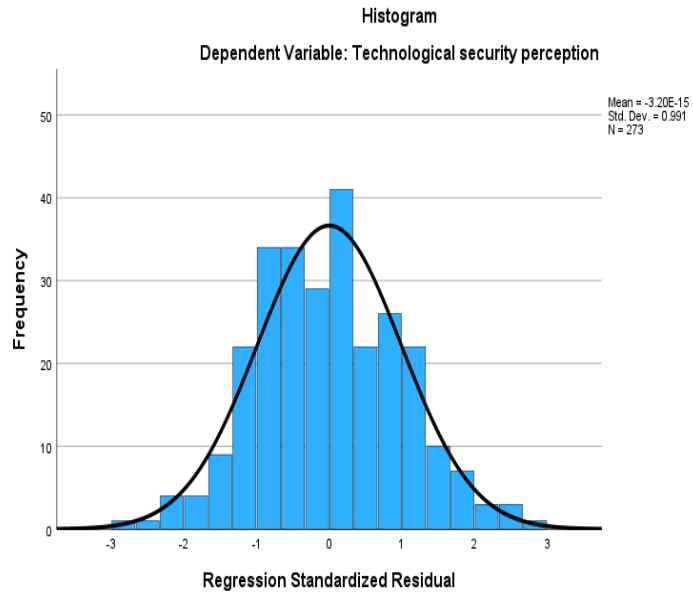
Residuals Statistics^a

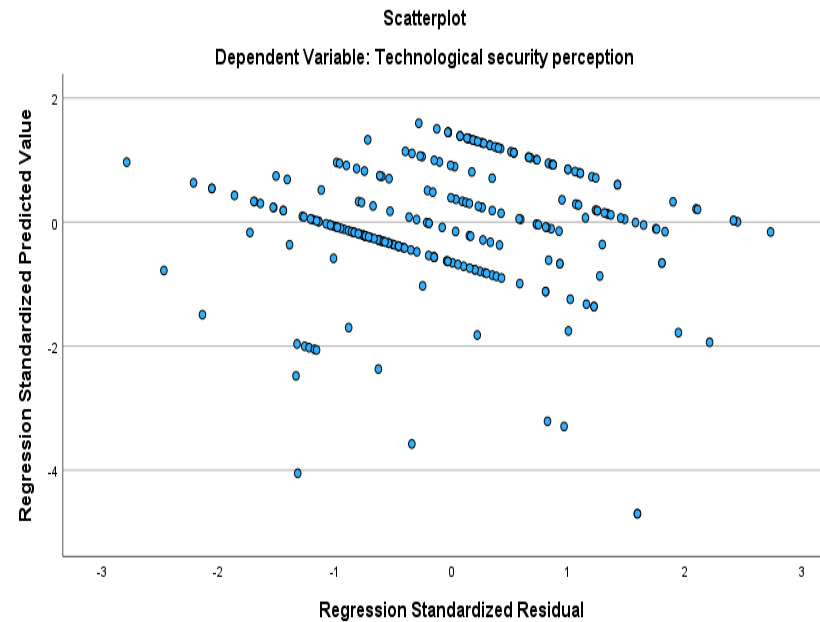
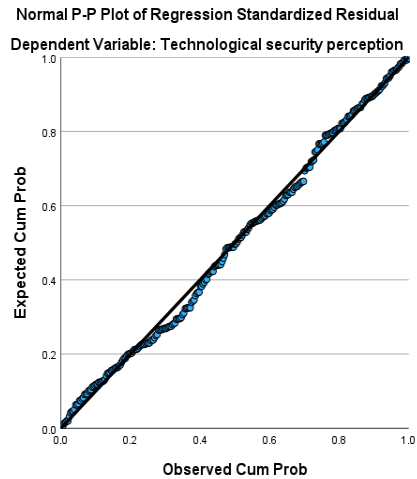
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.0556	4.0787	3.3138	0.48035	273
Residual	-0.77768	0.76314	0.00000	0.27655	273
Std. Predicted Value	-4.701	1.592	0.000	1.000	273

Std. Residual	-2.786	2.734	0.000	0.991	273
---------------	--------	-------	-------	-------	-----

a. Dependent Variable: Technological security perception

Charts





Regression 5 outliers removed only significant predictors

Notes

Input	N of Rows in Working Data File	273
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on cases with no missing values for any variable used.

Descriptive Statistics

	Mean	Std. Deviation	N
Technological security perception	3.3138	0.55427	273
Expected effort	2.9216	0.60623	273
Societal impact	3.3852	0.56615	273
Privacy and risk	3.1680	0.61771	273

Correlations

		Technological security perception	Expected effort	Societal impact	Privacy and risk
Pearson Correlation	Technological security perception	1.000	0.420	0.356	0.854
	Expected effort	0.420	1.000	0.112	0.386
	Societal impact	0.356	0.112	1.000	0.297
	Privacy and risk	0.854	0.386	0.297	1.000
Sig. (1-tailed)	Technological security perception		0.000	0.000	0.000
	Expected effort	0.000		0.032	0.000
	Societal impact	0.000	0.032		0.000
	Privacy and risk	0.000	0.000	0.000	
N	Technological security perception	273	273	273	273
	Expected effort	273	273	273	273
	Societal impact	273	273	273	273
	Privacy and risk	273	273	273	273

Variables Entered/Removed^a

Model	Variables Entered	Variables Removed	Method
--------------	--------------------------	--------------------------	---------------

1	Privacy and risk, Societal impact, Expected effort ^b		Enter
a. Dependent Variable: Technological security perception			
b. All requested variables entered.			

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.866 ^a	0.750	0.747	0.27867	1.884
a. Predictors: (Constant), Privacy and risk, Societal impact, Expected effort					
b. Dependent Variable: Technological security perception					

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	62.672	3	20.891	269.004	<.001 ^b
	Residual	20.890	269	0.078		
	Total	83.562	272			

- a. Dependent Variable: Technological security perception
b. Predictors: (Constant), Privacy and risk, Societal impact, Expected effort

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	0.441	0.129		3.406	0.001		
	Expected effort	0.097	0.030	0.106	3.221	0.001	0.851	1.175
	Societal impact	0.110	0.031	0.113	3.533	0.000	0.912	1.096

	Privacy and risk	0.699	0.031	0.779	22.664	0.000	0.786	1.272
a. Dependent Variable: Technological security perception								

Collinearity Diagnostics^a

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions			
				(Constant)	Expected effort	Societal impact	Privacy and risk
1	1	3.935	1.000	0.00	0.00	0.00	0.00
	2	0.031	11.205	0.02	0.65	0.30	0.00
	3	0.022	13.507	0.05	0.19	0.09	0.99
	4	0.012	18.202	0.93	0.16	0.61	0.00

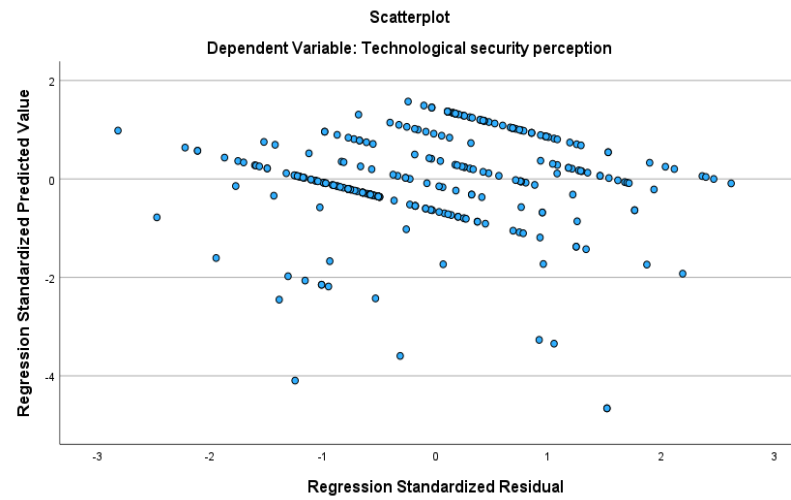
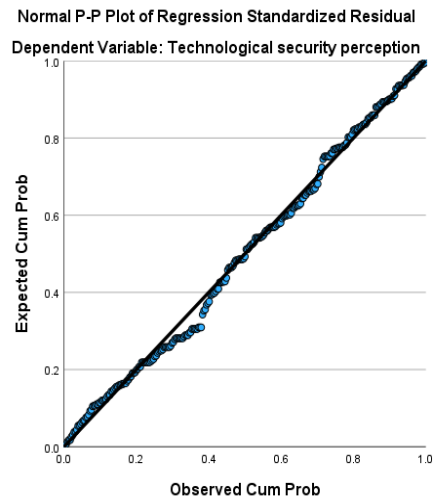
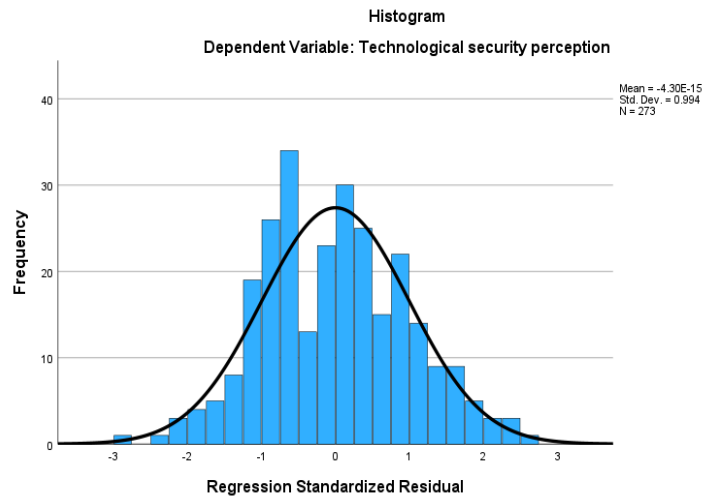
a. Dependent Variable: Technological security perception

Residuals Statistics^a

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.0770	4.0684	3.3138	0.48001	273
Residual	-0.78516	0.72975	0.00000	0.27713	273
Std. Predicted Value	-4.660	1.572	0.000	1.000	273
Std. Residual	-2.817	2.619	0.000	0.994	273

a. Dependent Variable: Technological security perception

Charts



Appendix K: Editorial certificate



CERTIFICATE OF EDITING

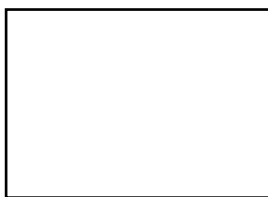
20 December 2023

This document serves to confirm that Rumbidzai P Goronga submitted the following dissertation for editing and proofreading:

Mobile banking application security factors model for aged users in South Africa

- The document was edited as per UK/SA English, in accordance with academic writing conventions.
- The focus of the edit was on consistency of grammar, spelling, and word use, conciseness of text, and clarity of meaning.
- It is the responsibility of the thesis author to implement the recommended edits to the original document

Please contact me if any additional information is required



Dr Isabel Meyer
PhD MBA BVSc

Impact Advantage, Postnet Suite 0103, Private Bag X37, Lynnwood Ridge, 0040, isabel@impactadvantage.co.za