The Impact of Demographic Indicators on Cybersecurity Behaviour of E-Commerce Users in South Africa

Weston Zorodzai Mberikwazvo

1789533

1789533@students.wits.ac.za

061 264 2961

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

Johannesburg, 2024

DECLARATION

I, Weston Zorodzai Mberikwazvo declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at this or any other university.

Name: Weston Zorodzai Mberikwazvo Signature:

Signed at Johannesburg

On the 26th of August 2024

ABSTRACT

This study aims to explore the cybersecurity behaviour of e-commerce users in South Africa, utilising a conceptual framework derived from some elements of both the Health Belief Model (HBM) and the Protection Motivation Theory (PMT). The study investigates the impact of demographic indicators specifically age, gender, and educational level impact the cybersecurity behaviour seeking to understand and contribute to the understanding of cybersecurity practices in response to perceived cyberthreats. A sample of 316 participants was used for the study which varied across different genders, age groups and educational levels. An online survey making use of a questionnaire was used to gather responses to the different dimensions making up cybersecurity behaviour guided by the established conceptual framework. The responses were statistically analysed to establish any patterns and trends using techniques such as correlation analysis and factor analysis. Analysis of the dataset concluded that there was significant difference to the cybersecurity behaviour of e-commerce users in South Africa for each of the demographic indicators of educational level, gender, and age and thus the null hypothesis was rejected for all three factors. Also, the null hypothesis was rejected for a combination of all three demographic indicators and cybersecurity behaviour indicating that a significant difference exists. The results showed that participants in the 36 to 40 years age group showed the highest cybersecurity behaviour level, with the 18 to 20 years and the over 60 years age group showing the lowest. Females showed a lower cybersecurity level in comparison to males with the non-binary participants scoring the lowest. The cybersecurity level increased in general with the educational level of the participants. In a nutshell, the results show that in the context of South African e-commerce users customised interventions based on the educational level, gender, and age need to be considered.

KEYWORDS

Cybersecurity, Cybersecurity Behaviour, E-commerce, E-commerce Users, Demographic Indicators, Age, Gender, Education Level, South Africa

DEDICATION

This research is dedicated to the memory of my beloved late grandfather, Weston Rasikayi Nyamukachi Mberikwazvo, who was always my greatest supporter. His encouragement to pursue my academic dreams has been a constant source of inspiration, and I know he would be proud of this milestone. Cheers to you, Tsoka, wherever you are.

I want to thank my parents for their unwavering support and sacrifices. My father, has always encouraged me to chase my academic aspirations, realising the dreams he once had. My mother, with her guidance, helped me choose this programme, setting me on a path that has been incredibly fulfilling.

To my ever-present support structure, my two boys, your presence has been my driving force. You remind me every day why perseverance is so important, and I hope this journey shows you the value of dedication and hard work.

I am deeply grateful to my family, friends, and colleagues for their support throughout this journey. Special thanks to my brother-in-law for being a sounding board and lifting my spirits when the road was tough. Your help has been invaluable. I also appreciate my employer for contributing to the funding of this program.

A heartfelt thank you to my supervisor, Dr. Kiru Pillay, whose guidance and support have been instrumental in shaping this research. Your dedication, whether through calls, meetings, or even weekend sessions, has helped me produce a report that I am genuinely proud of.

Lastly, I want to recognise the effort I have put into reaching this milestone. It has been a challenging journey filled with unseen battles, juggling a lot of competing interests but I am proud of my resilience and determination.

TABLE OF CONTENTS

LIST OF TABLES ..... **ix**

LIST OF FIGURES ..... **x**

LIST OF ACRONYMS AND ABBREVIATIONS ..... **xi**

CHAPTER 1. INTRODUCTION **12**

1.1 STATEMENT OF PURPOSE 12
1.2 BACKGROUND OF THE STUDY 12
1.3 RESEARCH PROBLEM 14
1.4 RESEARCH OBJECTIVES 16
1.5 RATIONALE 16
1.6 DELIMITATIONS OF THE STUDY 17
1.7 DEFINITION OF TERMS 18
1.8 ASSUMPTIONS 19
1.9 CHAPTER OUTLINE 19

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK 22

2.1 INTRODUCTION 22
2.2 E-COMMERCE IN SOUTH AFRICA 23
2.3 CYBERSECURITY IN RELATION TO E-COMMERCE 25
2.4 CYBERSECURITY BEHAVIOUR ON E-COMMERCE PLATFORMS 27
2.5 IMPACT OF AGE ON CYBERSECURITY BEHAVIOUR 28
2.6 IMPACT OF GENDER ON CYBERSECURITY BEHAVIOUR 30
2.7 IMPACT OF EDUCATIONAL LEVEL ON CYBERSECURITY BEHAVIOUR 31
2.8 FACTORS AFFECTING CYBERSECURITY BEHAVIOUR 32
2.9 COMMON CYBERTHREATS 33
2.9.1 PHISHING 34
2.9.2 MALWARE 34
2.9.3 SOCIAL MEDIA ENGINEERING 35
2.10 GEOGRAPHIC AND CULTURAL FACTORS AFFECTING CYBERSECURITY 35
2.11 GAPS AND LIMITATIONS IN EXISTING RESEARCH 37
2.11.1 HYPOTHESIS 1 38
2.11.1 HYPOTHESIS 2 38
2.11.1 HYPOTHESIS 3 38
2.11.1 HYPOTHESIS 4 38
2.12 ANALYTICAL FRAMEWORK 39
2.12.1 THEORETICAL FRAMEWORK 39

2.12.2 Conceptual Framework 42
2.13 Conclusion of Literature Review 44
2.13.1 Hypothesis 1 45
2.13.2 Hypothesis 2 46
2.13.3 Hypothesis 3 46
2.13.4 Hypothesis 4 46

CHAPTER 3. RESEARCH ETHODOLOGY 47

3.1 Research approach 47
3.2 Research design 48
3.3 Data collection methods 48
3.4 Population and sample 50
3.4.1 Population 50
3.4.2 Sample 51
3.4.3 Sampling method 52
3.5 The research instrument 54
3.6 Procedure for data collection 55
3.7 Data analysis strategies and interpretation 56
3.8 Possible limitations and challenges of the study 57
3.9 Quality Assurance 58
3.9.1 External Validity 58
3.9.2 Reliability 58
3.9.1 Internal Validity 59
3.10 Ethical considerations 59

CHAPTER 4. PRESENTATION OF RESULTS 60

4.1 Introduction 60
4.2 Statistical Analysis and Findings 60
4.2.1 Reliability Statistics 60
4.2.2 Factor Analysis 61
4.2.3 Rotated component matrix 63
4.2.4 Identified themes 65
4.2.5 Correlation analysis 66
4.3 Demographic data 69
4.3.1 Demographic distribution by age and gender 69
4.3.2 Demographic distribution by education level 72
4.4 E-commerce and e-commerce experience 74
4.5 Scoring pattern analysis 78
4.5.1 Personal cybersecurity practices 78
4.5.2 Self-efficacy in cybersecurity 82
4.5.3 Online risk awareness 86
4.5.4 Proactive security measures 89
4.5.5 Adherence to security advice 92
4.5.6 Engagement with cybersecurity information 95
4.5.7 Summarised dimension scores 98
4.6 Testing of hypotheses 101
4.6.1 Hypothesis 1 101
4.6.2 Hypothesis 2 104

4.6.3 Hypothesis 3 105
4.6.4 Hypothesis 4 107
4.6.5 Conclusions 108

CHAPTER 5. DISCUSSION OF RESULTS 109

5.1 Introduction 109
5.2 Inclusion criteria 109
5.3 Overview of key findings 109
5.4 Discussion of hypothesised relationships 110
5.4.1 To investigate how varying age groups impact cybersecurity behaviour amongst South African e-commerce users. 110
5.4.2 To investigate how gender influences the cybersecurity behaviour of South African e-commerce users 111
5.4.3 To investigate how the cybersecurity behaviour of South African e-commerce users varies based on their educational level 113
5.4.4 To investigate how the combined impact of age, gender and educational level serves as a predictor of cybersecurity behaviour among South African e-commerce users 114

CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS 116

6.1 Introduction 116
6.2 Deductions 116
6.3 Conclusions regarding the Hypothesis 117
6.3.1 Conclusions regarding Hypothesis 1 117
6.3.2 Conclusions regarding Hypothesis 2 118
6.3.3 Conclusions regarding Hypothesis 3 119
6.3.4 Conclusions regarding Hypothesis 4 120
6.4 Recommendations 120
6.5 Limitations 122
6.6 Suggestions for further research 122
6.7 Conclusion 124

REFERENCES 126

APPENDIX A – Participant Information Letter 142

APPENDIX B – Survey Instrument 144

APPENDIX C – Ethics Approval 151

LIST OF TABLES

Table 1: Acronyms and abbreviations xi

Table 2: Definition of terms 18

Table 3: Cronbach's Alpha Scores 61

Table 4: KMO and Bartlett's Test 62

Table 5: Rotated Component Matrix 63

Table 6: Correlation analysis 66

Table 7: Gender distribution by age 70

Table 8: Scoring patterns (personal cybersecurity practice) 78

Table 9: Scoring patterns (self-efficacy in cybersecurity) 82

Table 10: Scoring patterns (online risk awareness) 86

Table 11: Scoring patterns (proactive security measures) 89

Table 12: Scoring patterns (adherence to security advice) 92

Table 13: Scoring Patterns (Engagement with Cybersecurity Information) 95

Table 14: Summarised dimension scores 98

Table 15: Overall Score Comparison (gender) 101

Table 16: Mean Scores (age) 102

Table 17: Pairwise comparison (age) 102

Table 18: Overall score comparison (gender) 104

Table 19: Mean scores (gender) 104

Table 20: Pairwise comparison (gender) 105

Table 21: Overall score comparison (educational level).....105

Table 22: Mean scores (educational level).....105

Table 23: Pairwise Comparison (educational level) 106

Table 24: Multifactor analysis: overall score by age, gender, educational level 108

LIST OF FIGURES

Figure 1: Protection Motivation Theory.....40

Figure 2: Health Belief Model 41

Figure 3: Conceptual Framework 43

Figure 5: E-commerce experience 75

Figure 6: E-commerce monthly average use.....76

Figure 7: Number of e-commerce platforms.....77

Figure 8: Mean scores (personal cybersecurity practices).....80

Figure 9: Mean scores (self-efficacy in cybersecurity) 84

LIST OF ACRONYMS AND ABBREVIATIONS

Table 1: Acronyms and abbreviations

Acronym	Description
B	Billion
BRICS	Brazil, Russia, India, China, and South Africa
CAGR	Compound Annual Growth Rate
CNP	Card Not Present
CIA	Confidentiality, Integrity, and Availability
COVID-19	Coronavirus Disease of 2019
df	Degrees of Freedom
E-Commerce	Electronic Commerce
EGA	e-Governance Academy
E-Mail	Electronic Mail
ENISA	European Union Agency for Cybersecurity
Etc	Et cetera
EU	European Union
HBM	Health Belief Model
INTERPOL	International Criminal Police Organisation
iOS	iPhone Operating System
KMO	Kaiser-Meyer-Olkin
M	Million
NCA	National Cybersecurity Alliance
NPA	National Prosecution Authority
MacOS	Macintosh Operating System
PMT	Protection Motivation Theory
POPIA	Protection of Personal Information Act
sig.	Significance Level
SA	South Africa
SAPS	South African Police Service
SME	Small and Medium Enterprises
SMS	Short Message Service
SPSS	Statistical Programme for Social Sciences
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TTAT	Technology Threat Avoidance Theory
UAE	United Arab Emirates
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
WEF	World Economic Forum

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This quantitative study examines the extent to which demographic indicators of age, gender and education levels of South African consumer affects their cybersecurity behaviour in response to risks and threats when transacting on electronic commerce (hereafter referred to as e-commerce) platforms. The study aims to provide helpful insights to understanding the action and attitudes of e-commerce users in relation cybersecurity in the South African context.

1.2 Background of the study

E-commerce allows consumers to make use of various smart devices such as laptops, desktops, smartwatches, smartphones, tablets, and digital voice assistants to electronically buy goods and services online (Yue, 2022). South Africa has seen a boom in e-commerce adoption with low-income earners in South Africa spending 19% of their disposable income on e-commerce platforms. 63% of South African consumers prioritise a secure transaction on e-commerce platforms as a top priority (Stitch, 2024). The e-commerce sector in South Africa is experiencing significant growth with an expected compound annual growth rate (CAGR) of close to 10% expected from 2019 to 2024 (Schaefer & Bulbulia, 2021). The survey further indicates that increased e-commerce adoption has been accelerated by the COVID-19 pandemic with the country expecting over 30 million users to become e-commerce users by 2024. South Africa mirrors the global trends in the most common type of e-commerce sectors with clothing, electronic, footwear, household appliances and health products making up the top five categories (Schaefer & Bulbulia, 2021).

Despite the several benefits brought about by the adoption of e-commerce platforms to consumers across the globe it also presents challenges for consumers such as potential cybersecurity risks as well as the technology challenges when utilising these platforms (Bartczak, 2021). Increased adoption

of e-commerce due to various drivers such as COVID-19 has also seen an increase in fraudulent activities, necessitating the need for role players to put adequate measures in place and protect consumers (Rodrigues et al., 2022). In the next 2 years, cyber insecurity is ranked as the 4th biggest risk facing the globe ranking higher than armed conflict, debt, inflation, and labour shortages whilst 39% of global (government and private sector) respondents based on a survey carried out by the World Economic Forum (WEF) believe that cyberattacks present the 5th biggest risk on a global scale in 2024 (World Economic Forum, 2024). Over the period of July to December 2020, human initiated attacks amounted to US$235M whilst bot attacks contributed a total of US$1.2B on the network during the pandemic period (LexisNexis, 2020). Cyberthreats in Africa include online scams, email compromise, ransomware, botnets with cyberthreats becoming increasingly more sophisticated, organised, and targeted with customised tools intended to trick unsuspecting and often vulnerable consumers who are still getting to grips with online capabilities (INTERPOL, 2021).

Various studies have been done to further understand the relationship between cybersecurity awareness which helps foster safe cybersecurity behaviour and the demographic indicators of age, gender, and education levels as described in a study undertaken by Fatokun et al. (2019). Older students were more likely to fall victim to cybercrime with the younger population showing better levels of cybersecurity behaviour against cyberthreats (Fatokun et al., 2019a). However, these findings were contradicted by Jewel Jean-Pierre et al. (2021) who found that age had no impact in a study conducted in the Commonwealth of Dominica. The study by (Fatokun et al., 2019) also found that educational level did not have impact on the cybersecurity behaviours of organisational employees whilst gender had an impact on some of the constructs.

This study will focus on investigating if there is a significant relationship that may exist between cybersecurity behaviours of consumers making use of the e-commerce platforms in South Africa and their age, gender, and education levels.

1.3 Research problem

More organisations are likely to adopt e-commerce to expand their offerings, minimise cost and improve customer retention (Rahayu & Day, 2015). Since the late 1990's e-commerce platforms have taken off globally, with South Africa experiencing a boom with adoption expected to increase by an average of 13% from 2019 for the next 5 years (Schaefer & Bulbulia, 2021). Just as e-commerce adoption has increased so has the levels of cybercrime with South Africa ranked as being the biggest source of cyberattacks in Africa dominated by online scams with over 700 unique incidents in a 6-month period (INTERPOL, 2021).

The proliferation of cybercrime in the country is a huge concern as it has the potential to negate the benefits realised from the growth of e-commerce causing the country to bleed over R34 billion annually (Mcanyana et al., 2020). The country intends to leverage off e-commerce as one of several vehicles to drive the much-needed growth through inclusivity and employment creation. For these benefits to be realised, all consumers and e-commerce providers need to be aware of safe behaviour and practices that will help them to avoid falling victim to the ever-escalating cybercrime levels in the country and globally. Despite several awareness campaigns, South Africa is still an attractive target for cybercrime according to (Nganga, 2022).

People are more vulnerable to cybercrime when they level of cybersecurity awareness is less (Bahl et al., 2021). The is a relationship between age and the level of vulnerabilities to cyberthreats, with the 18 to 25 years age group most vulnerable to cybercrime. Consumers who are over 75 years age group are a close second to being susceptible to online scams and phishing threats followed by the 65 to 75 years age group (LexisNexis, 2020). This research shows a link between age and cybercrime behaviour even though these studies where not focused on e-commerce platforms. This study seeks to investigate if some of these findings would be similar on e-commerce platforms.

In a study conducted in the United Arab Emirates (UAE) and the United States (US) focused on understanding the impact of gender on security behaviour whilst utilising smartphones. The behaviour of employees varied based on gender when

it came to cybersecurity behaviour on smartphones with very few studies done on understanding the impact of gender in relation to cybersecurity behaviour (Ameen et al., 2020). In a study by conducted amongst tertiary students in Malaysia found that people with a higher education level are more susceptible to cybercrime and the study linked this to how often they accessed the cyberspace (Muniandy et al., 2017). The study also pointed out that there is a general lack of cybersecurity awareness amongst the highly educated.

The South African population offers different dynamics to other countries and this study provides specific insights and findings in a South African geographical context. A wealth of research has been done on this area of study with other countries (Anwar et al., 2017; Bartczak, 2021; Chua et al., 2018; Fatokun et al., 2019), but the aspect of demographic indicators does not appear to have been investigated with a view to how it affects cybersecurity behaviour in South Africa. Several studies tend to agree that age, gender, and education levels influences the cybersecurity behaviour of individuals (Fatokun et al., 2019; Jiang et al., 2016). It is also worth noting that there are other contradicting studies which identify that some demographic indicators have no effect at all on the cybersecurity behaviour (Chua et al., 2018; Kovacevic et al., 2020; Jeske & van Schaik, 2017). Most studies have been mainly done at tertiary institutions which might provide a relative similar profile of respondents in terms of age and education level (Fatokun et al., 2019; Harerimana & Mtshali, 2021; Muniandy et al., 2017). This study also investigates if these outcomes are replicated within the context of South African e-commerce users.

This study therefore seeks to understand the following summarised problem:

This study seeks to examine the influences of demographic indicators, specifically age, gender, and educational level, on the cybersecurity behaviour of individual e-commerce users in South Africa looking to discern trends and patterns.

1.4 Research objectives

Investigating the effects of age, gender, and levels of education on cybersecurity behaviour in the context of e-commerce among South African consumers is the main goal of this study. The research seeks to achieve the following objectives which will ensure that the primary purpose of the study is achieved as well as address the stated research problem:

I. To assess the extent to which varying age groups impact cybersecurity behaviour amongst South African e-commerce users.
II. To assess the extent to which gender influences the cybersecurity behaviour of South African e-commerce users.
III. To assess the extent to which cybersecurity behaviour of South African e-commerce users varies based on their educational level.
IV. To assess the extent to which the combined impact of age, gender and educational level serves as a predictor of cybersecurity behaviour among South African e-commerce users.

In summary, the main goals of this research are to analyse trends based on age, gender disparities and educational levels impact cybersecurity behaviour among South African e-commerce users. These objectives are specifically defined to explore and improve the current understanding of the cybersecurity challenges faced by e-commerce users in South Africa, with a view to improving their security online.

1.5 Rationale

Significant and several studies have been conducted over the years locally and globally around cybersecurity and cyberthreats with a view to enhance and contribute to the field (Anwar et al., 2017; Bartczak, 2021; Chigada & Madzinga, 2021; Chua et al., 2018; Fatokun et al., 2019; Oz et al., 2022; Pieterse, 2021). Researchers have done a lot of work in trying to understand the security issues posed by the emergence of e-commerce platforms as a vital cog in the local and international economies. Some studies have combined the variables related to cybersecurity and e-commerce of lives of people. Other studies have also

specifically looked at the various factors that influence the behaviour of people in relation to their cybersecurity awareness.

Most of these studies have been conducted in countries outside of South Africa and the study aims to understand what the outcome would be locally (Alqahtani, 2022; Anwar et al., 2017; Bartczak, 2021; Chua et al., 2018; Fatokun et al., 2019; Kumbhar & Gavekar, 2017). A specific focus on demographics brings an important dynamic and perspective of which this study will aim to understand how important a factor is if at all.

The study will prove valuable to various stakeholders in this space in different ways. E-commerce providers and law enforcement agencies may better understand the consumers and formulate targeted educational awareness campaigns. The Department of Education may develop a fit-for- purpose curriculum that can assist in equipping students to handle e-commerce platforms better. Legislators may gain more insights into the kind of legislation that could potentially be enacted to regulate the e-commerce and cybersecurity space in the country.

The outcome of this study might end producing interesting findings that could help trigger stimulating debates and conversations amongst critical role players in this domain. The South African perspective that takes into consideration introduces a local dimension that takes into consideration the uniqueness of the local society and would probably contribute to the developing world and the sub-Saharan geographical context. An understanding of consumer limitations and strength can assist in developing targeted interventions to counter cybercrimes.

1.6 Delimitations of the study

The following delimitations apply to this research and should be considered when analysing the findings:

I. Consumers who have accessed e-commerce platforms at least once before will be allowed to take part.

II. Study is focused within the South African geographical space. This means users or individuals who have utilised e-commerce platforms in the country.
III. No respondents under the age of 18 will be considered as respondents for this study.
IV. Study is focused only on e-commerce platforms, and this excludes the use of social media or just general utilisation of other online platforms.
V. Whilst other demographic indicators such as income level, ethnicity, language proficiency, occupation etc could have been used, this research is only limited to the three aspects of age, gender, and education level.

1.7 Definition of terms

The following keywords and key concepts are used in this document:

Table 2: Definition of terms

Term / Concept	Description
Botnet	A set of computers that are remotely controlled by cybercriminal whilst running harmful programmes and can be directed to execute criminal tasks on command (Ahmad et al., 2022).
Cybercrime	Refers to any illegal and criminal actions performed on internet enabled devices or the network itself (Hong & Furnell, 2021).
Cybersecurity	A capability designed and managed to ensure that there is no unauthorised access of resources connected to the internet (Hong & Furnell, 2021).
Cybersecurity Behaviour	Refers to the actions that are taken by an individual to avoid being a victim various cyberthreats and this includes awareness and safe online behaviour (Hong & Furnell, 2021).
E-commerce	A platform that allows customers to buy products and services whilst utilising the computer networks like the internet (Rodrigues et al., 2022).
Malware	A generic term used to define different types of software that have a harmful intent to the computer (Ahmad et al., 2022).
Phishing	A technique utilised by cybercriminals to obtain sensitive and private information such as passwords, banking card

	details, account numbers etc usually through deception like fake emails, user interfaces etc. (Ahmad et al., 2022).
Ransomware	A kind of malware that gets hold of your files or the computer and/or data preventing access with the aim of soliciting ransom (Oz et al., 2022).

1.8 Assumptions

The following assumptions have been identified for this research:

I. The Age, gender, and education levels provided by the survey participants will be considered as honest and accurate.
II. Survey responses on behaviour of the respondents on e-commerce platforms will be assumed to be honest and true feedback.
III. The respondents will provide feedback having fully understood the questions asked, every effort will be made to ensure that the questions are as simple as possible.
IV. The characteristics that are important for this study remained the same for the entire duration of the study period.

1.9 Chapter outline

The following section provides an indication of how the research report will be structured and the order in which they will appear:

Chapter 1: Introduction

This chapter introduces the study with a view to articulate the intention as well as the justification of the study. The purpose will be stated and the research problem that the study seeks to address will be detailed. The objectives as well as the rationale behind study including any underlying assumptions as well as any delimitations of the study will also be included in this chapter.

Chapter 2: Literature Review

This chapter will seek to review the existing literature related to cybersecurity awareness, behaviour, e-commerce platforms and common cyberthreats. The

study will be located within the existing literature proving the importance of the study. The theoretical frameworks on which the study was based will be identified and explored leading to an adapted conceptual framework that will provide a plan for the research.

Chapter 3: Research Methodology

The map that will detail how the study will finally come to its findings and conclusion will be articulated in this chapter. Research approach, design, and the process to be followed in collecting the research data will be detailed. The chapter will also include the research instrument that will be used, together with the sample taking into consideration the ethical issues as well as any study limitations that apply to the study.

Chapter 4: Presentation of Findings

This chapter will seek to present the findings of the conducted quantitative survey. Information pertaining to the respondents including the number of responses and their demographic profile will also be presented in this chapter.

Chapter 5: Discussion of the Findings

This chapter will include discussion of the findings with a view to ascertain if the research objectives have been met and provide a conclusion in relation to the stated hypothesis statements.

Chapter 5: Conclusions and Recommendations

This is the final chapter which seeks to conclude and summarise the findings, contributions, and any suggestions for future research.

In conclusion, this chapter has established the study framework by outlining its purpose, research problem, research objectives, and the rationale. This chapter has further defined the parameters by highlighting the importance of understanding cybersecurity behaviour of e-commerce users in the context of South Africa, the chapter further outlined the scope and limitations of the research. Now that these essential elements have been established, the following

chapter will undertake a thorough analysis of the literature, looking at previous studies and theoretical frameworks that serve as the basis for this research.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

In the digital age, accelerated by the restrictions brought about by the coronavirus disease 2019 (COVID-19), convenience (Evanschitzky et al., 2020; Musakwa & Petersen, 2023) e-commerce has become an integral part of everyday life for most South Africans allowing for more economic inclusion and participation in a highly unequal country like South Africa (Shenjere & Middelberg, 2023). However, with increased adoption of e-commerce platforms, there is also a growing risk of cyber threats and attacks.

South Africa as a developing country still lags the developed countries in internet penetration (Musakwa & Petersen, 2023). However, the country is ranked first on the African continent as having the highest proportion of users with access to the internet on the continent (Roos & Jordaan, 2006). Smart mobile devices such as laptops, smartphones and tablets have become an integral part of South Africans with users utilising them to access various internet-based services and platforms (Harerimana & Mtshali, 2021). The bigger the number of middle-class consumers grow in country the higher the e-commerce adoption in the country (Balasudarsun et al., 2022).

However, whilst the increased adoption of e-commerce has brought about more opportunities for the service providers and the users, a report by Lexis Nexis Risk Solutions points out that this has created an unprecedented opportunity for cybercriminals. E-commerce has surpassed all other industries like the media, financial services, gaming as being the most targeted by cybercriminals globally with the number of identity theft by use of automated bots rising to over 2 billion (LexisNexis, 2020). In a detailed analysis of the specific cyberthreats that are most common in Africa INTERPOL (2021) highlights online scams (phishing, payment scams, cryptocurrency fraud etc), email spoofing and botnets as some of the biggest challenges.

The link that exists between the rise in e-commerce adoption and the increase in cybercriminal activity is a key aspect to understand. By shedding more light into the various factors that influence the safety or vulnerability of users in the e-commerce context of South Africa can help to formulate targeted measures that may help to alleviate this threat.

Many factors affect cybersecurity behaviour, but this research is limited to only demographic factors of age, gender, and educational level. The section will locate this research and review literature related to the various factors that affect cybersecurity behaviour whilst establishing the link between demographic indicators and e-commerce in South Africa. Existing literature related to the focus areas will be evaluated and critiqued with a view to emphasise the significance of the study. As we go through the section, extensive literature of the current understanding and any identified gaps will be highlighted which will provide a basis for the objectives and investigation of this study.

2.2 E-commerce in South Africa

E-commerce is a platform that allows customers to buy products and services whilst utilising the computer networks like the internet (Rodrigues et al., 2022). Over 30 million South Africans representing a staggering increase of 44% from 2021 are expected to utilise e-commerce platforms by 2024 (Schaefer & Bulbulia, 2021). These numbers are encouraging providing a basis for inclusion for the wider population of the country as internet services become more accessible.

Increased availability and affordability of smart devices provides an important platform for users to adopt internet-based services such as e-commerce platforms (De Wet et al., 2016). For South African organisations seeking to increase their market share locally and beyond the country's borders, leveraging off e-commerce platforms is a no brainer. Growth of the e-commerce adoption for South African consumers has accelerated because of the COVID-19 pandemic, increased convenience, more variety, and competitive pricing (Schaefer & Bulbulia, 2021).

Providing e-commerce platforms to consumers has become an integral part of the business strategy for South African service providers including Small and Medium-Sized Enterprises (SME) and large corporates as well (Mbatha & Ngwenya, 2018). A study by Elrhim and Elsayed (2020) found that there is a strong positive correlation between the prevalence of the COVID-19 pandemic and the use and adoption of e-commerce platforms. The investigation was centred on the biggest international e-commerce platforms based on their market size as well as income levels. The e-commerce providers included in the scope of the investigation were Alibaba, Amazon, Rakuten, Zalando and ASOS.

Increased proliferation of e-commerce platforms has led to healthier businesses characterised by reduction in cost, increased reach, and availability (Kartiwi et al., 2018). Johnson and Iyamu (2019) highlight that for South African consumers, access to e-commerce helps in minimising traveling cost to physical location to access much needed products and services. E-commerce platforms provide a platform that helps to foster long term relationships between customers and service providers (Safa & Von Solms, 2016) which in turn helps improve inclusivity for the marginalised population. Better customer experience, improved accessibility to relevant information and boosting economies on the developing African continent (Makame et al., 2014) are some of the key reasons why adoption of e-commerce provides should be a strategic imperative for African governments.

Studies have been carried out to explore the various factors influencing users to adopt e-commerce platforms. Rosário and Raimundo (2021) in their study of e-commerce users over the last decade identified demographic factors as key to understanding the segments utilising e-commerce. Age, gender, income where some of the factors identified. In a study of over 400 Generation Y respondents who were below 29 years shopped at least twice on e-commerce platforms (Zhu et al., 2020). The study points out that trust is an important ingredient in ensuring that the users in this age group feel comfortable in utilising these e-commerce platforms. This study provides useful insights about the link to age with e-commerce adoption. However, there was no focus on also understanding if this phenomenon also existed amongst the older people. Mbatha and Ngwenya

(2018) point out that in South Africa factors linked to illiteracy, lack of knowhow in using e-commerce platforms and general lack of confidence are some of the critical factors that inhibit greater adoption of e-commerce.

The growth of e-commerce adoption going forward is mainly going to be based on how much trust the users place on the e-commerce platforms (Yoon & Occeña, 2015).The study noted that because of the increasing penetration and importance of understanding the customer, age as a factor in understanding customer behaviour needs to be researched more and understood. The outcome of the study by Yoon and Occeña (2015) was that age had a significant impact on how people are likely to trust and adopt e-commerce platforms. The sample had wide range of respondents from 20 years to over 40 years old. One of the common characteristics that has a significant influence on the behaviour of users when shopping online is age (Molinillo et al., 2021). A study was done with a sample of 272 people, and they were classified in two age groups of less than 24 years and greater than 23 years. According to the findings of the study age was found to not have a significant difference in terms of how consumers would utilise online platforms and including their loyalty, engagement on the platform. These studies show the contradictory findings of different research. Of note is the fact that the research by Yoon and Occeña (2015) was done about nine years ago, and dynamics might have changed with the research by Molinillo et al. (2021) being more current.

2.3 Cybersecurity in relation to e-commerce

A very high proportion of users (86%) are worried about the level of security on e-commerce platforms whilst 81% are worried about the inadequate security of their personal data (Schaefer & Bulbulia, 2021). Whilst the emergence of e-commerce technologies has seen increased adoption, it has also exposed a challenge related to security when transacting on the platform (Badotra & Sundas, 2021). Cybersecurity related challenges present the single biggest threat to the wider adoption and use of e-commerce platforms (Bartczak, 2021). Silaule et al. (2022) highlights that cybersecurity concerns are increasingly becoming a significant impediment to the growth of the digital economy.

Due to vital role that digital platforms play in the economies of most countries, cyber-attacks have the potential to be considered modern warfare (Peng, 2023). Distributed technologies like blockchain are now being widely utilised globally to facilitate relatively secure payments on e-commerce platforms but because of the accelerated pace at which the technology has been developed some cyberthreat vulnerabilities have come to the foe (Rathore et al., 2020). According to Peng (2023) major global economies (US, China) and blocs like the EU have made protecting the digital economies at the forefront of their government's strategies pouring enormous resources as well as enacting applicable legislation to protect their supply chain processes.

Badotra and Sundas (2021) analysed different e-commerce platforms for cybercrime vulnerabilities and the findings were concerning. The results indicated that different facets of security concerns like credit card information and sensitive information was sometimes not properly secured making it easily available to cybercriminals. The study was limited to Ghana a developing country and could present useful insights into South Africa as well. A similar study was also done by Bartczak (2021) and identified the cybersecurity shortcomings of the e-commerce businesses. The study pointed out that different platform vulnerabilities contributed to the scepticism to adopt e-commerce for some users. As much as the studies exposed the security challenges that some of the e-commerce platforms face, the study focused more on understanding the cybersecurity weaknesses of the platforms themselves and not from a user perspective.

In the absence of trust, users are unlikely to adopt e-commerce platforms at the expected rate and this could potentially hamper much needed business growth especially in the developing world. A study by Apau and Koranteng (2019) based on a survey of about 476 participants found that cybercrime perceptions had a significant impact on the decision by users to transact on e-commerce platform or not. This study conducted in Ghana emphasises the fact that perceptions of security on e-commerce platforms play a significant role in increased adoption. This study did not explore the different behaviours and common cyberthreats that are likely to result in people falling victim to cybercrimes.

2.4 Cybersecurity behaviour on e-commerce platforms

Cybersecurity is the utilisation of tools, legislation, and various other techniques to assist in ensuring that the integrity, availability, and confidentiality of information is maintained in the cyber domain (ENISA & EGA, 2021). To get a good understanding of what is cybersecurity behaviour, defining human behaviour first will be beneficial. Mashiane and Kritzinger (2019) describe human behaviour as the different ways in which people act or respond due to some form of trigger which can either be within or external to their environment. Linking the definition of cybersecurity and human behaviour, this research defines cybersecurity behaviour as the steps undertaken by individual i.e. to act or respond as result of trying to protect assets in the cyber space.

Cybersecurity has increasingly become an issue of concern as more people utilise internet based digital platforms. Cybercriminals are busy devising new ways of scamming unsuspecting consumers through the new digital technologies (Chigada & Madzinga, 2021). INTERPOL (2021) suggest that it is critically important that countries in Africa considerably aim to improve the level of cybersecurity awareness among its populace. Research conducted by Kumbhar and Gavekar (2017) evaluated the level of awareness using the types of attack which are hacking (93%), trojan attacks (43%), virus and worm attack (11.5%) and email spamming (8%). This finding raises significant concerns considering the high adoption of emails and the fact that at least one in every ten people are unaware of the dangers posed by email spamming (Kumbhar & Gavekar, 2017). This research has its shortcomings especially because it does not include other common and critical sources of cyberthreats faced by consumers over the last few years.

However, the study by Alqahtani (2022) addressed some of the shortcomings from the study by Kumbhar and Gavekar (2017). The study investigates how users manage password security, browser security and social media as a way of understanding safe cybersecurity behaviour online. Alqahtani (2022) conducted research on about 450 students at a university using varied demographic profiles of the respondents of gender, age, education, computer skill and frequency of purchasing online. The outcome of the study found that there is a strong

correlation in the respondents who practiced safe cybersecurity behaviour like password security, browser security and social media activities with a higher level of cybersecurity awareness. This study touches on critical factors that influence cybersecurity awareness though its limitations are that it was limited to students at a university in Saudi Arabia with only 1% of the responding students being over 50 years.

Senthilkumar and Easwaramoorthy (2017) concurred with some aspects of the study by Alqahtani (2022) and Kumbhar and Gavekar (2017) by identifying virus attacks, password strength, social media behaviour as key attributes to measure cybersecurity behaviour and then taking it further by including phishing. The survey conducted with 500 respondents over the city of Tamil Nadu in India was that the overall cybersecurity awareness was relatively high at just under 70% (Kumbhar & Gavekar, 2017). This study again poses questions about the differences that might potentially exist between the e-commerce users in South Africa and those in other geographical areas like India, Malaysia, Ghana, Saudi Arabia, Latin America, Europe, US etc.

2.5 Impact of age on cybersecurity behaviour

Understanding various factors that affect the cybersecurity behaviour of individuals is a difficult concept to understand and not a lot of research has been done in that regard (Gillam & Foster, 2020). This section identifies and discusses the literature that exists in the field to gain an understanding of how age plays a role in the cybersecurity behaviour of individuals and in some cases with a specific context of e-commerce platforms. Reviewing of this literature will assist in the formulation of age group targeted interventions in raising cybersecurity awareness.

A study conducted by Gillam and Foster (2020) concluded that age played a significant role in cybersecurity behaviour that could potentially lead to one being a victim of cybercrime. Most users are not aware of the security features that they can employ when engaging with e-commerce platforms based on the findings of Shah and Agarwal (2020) in a study conducted in India. They also found that the

behaviour of e-commerce users varied significantly with age. Younger users aged between 18 to 24 years are technologically astute and hence likely to exhibit more responsible cybersecurity behaviour unlike the older users who are older than 24 years (Shah & Agarwal, 2020).

An extensive study conducted in Turkey of over 12 000 participants of teachers, students, and parents found that students were more aware of cyberthreats and exhibited more cybersecurity awareness than their generally older parents and teachers (Mıhcı Türker & Kılıç Çakmak, 2019). A study conducted in the United Kingdom (UK) pointed out that people around the retirement age become more vulnerable to cybercrime (Morrison et al., 2020). To further emphasise the vulnerability of the older generation to technology related platforms Vaportzis et al. (2017) indicated they were generally apprehensive and generally found using technology confusing without support. Von Solms and Van Niekerk (2013) place responsibility on the South African society by stating that it the responsibility of the broader society to protect the more vulnerable age groups.

On the other hand, Das and Khan (2016) pointed out that it is difficult to conclude whether age influences the cybersecurity behaviour of users in a certain direction. The study finds that while older people would generally be more cautious when engaging on the internet on the flipside, they are not well versed with internet-based technologies which makes them more vulnerable to cybercrime. All age groups have a certain level of vulnerabilities when transacting online but the older age groups of 70 years and above are particularly more vulnerable to cyberattacks (Jiang et al., 2016). The study also found some interesting perspectives from those aged between 24 and 39 years indicated that they were not worried about security when conducting financial online transactions as they did not have as much money as their parents. Younger people of ages between 18 and 24 years show a greater sense of awareness, self-belief, and self-efficacy when it comes to protecting sensitive data that might make them susceptible to cybercrimes (Miltgen & Peyrat-Guillard, 2014).

2.6 Impact of gender on cybersecurity behaviour

This section seeks to explore the existing literature on how the demographic indicator of individuals influences the various aspects of cybersecurity behaviour of individuals. There has been minimal research to fully understand how gender differences influence the behaviour of individuals when it comes to securing their information online (McGill & Thompson, 2021). The intention, attitude, and approach to secure private information on social media shows that it varies significantly with the gender of the individual (Chen & Sharma, 2015). Most users are not aware of the security features that they can employ when engaging with e-commerce platforms based on the findings of Shah and Agarwal (2020) in a study conducted in India found that the behaviour of e-commerce users varied significantly with gender.

Females in general tend to be more worried and are likely to engage in more cautious behaviour that protects their privacy when utilising online platforms than their male counterparts (Rowan & Dehlinger, 2014). In a study conducted in Malaysia, female learners showed more cybersecurity awareness than male learners when utilising online digital technologies (Maon et al., 2021). The study further points out that more training is required for both males and females to practice more responsible cybersecurity behaviour. A big study of about 20 000 employees of a financial institution in Thailand found that gender was a significant factor in the cybersecurity practices of users and hence their susceptibility to cyber-attacks like phishing. The finding was that females were generally more aware and cybersecurity conscious than males specifically when confronted with a potential phishing attack (Daengsi et al., 2022).

Offering a different perspective, McGill and Thompson (2021) found that men tend to be more substantially aware of recommended cybersecurity behaviour that helps to keep them safer online than women. Concurring with this finding, Thompson and Brindley (2020) stated that females are more likely to disclose private information on social media that can make them more vulnerable to cyber-attacks than males. Colley and Maltby (2008) attributes this behaviour to the propensity of females who are more likely to gain more gratification by sharing information on social media than males would. Women tend to be excluded in the

cybersecurity discussions deliberately even though they are more likely to be a victim of financial fraud online than men. Females of an organisation in the US were more likely to fall victim to phishing attacks than males even though no significant difference was found between the genders in terms of adhering to safe cybersecurity practices (Chua et al., 2018).

In conclusion, understanding how gender affects the cybersecurity behaviours of individuals is fluid and requires consistent research to stay abreast of the changing dynamics in the field. Based on the reviewed literature there seems to be a divergent of views with some research showing significant variations on how gender impacts cybersecurity behaviour whilst other studies have found no significant differences.

2.7 Impact of educational level on cybersecurity behaviour

In an endeavour to further grasp the factors influencing the cybersecurity behaviour and awareness of individuals, educational level should be considered and explored as a factor (An et al., 2023). This section of the literature seeks understand the thread that links cybersecurity behaviour and educational level. The relevant existing literature that exists will be explored to form a picture of the current understanding of this important relationship.

Cybersecurity behaviour of individuals showed no difference between those individuals with an undergraduate degree and those with a postgraduate degree (An et al., 2023). However, interestingly the level of cybersecurity knowledge was significantly less for those with a postgraduate degree. Among the various demographic factors investigated, educational level showed the least to no impact in impacting cybersecurity behaviour and this according to a study conducted in Malaysia amongst university students (Fatokun et al., 2019). Consistent with these findings, Jeske and van Schaik (2017) contributed by indicating that educational level did not seem to have an impact in terms of cybersecurity familiarity and consequentially the cybersecurity behaviour. University students who are the more active digital users of the society, irrespective of their educational level did not feel confident of their security when

transacting online and did not practice safe cybersecurity behaviour or have enough cybersecurity knowledge to protect themselves from cyberthreats (Kovacevic et al., 2020).

Factors that impact cybersecurity behaviour have not been fully explored according to Gillam and Foster (2020), and to address this apparent gap a study was carried out in the US and education level among other demographic factors was found to be a significant factor.

2.8 Factors affecting cybersecurity behaviour

Significant research has been done over the years to try and understand the various factors that influence how different people conduct themselves in respect to cybersecurity behaviour. Most people fall victim to cybercrime because of human factors (Anwar et al., 2017). The study survey focused on employees of different companies with a view to understanding if gender played a role in how people's cybersecurity behaviour varied based on identified psychological variables like previous experience and self-efficacy. The outcome indicated that the gender of a user could be used as a determinant of cybersecurity behaviour (Anwar et al., 2017). A different study with similar significance in this same domain carried out by Fatokun et al. (2019) with the sample of 340 students derived from Malaysian universities. This study added more depth to the one by (Anwar et al., 2017) by including demographic factors such as age, gender, and educational level. Age and gender also played a significant role in determining cybersecurity behaviours amongst university students (Fatokun et al., 2019). Whilst these studies provide useful insights into the different factors that contribute to people's cybersecurity behaviour, it would be interesting to note if these findings would be similar if the focus was based on the behaviour on e-commerce platforms and if the sample was not restricted to a university which could present similar demographics in certain aspects.

A study by Gillam and Foster (2020) was conducted to understand a different dimension to cybersecurity behaviour with a focus on avoidance behaviour leveraging off the Technology Threat Avoidance Theory (TTAT). Factors

considered were perceived susceptibility, perceived costs, perceived severity, and self-efficacy. Gillam and Foster (2020) identified educational levels, age, and gender as the confounding variates. The study concluded that age did not significantly influence the TTAT constructs. The study was conducted with a sample of more than 1000 employees who were generally more educated and on average older than the average US population. This sample might have skewed the results and would be keen to exploit a similar study with a more varied sample of respondents.

All the previous studies have contributed to the knowledge and the different factors influencing cybersecurity behaviour. Whilst the studies have answered some important questions, they have however left more questions like would these findings hold in a different geographical area like South Africa.

2.9 Common cyberthreats

An important consideration in trying to understand the cybersecurity behaviour on e-commerce platforms is to ensure that the most common cyberthreats are identified. Having a good understanding of these common cyberthreats and their characteristics assist in ensuring that fit for purpose counter measures can be put in place and the right education and awareness is conducted. In the digital age various attacks are specific at various layers of the technology architectures. The survey used the CIA (Confidentiality, Integrity, Availability) triad as the basis to identify the more common threats to cybersecurity (Alharbi & Tassaddiq, 2021). The investigation was conducted based on how the respondents updated their devices, password management and understanding of social network sites. This research brought about an important dimension which relates to the behaviour of consumers when updating software on their smart devices.

No system is immune to being hacked stating that vulnerabilities will always be there and cyberattacks can only be minimised but not eradicated. The study identifies potentially useful advice to users by stating that consumers should never open any attachments from unknown sources, avoid utilising internet cafes and deleting important personal data (Minnaar, 2014).

With increased internet accessibility and e-commerce increased usage Lim Ka Yong et al. (2020) reckons that cybercriminals are coming up with new ways to exploit vulnerable consumers and this has led to more cybercrime victims. The study agrees with most other studies and points out that identity theft, social engineering, malware, and phishing as common attacks that most users are vulnerable to. The study adds an important dimension to other research even though it dedicates a lot of focus on the whole solution domain whilst not giving particular attention of the cyberattacks from a user or consumer perspective.

2.9.1 *Phishing*

Described as a common type of cyberthreat whereby the attacker seeks to trick users through presenting oneself, an e-mail, URL, SMS, website, or domain as being trusted with a view to obtain private and sensitive information (El Aassal et al., 2020). End users provide as the biggest source of vulnerability and weakness for cybercriminals when trying to obtain private information like passwords Phishing attempts have evolved over time with the cybercriminals resorting to targeting a relationship with individuals so that they can build trust making it easier to obtain private and sensitive information (Bhardwaj et al., 2021). End users need to be continually aware of the evolving phishing attempts to avoid being victims of cybercrime (El Aassal et al., 2020). Since the COVID-19 pandemic, malicious websites numbers have also increased. More and more fake websites that look like the real website are being used to dupe users into providing confidential information such as credit card details, passwords, and personal information (Alhashem et al., 2023).

2.9.2 *Malware*

Malware refers to a general term that is used to identify harmful software that is created to exploit computers and their systems (Branch et al., 2016). The threat of different malware types which includes viruses, ransomware, worms, trojans, spyware pose a huge challenge for users who intend on adopting e-commerce. A significant number of customers are discouraged from fully utilising and

adopting e-commerce because of the danger posed by malware (Keshri et al., 2020).

There has been a proliferation of vendors that specialise in selling specialised malware tools to cybercriminals enabling an increase in their popularity growth trend (Leukfeldt & Holt, 2022). It is vitally important that end users of online platforms need to continually check their devices for unauthorised access, be vigilant with software purchases, updates, secure devices whilst being careful with any unknown links (Gopinath & Sethuraman, 2023).

2.9.3 *Social media engineering*

Cybercriminals are increasingly exploiting the lack of awareness and knowhow of threats to obtain information that they might not have obtained independently (Alharbi & Tassaddiq, 2021). This type of cyberthreat is mainly prevalent on social media in the cyberspace and is sometimes called human hacking. The increased popularity and accessibility of social media platforms presents information that the cybercriminals that are keen to exploit (Wilcox & Bhattacharya, 2020). Social media engineering phenomena has been exacerbated because users tend to share information that they are not supposed to share on public social media platforms. Information like location, job role, work email address, credentials, phone numbers, addresses and financial status are some of the information that should not be shared on social media (Tayouri, 2015).

2.10 Geographic and cultural factors affecting cybersecurity

The International Criminal Police Organisation (INTERPOL) conducted a comprehensive analysis of countries in Africa to understand their vulnerability to various common cybercrimes. A cause for concern, INTERPOL (2021) found that more than 90% of African countries did not have the requisite tools (skills, technology, legislation) in place to help prevent cybercrime. Unlike other African countries, South Africa has been the most exposed to cybercrime than any other country on the continent accounting for more than 200 million threats in total, three times more than the next country which is Kenya with about 70 million

threats. Adding to the grim picture, the report goes further and states that South Africa ranks as the third country with the most victims of cybercrime globally which is truly concerning and requiring some impactful intervention (INTERPOL, 2021).

In an endeavour to answer why South Africa is such a magnet for cybercriminals, Kortjan and Von Solms (2014) indicate that there is low level of cybersecurity knowhow and familiarity amongst the internet users in the country. The slow nature of implementing relevant legislation, socioeconomic factors are some of the main reasons why South Africa struggles with cybercrime. Du Toit et al. (2018) conducted a study in South Africa and found that almost 50% of the respondents had been a target of cybercrime recently with more than 65% of those not reporting the incidents to the relevant authorities with about 40% of those expressing a worrying sentiment of not having confidence in the current legislation to combat cybercrime. South Africa has experienced a boom in the adoption of internet-based technologies and in the same vein has seen an increased exposure to cyber-attacks (Pieterse, 2021). The scale of the challenge is further exacerbated by the fact that the South African Police Service (SAPS) and the National Prosecuting Authority (NPA) do not release any official figures to help shed light on the extent of the problem.

The South African government has successfully spearheaded efforts to improve internet access to most parts of the country but unfortunately the country lacks a cybersecurity culture to repel off the increasing cybercrime threat (Gcaza & von Solms, 2017). In response to this lack of culture and guidelines that promote responsible cybersecurity behaviour the South African government has responded by drafting and adopting the National Cybersecurity Policy Framework (NCPF) (Government Gazette, 2015). In an assessment of the South African environment to understand why it's characterised by poor cybersecurity culture, Gcaza & von Solms (2017) identified some of the following main issues in South Africa as limited resources, limited skills, lack of government leadership, limited stakeholder engagement and monitoring structures (Gcaza & von Solms, 2017).

The global community has embraced the use of online platforms to further develop their communities and improve accessibility to essential services, most

countries have also embraced measures that help protect their citizens from the ever-growing threat of cybercriminals (Kortjan & Von Solms, 2014). The study goes further by pointing out that South Africa has lagged other countries in developing a structured state-led approach to improving the cyber-secure behaviour of its populace.

South Africa is a member of Brazil, Russia, India, China, and South Africa (BRICS) which has developed and adopted measures and frameworks to create a coordinated effort to help repel the increasing threat of cybersecurity issues within member countries (Belli, 2021). Despite this cybersecurity approach as a bloc of countries within BRICS it is noted that each country has different approaches and levels of maturity. Whilst South Africa has signed significant pieces of legislation such as the Protection of Personal Information Act (POPIA) and the Cybercrimes Act over the last few years, practical implementation has lagged. Belli (2021) notes that amongst the BRICS countries China and Russia have relatively mature cybersecurity related legislation which keeps pace with the rate of technological advancement. Low levels of cybersecurity awareness and increasing cyberthreats remain a big challenge for countries like Brazil and the Latin American geographical area beyond the legislation (Carapeto & Calil, 2022). Countries like Brazil and Chile have shown a more developed regulatory driven approach framework with a country like Mexico still with a long way to go to catch up.

2.11 Gaps and limitations in existing research

The current literature has explored the study of cybersecurity behaviour from different from other geographical countries such as India, Kenya Malaysia, US, UK, Brazil and regions of Latin America, North Africa, Europe, and Asia mainly. Limited research exists to fully understand the uniqueness of South Africa as a country and even from the Southern African region where South Africa is. This is a significant gap as highlighted in some sections of this literature review section which shows the cybersecurity behaviour of individuals seem to vary between different countries and regions.

Whilst there has been significant research done to explore how the individual demographic indicators of age, gender, and educational level impact the cybersecurity behaviour of individuals, there is a noticeable gap exists to understand how a combination of these indicators would impact cybersecurity behaviour from a South African context. Exploring and understanding the combined effect of these demographic indicators would greatly assist in adding more perspective and understanding in the field to come up with more impactful interventions to assist South African e-commerce users.

2.11.1 *Hypothesis 1*

There is a significant relationship between cybersecurity behaviour and age in South African e-commerce users.

2.11.1 *Hypothesis 2*

There is no significant difference in cybersecurity behaviour across gender disparities of e-commerce users in South Africa.

2.11.1 *Hypothesis 3*

There is a significant relationship between cybersecurity behaviour and educational level in South African e-commerce users.

2.11.1 *Hypothesis 4*

The combined impact of age, gender, and educational level can significantly predict cybersecurity behaviour in South African users.

2.12 ANALYTICAL FRAMEWORK

2.12.1 *Theoretical Framework*

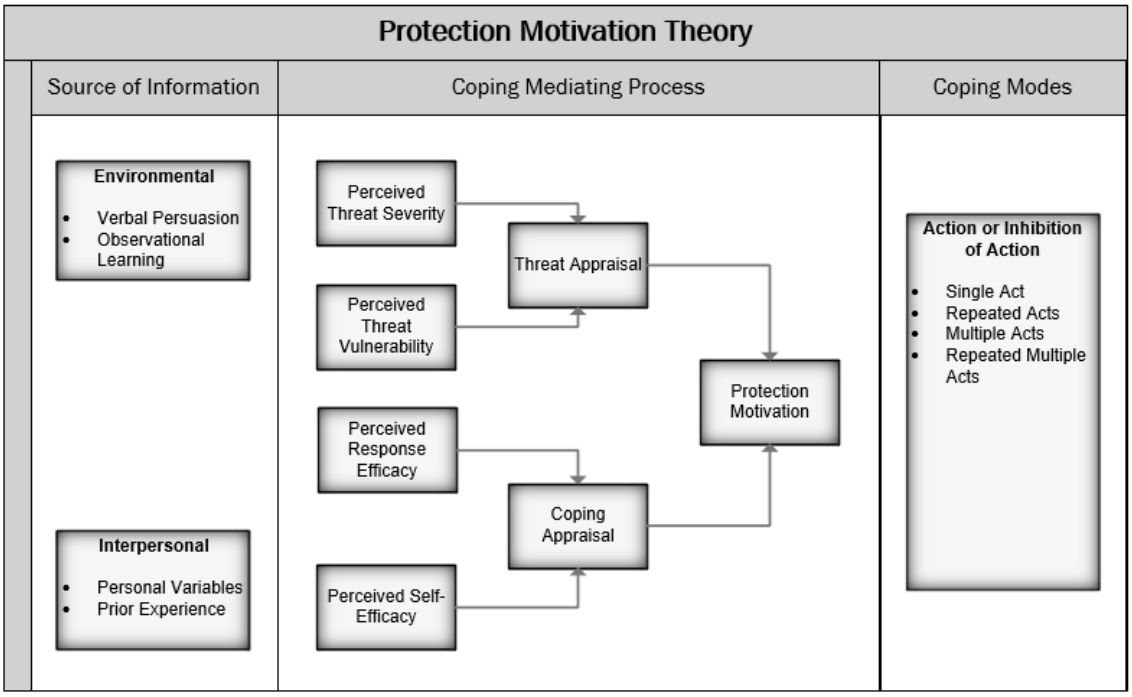
Understanding the users' cybersecurity behaviour is generally complex and when confined to a dynamic context of e-commerce platforms makes understanding the various factors at play even more difficult. This section is focused on further exploring the theoretical frameworks that can assist in interpreting the research findings as well as provide the much-needed direction to fully understand the variables of this research.

The combination of concepts relevant to this study from the Protection Motivation Theory (PMT) and the Health Belief Model (HBM) will result in a custom conceptual framework providing more insights on the behavioural phenomena of how users react to various forms of cybersecurity in relation to e-commerce. (Anwar et al., 2017) points out that combining the strengths of both PMT and HBM has been widely used in exploring the user's behaviour when responding to security related threats.

Protection Motivation Theory

Protection Motivation Theory (PMT) was initially developed in the 1970's with the objective to understand how people's behaviour changes based on health and safety concerns (Conner & Sparks, 2015) . However, over the last decades PMT has been adapted and is widely used in various industry domains including cybersecurity for research purposes (Anderson & Agarwal, 2010). The crux of the theory is based on understanding and predicting motivations which help to drive behavioural change in people. The theory is primarily rooted in the primary premise of understanding the human behaviour from a perceived vulnerability and severity perspective (Menard et al., 2017). PMT helps to explain how certain cybersecurity behaviour on e-commerce platforms is influenced by the perceived threat of cybercrime.

Figure 1: Protection Motivation Theory



Note. Adapted from (Bamberg et al., 2017).

The PMT is underpinned by the premise that an individual's motivation to engage in a behaviour to fend off the perceived security threat is driven by the user's perceived appraisal of the threat (Vance et al., 2012). Further clarity to understanding threat appraisal is provided by Kim et al. (2022) who explains that threat appraisal is made up of perceived threat vulnerability and perceived threat severity.

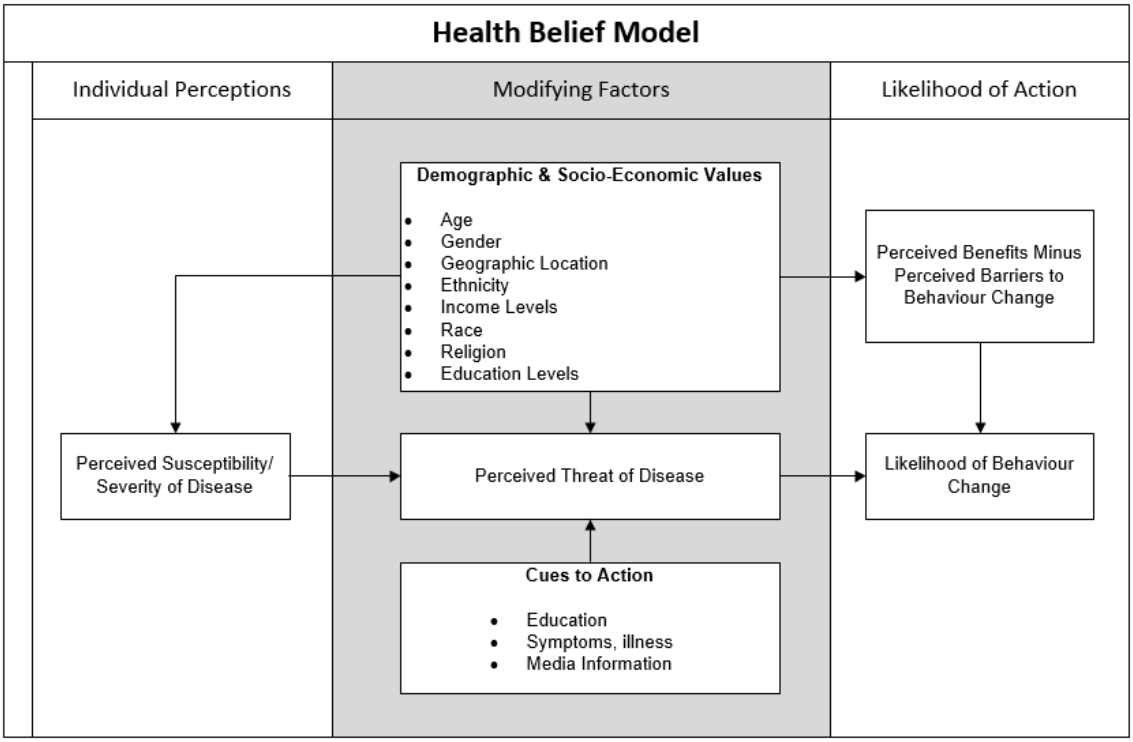
High levels of perceived threat vulnerability and perceived severity are associated with an increased adoption of preventative measures to avoid the being a victim of the perceived security threat. Threat vulnerability is defined as how an individual analysis the treat and determines how they are likely to be personally affected by the perceived threat. Whilst perceived severity refers to the how the individual evaluates the potential negative impact to them personally because of being a victim of the potential threat (Kim et al., 2022; Menard et al., 2017; Vance et al., 2012).

Health Belief Model

The Health Belief Model (HBM) is one of most used psychological based models that was initially developed to explain and understand the reasons why people failed to actively participate in initiatives to help prevent and identify diseases in the 1950's by social psychologists from the US. Over the years the model has been adapted by researchers to help in understanding hie phenomenon in other industries as well (Dodel & Mesch, 2019).

The HBM illustrates that for people to achieve the desired behavioural change they must place targeted focus on the perceived severity, perceived benefits, perceived susceptibility, perceived barriers, cue to action, self-efficacy and some modifying variables which can include demographic and socio-economic values such as age, gender, and education level (Paganin et al., 2023; Tsai et al., 2021).

Figure 2: Health Belief Model



Note. Adapted from (Carico et al., 2021).

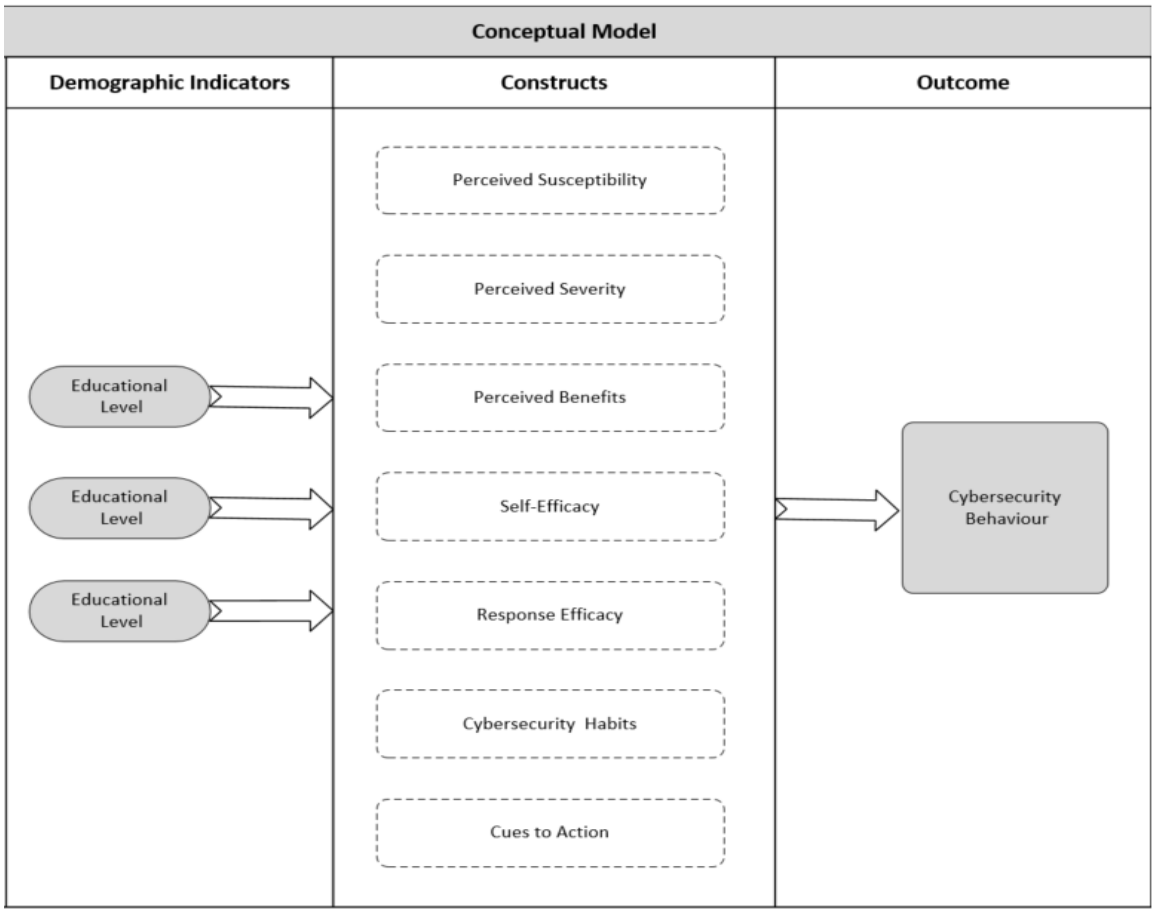
The HBM has evolved over the years and can be applied in various fields including predicting people's behaviour when trying to protect themselves from

cyberthreats (Dodel & Mesch, 2019). In the cybersecurity context, the health behaviour can be substituted with cybercrime behaviour making this model a very useful theoretical model for this research. The HBM can be used to shed more light into why people do not practice in recommended behaviours that would help protect them from being victims of cybercrime (Pickering et al., 2021).

2.12.2 *Conceptual Framework*

The conceptual framework utilised for this study is underpinned by the Protection Motivation Theory (PMT) and the Health Belief Model (HBM). A hybrid of the two theories have been adopted to provide a fit-for-purpose lens into the specificities of the user's cybersecurity behaviour with an e-commerce context. Combining the two theories to come up with a custom framework also helps to introduce and understand how the demographic factors of age, gender, and educational level impact the cybersecurity behaviour of user's when utilising e-commerce platform in a South African context.

Figure 3: Conceptual framework



The table below identifies the constructs that will form part of the research as depicted by the conceptual framework.

Table 3: Conceptual framework constructs

Construct	Description
Perceived Susceptibility	Refers to the subjective perception of how an individual evaluates their vulnerability to potential cyberthreats and risks (Begum et al., 2022).
Perceived Severity	Refers to the subjective perception of how an individual evaluates the depth of the harm or negative consequences of experiencing a cybersecurity issue (Begum et al., 2022).
Perceived Benefit	Refers to an individual's perception of how what could be positively gained by practicing the recommended cybersecurity behaviour and how they deem the

	effectiveness of the action in preventing a cyberthreat (Dorce et al., 2021).
Self- Efficacy	Refers to an individual's confidence in their ability to practice safe cybersecurity behaviour so that they can be able to fend off possible cyberthreats (Kaufmann et al., 2022).
Response Efficacy	Refers to an individual's confidence that practicing cybersecurity behaviour considered safe will be successful in fending off potential cyberthreats (Zhang et al., 2017).
Cybersecurity Habits	Refers to an individual's routine actions regularly utilised by an individual that can assist in protecting them from cyberthreats and improve their security in the cyberspace.
Cues to Action	Refers to the various outside triggers or signals that will lead to an individual adopting safe cybersecurity behaviour that can help to secure them from potential cyberthreats (Coman et al., 2023).

In conclusion, the rapport between PMT and HBM helps to formulate and aid in formulating a conceptual framework that will provide a basis to understand the dynamics of this study. The conceptual framework provides guidance in assisting to help to interpret the findings of the study and make sense of the outcome.

2.13 Conclusion of literature review

The chapter shows that there has been a wealth of literature related to understanding cybersecurity behaviour as well understanding the common cyberthreats (Anwar et al., 2017; Bartczak, 2021; Chigada & Madzinga, 2021; Chua et al., 2018; Fatokun et al., 2019; Oz et al., 2022; Pieterse, 2021). This study evaluated on most recent literature with majority of them not more than seven years old. This was a conscious decision because of the understanding of how much the cybersecurity, cybercrime and e-commerce platforms continue to evolve at a fast pace over the last few years.

The evaluated literature shows that organisations and individuals are investing resources into ensuring that users of their internet platforms are consistently aware of best practice cybersecurity behaviour. Various demographic factors have been evaluated by different researchers to understand their influence if any on the cybersecurity or cybercrime vulnerability. Various studies have found different findings with some concluding that it has no effect whilst others have significant effect on cybersecurity behaviour. The review of literature also noted that most of the studies focused on university students or employees of a particular organisation which presented a risk of a homogeneous sample.

Significant review was conducted of the existing literature to understand the common types of cyberthreats. It is evident that cybercriminals are continually evolving their attack methods depending on their specific objective and understanding of the weaknesses of their targeted consumers. However, it was also clear that as the methods evolved the basics remained the same which include targeting and trying to manipulate or deceive the end users into obtaining the required information using different vectors which include social media, malicious software and fake websites and applications.

This study will focus on understanding if age, gender, and educational level has any effect on the cybersecurity awareness of people. The scope will be limited to understanding the awareness within an e-commerce platform context and will seek to add to the conversation and contribute to this subject area with a South African context.

Below are the identified hypotheses of this study:

2.13.1 *Hypothesis 1*

There is a significant relationship between cybersecurity behaviour and age in South African e-commerce users.

2.13.2 *Hypothesis 2*

There is no significant difference in cybersecurity behaviour between male and female e-commerce users in South Africa.

2.13.3 *Hypothesis 3*

There is a significant relationship between cybersecurity behaviour and educational level in South African e-commerce users.

2.13.4 *Hypothesis 4*

The combined impact of age, gender, and educational level can significantly predict cybersecurity behaviour in South African users.

While this study primarily utilised the Protection Motivation Theory (PMT) and the Health Belief Model (HBM) to explore cybersecurity behaviour, other theoretical frameworks, such as the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM), also offer valuable perspectives. The TPB could provide insights into how attitudes, subjective norms, and perceived behavioural control influence cybersecurity actions, while the TAM focuses on perceived ease of use and perceived usefulness, which could be particularly relevant for understanding user engagement with security technologies.

In summary, the literature review has delved into key concepts and previous studies related to e-commerce platforms, demographics (age, gender and education level), common cyber threats, geographical and cultural factors as they pertain to cybersecurity behaviour. By critically analysing existing research, gaps and limitations where identified. This chapter has further emphasised the relevance of the current study and provided a fit for purpose theoretical framework for the research. Extending on this foundation, the following chapter will outline the research methodology, detailing the approach, design, and procedures utilised to gather and analyse data in this study.

CHAPTER 3. RESEARCH ETHODOLOGY

This section outlines the plan followed to ensure that the research problem articulated is addressed reliably and as accurately as possible. The research methodology describes in detail the plan of how the study produced valid results consistent with the requirements of this research (Hofstee, 2018).

3.1 Research approach

The research approach pertains to the steps and procedures as related to the research method as well as the research types to be used. This study will make use of the quantitative method to enable the researcher to collect data that directly responds to the research questions (Creswell & Guetterman, 2020). One of the main reasons for selecting the quantitative approach is that it allows for an independent investigation of the constructs without any bias of the researcher (Tan, 2022). A quantitative approach provides an effective way of obtaining and quantifying the views, opinions, and behaviour of respondents in certain situations or scenarios (Hofstee, 2018).

Making use of quantitative research will provide the researcher with some of the following benefits (Saunders & Lewis, 2012):

- Provides a means to gain insights of a large population through a smaller sample.
- The findings of the study are more scientific with the data obtained analysed through statistical methods and hence helping to minimise researcher bias.
- Likely to provides more reliable results that can be repeated or replicated in other studies.

Numerical data collected was analysed using statistical methods and tools to derive useful patterns in a way that allows for easy interpretation of the data and assist to fully understand the impact of age, gender, and educational level on cybersecurity behaviours through the lenses of South African e-commerce users.

3.2 Research design

Research design refers to the framework that will be utilised in the research to bring together different components of a study to address the research problem and achieve the research objectives (Creswell & Guetterman, 2020).

This study employed a survey as the research design. Using survey as the research design enables for a smaller group of the population (sample) to be used in deducing the population behaviour, attitudes, and opinions (Tan, 2022). Surveys provide a way for the study to obtain quantifiable variables of age, gender, educational level, and correlate these with the respondents' cybersecurity behaviour as it relates to their experience in e-commerce platforms. Selecting to utilise surveys was beneficial as this proved to be a quick and relatively easier way to obtain responses on a sample and then inferring the outcome to the larger population of South African e-commerce users (Creswell & Guetterman, 2020).

The survey design employed for this study was a cross-sectional survey design which is the most popular survey design according to (Creswell & Guetterman, 2020). Cross sectional provided a framework that allowed the capturing of age, gender, and educational level of the respondents at a particular point in time to understand the cybersecurity behaviour of South African e-commerce users.

Cross sectional quantitative design was chosen and proved to be an effective approach for this study because it allowed for the collection and analysis of the data over a short period of time which aligned with the limited time available (Tan, 2022). Cybersecurity trends and behaviours can change over time and this research design approach enabled the study to capture the views, attitudes, and behaviour of respondents at a moment in time providing more current and relevant insights.

3.3 Data collection methods

Data collection is systematic series of activities of eliciting and obtaining relevant data that answers the research questions and address the research problem

(Creswell & Guetterman, 2020). A questionnaire with a list of close-ended questions was used as the data collection method for this study. A questionnaire is set of questions that are intended to solicit information from the respondents (Tan, 2022).

The questionnaire was created using a web-based software called Qualtrics which also provides functionality to view feedback from respondents as well as generate reports in different formats. Qualtrics is an online platform and so this enabled the questionnaire to be conveniently shared with the targeted population easily and timeously via a link. The questionnaire was created to accommodate participants utilising either computers (laptops and desktops) or mobile devices. For the computers, operating systems like Windows, MacOS and Linux whilst for the mobile devices, Android and iOS were catered for.

Peer review

Before finalising the questionnaire, a meticulous review was done to ensure that it was error free, clear, and addressed the research objectives. Colleagues in the research community assisted in peer-reviewing the relevance of the questions and checking that it addressed the constructs of the study. Some questions and questions were removed because of this exercise.

Pilot study

Subsequently, the updated draft questionnaire underwent a pilot study with five of eleven of my colleagues who represented a subset of the target population of e-commerce users in South Africa. The researcher gave the six participants of the pilot study a summary of the research problem, objectives, and the conceptual framework beforehand. Insightful input was provided concerning grammatical concerns, clarity of questions, question length, and the appropriateness of the survey queries. The questionnaire was further refined by simplifying the questions, correcting grammatical mistakes, and reordering the sequence of some questions. The pilot study was conducted on the Qualtrics platform which also helped to identify any potential technical and user experience challenges arising from the tool. This exercise helped the researcher to get familiar with utilising Qualtrics to monitor feedback and progress.

Once the questionnaire was finalised, a link was made available to participants utilising diverse channels like social media platforms (WhatsApp, Facebook, Instagram, LinkedIn), targeted SMS and email. Making use of these accessible platforms and channels contributed to receiving of relatively high responses. Qualtrics provided the researcher with tools and functionality to view the survey progress, collection of the data and presenting it into downloadable reports which was used as input for statistical analysis. The researcher sent out notifications to the invited participants who might not have had a chance to complete after a couple of weeks.

Data collection was closed on Qualtrics by the researcher when the number of responses had reached 386 as this had reached the minimum required sample size. More responses would have been ideal but based on the limited timelines to finalise the study, data collection was stopped at his juncture.

3.4 Population and sample

3.4.1 *Population*

For the purposes of this study, the target population are individuals who have used e-commerce platforms in South Africa. A population is all the people who qualify to be part of the study and is the source of the sample (Creswell & Guetterman, 2020).

Demographic indicators of age, gender and education levels are analysed on how they impact the cybersecurity behaviour of e-commerce users in South Africa. The target population consists of e-commerce users and those were individuals that would have bought goods or services in South Africa. The participants had to at least 18 years at the time of the survey. The participants needed to have consented voluntarily to take part in the survey. Individuals who did not meet the stated criteria were therefore excluded from the study.

3.4.2 *Sample*

A sample is a subset of the population that is going to be studied, and the outcome used to generalise the behaviour of the much larger group which is the population (Creswell & Guetterman, 2020). The sample for this study was obtained from users who have used e-commerce in South Africa.

Participants were included in the study if they were at least 18 years and had used an e-commerce platform while in South Africa, or a South African e-commerce platform from a foreign country (outside South Africa). The survey aimed to elicit insights from individuals who had experience with e-commerce within the South African context, regardless of their current residence. There was no requirement for participants to currently reside in South Africa. However, they needed to have engaged in online shopping either on an international platform like Alibaba while in South Africa, or on a South African platform like Takealot from abroad. Individuals who did not meet this criterion, such as those under 18 or those who had never engaged in e-commerce activities related to South Africa, were excluded from the study.

A total of 316 participants passed the inclusion criteria for this study and were used for statistical analysis. The sample had participants with ages ranging from 18 years to over 60 years with the 41- 45 years age group contributing the most (17.4%) and the over 60 years having the least (4.7%). In terms of gender, the females dominated the sample with 62%, males (37.7%) and non-binary (0.6%). Highest educational level represented in the sample was varied with bachelor's degree dominating with 20.6% and those with a doctorate degree having the least at 4.4%.

The participants in the study were recruited through an online survey link shared through social media platforms, emails, and SMS. The inclusion criteria were based on users who have transacted on e-commerce platforms in South Africa before and were at least 18 years of age.

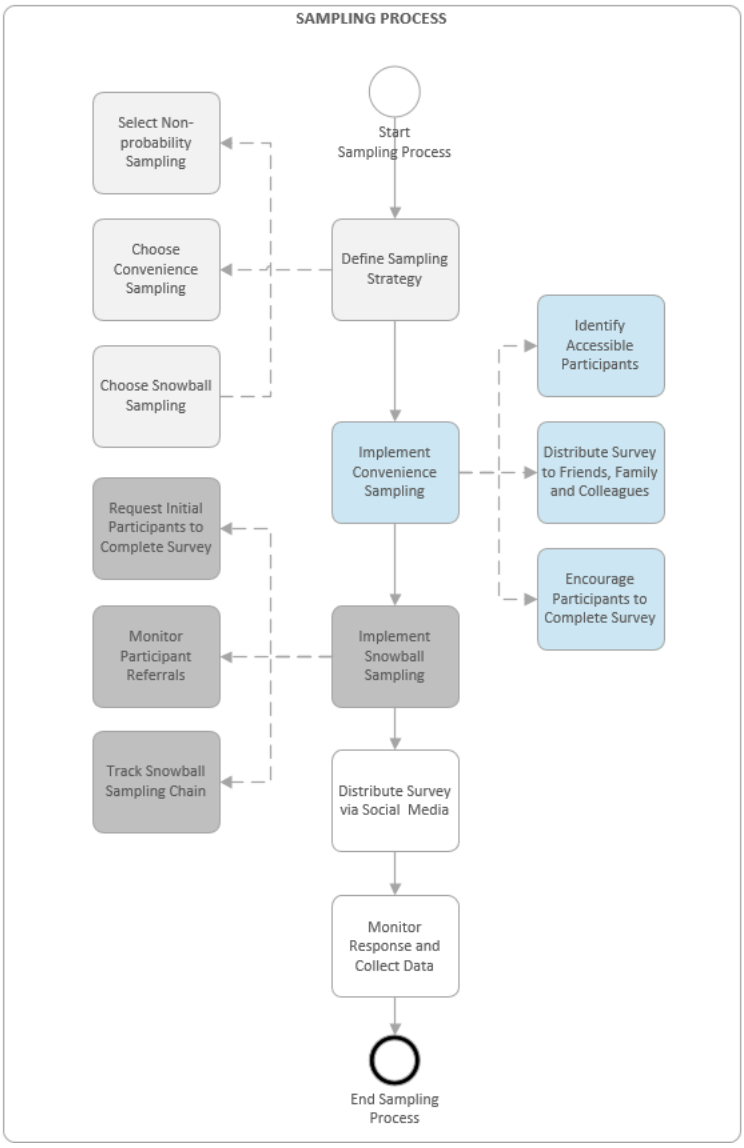
3.4.3 *Sampling method*

The study employed non-probability method specifically convenience and snowball sampling for identifying the participants in the survey. This method was used because it was convenient based on them being available and participants who were willing to take part in the survey (Creswell & Guetterman, 2020).

At the initial phases of the survey, convenience sampling was used to select participants like work colleagues, classmates, friends, and family who were easily accessible. This approach enabled the study to gather data from a broad range of South African e-commerce users, leveraging both direct contacts and extended networks.

The diagram below illustrates the sampling process used in this study, detailing each step involved in recruiting participants through convenience and snowball sampling methods. This visual representation highlights how the survey was initially distributed to a readily accessible group and subsequently expanded through participant referrals and social media to ensure a diverse and comprehensive sample.

Figure 4: Sampling process



Some of the participants identified as part of this method were not known to the researcher and were sampled from social media platforms. The survey was also published on social media platforms, allowing for quick and convenient distribution among diverse users who were readily available and willing to participate. These were participants who expressed a propensity to engage and complete the survey. Utilising convenience sampling was beneficial for the study as it enabled for more responses to the survey to be obtained in the limited time available (Creswell & Guetterman, 2020; Tan, 2022).

To further expand the sample size and reach a more diverse demographic, snowball sampling was incorporated. The initial sample consisted of a small circle

of participants. Participants who received the survey were encouraged to forward it to others within their networks, including those who might not have been reached through the initial distribution methods. This method helped to generate a large volume of responses though the researcher had no visibility of the individuals who eventually ended up forming part of the sample (Tan, 2022).

3.5 The research instrument

The study employs an online questionnaire as the research instrument to elicit primary data from respondents. An online questionnaire is an instrument used to obtain data from respondents and is accessed using a link via the internet through a smart device such as a desktop, laptop, smartphone, tablet etc. (Creswell & Guetterman, 2020).

A questionnaire was chosen for this study because of its capability to effectively elicit responses and allowing for the statistical analysis of the received responses. The questionnaire was developed with an objective to capture the demographic indicators of age, gender and education level and the self-reported cybersecurity behaviour of the e-commerce users in South Africa.

The first question was to ascertain if the user had utilised e-commerce platforms in South Africa and any respondents indicating that they had not were excluded from the study. The next section was used for capturing the three demographic indicators of age, gender, and educational level of the respondent. Age was dived into age groups, the highest education level obtained was captured and the participant could select their gender.

The questionnaire has eight other different sections linked to the constructs of the study to help address the aspects of self-efficacy, response efficacy, cues to action, perceived benefits, perceived susceptibility, perceived severity. A 5-point Likert interval scale using close ended questions with options between “strongly agree” and “strongly disagree” were provided for these sections. This scale was selected because it is common and well understood by a lot of people. Questions are close ended which allows for quicker and more detailed analysis (Tan, 2022).

Close ended questions help the respondents to complete the questions quicker and improve the response rate.

Using the questionnaire will allow the study to elicit responses to ascertain the respondent attitudes and beliefs based on each question presented. The responses will be analysed and provide insights into the research problem which is the focus of the study.

A questionnaire will provide a tool for posing structured questions directly to respondents and this instrument provides advantages and disadvantages. Structured questions will ensure that the all the respondents are provided with the same questions and hence the results can be evaluated on the same basis improving the quality of the results (Hofstee, 2018). A questionnaire is the selected instrument for the study as it will provide primary data from the respondents enhancing the quality of the outcome.

Even though a questionnaire provides significant advantages for this study it provides several limitations. The researcher will not be able to interact directly with the respondents. This limits the ability to pick up and observe any other non-verbal responses which could be useful for the study. This also prevents the researcher from asking probing and unstructured questions to get a deeper understanding on some other aspects of the study.

3.6 Procedure for data collection

Data for this study will be collected using a questionnaire that will be sent out to the participant via email or a social media link and hosted on Qualtrics which is an online platform. Making use of Qualtrics provides the respondents with a simple, secure, and easy to use platform helping to improve the quality and volume of results. The design of the online survey allows convenience and flexibility for the participants to complete the questionnaire at their own speed and using a device of their choice.

Participants to the study will be invited using various platforms on social media, targeted emails, and SMS. Initially utilising convenience sampling to identify a

small sample of participants known to the researcher. Snowball sampling will then be used to encourage the initial participants to forward to other participants they know who meet the inclusion criteria of the study. Each link to the survey will contain a brief overview of the study, its objectives and indicate clearly that participation is entirely voluntary.

The expected duration of the survey was 10 minutes with only relevant questions to the study being asked with a view to minimise the length of time as much as possible. Measures were taken to ensure the quality and relevance of the research instrument which included conducting a peer review and pilot testing with a small number of the sample participants.

All the responses received were secured and password protected by the researcher to ensure the privacy of the participants. The data was also secured through access control mechanisms. Physical security of the hardware used to store the data was used to keep the data safe from unauthorised access. Assurances were given and adhered to protect the confidentiality of the participants.

During the collection of data, the researcher consistently checked for the progress in the received data on Qualtrics. Follow up reminders to the respondents was sent out to help improve the volume of responses.

3.7 Data analysis strategies and interpretation

Quantitative research design using a survey to collect data on the demographics of age, gender, and educational level as well the cybersecurity behaviour of the respondents. Responses were obtained from the survey and used for data analysis.

The data obtained to understand cybersecurity behaviour was scored by associating each response with a numeric value. This helped to come up with a standard way of quantifying and compare the cybersecurity behaviour responses. Utilising a scoring system for the responses enabled the analysis of the responses to assist in developing and identifying patterns and trends.

Data was prepared to ensure that the collected raw data is cleaned and enhance the reliability of the data so that it ready to be analysed. The raw data obtained via the online survey from the was transferred to a statistical tool, Statistical Programme for Social Sciences (SPSS). SPSS was used for this study because it a very common software package and it can be used to interpret complex data quite easily (Creswell & Guetterman, 2020). The statistical tool was also readily available from the researcher's institution. The variables were then checked for the correctness of the coding and alignment with the research objectives.

3.8 Possible limitations and challenges of the study

The following limitations apply to this research and should be considered when analysing the findings:

- The study has a relatively timeframe of less than 6 months to elicit responses from the participants which limit the number of respondents who can be reached.
- Data will not be obtained from any respondents less than 18years even though some of them make use of e-commerce platforms.
- Data obtained from the respondents cannot be verified for accuracy.
- Access to literature was limited as some research material could not be accessed due to cost constraints as some of the platforms required a payment subscription.
- The field of study related to cybersecurity behaviour and cyberthreats is a fast-evolving field and hence some materials relied on could have been outdated even though priority was placed on sourcing the latest information.

Utilising convenience and snowball sampling assisted provided an efficient approach for data collection but it also introduced certain limitations. By initially sending the survey to friends, classmates, family, work colleagues, and then encouraging participants to share it further within their networks, the study may have introduced selection bias. This sampling approach relies on participants who are easily accessible or within specific social networks, which might not be

a fair representation of the South African e-commerce users' population. Additionally, the use of social media for survey distribution could lead to a sample leaning towards individuals who have resources to be online, possibly excluding those with no internet access. This can limit the relevance of the findings, as they may not fully reflect the diversity South African e-commerce users. These limitations should be considered when interpreting the study's findings and drawing conclusions.

3.9 Quality assurance

Quality assurance refers to the mechanisms and procedures put in place to ensure the reliability, quality, and validity of the study at various stages of the study as defined by Lavrakas (2012). Prioritising quality assurance is important so that the findings are reliable and can provide useful insights and contribute positively to the field.

3.9.1 *External validity*

External validity refers to the extent to which the findings of the study can be used to predict other situations (Tan, 2022). The online survey was distributed as widely as possible, and data collected from geographically dispersed respondents in the country. The sample had users with representing various age groups, educational levels and different genders further strengthening the external validity of the study.

3.9.2 *Reliability*

Creswell and Guetterman (2020) describe the reliability of a study as the level to which the findings of a study would stay the same if the same environment was recreated. The same Likert scale will be used for most of the questions on the research instrument helping to standardise the response and hence the consistency of data interpretation. Also, all the respondents will receive a standardised questionnaire with the same questions to eliminate variability in the questions and responses which could negatively impact the reliability of the study.

Cronbach's alpha coefficients indicated a good level of internal consistency strengthening the reliability of the study.

3.9.1 *Internal validity*

Internal validity of the study is hugely dependent on the process followed in the study as well as how meticulously it was conducted (Tan, 2022). The researcher approached the study with objectivity and did not influence the outcome of the study. The questions in the research instrument will be made as short as possible and designed to be simple and clear to minimise ambiguity for the respondents. To further strengthen the internal validity of the study, statistical techniques including factor analysis and correlation analysis were applied.

3.10 Ethical considerations

Due care will be taken to ensure that ethical standards as stipulated by the university will be followed.

- The participants anonymity will be observed, and this will be communicated clearly to them.
- Participants can opt out of the survey at any time if they feel uncomfortable and this will also be clearly communicated to them.
- The study was done at no risk to the participants and no prejudice to them if they decide to withdraw or not participate.
- Permission will be sought from the human resources department of the company where some of the respondents will come from.
- Ethical approval will be sought from the university before engaging with the respondents.

In conclusion, this chapter has discussed the research methodology, including the chosen research approach, design, data collection methods, and ethical considerations. The detailed explanation of the research instrument and sampling strategy ensures the reliability and validity of the study's findings. The next chapter will present the findings derived from the quantitative survey, providing a detailed account of the data collected from the participants of the study.

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

This chapter presents the results and discuss the findings obtained from the questionnaires in this study. In this research, an online questionnaire was the primary tool used to collect data and was distributed to over 600 users, with 382 responses received and eventually 316 responses were considered eligible for the study. The study responses were analysed using SPSS version 29.0. cross tabulations, graphs and other figures will be used to dissect the collected quantitative data. Some inferential techniques like chi-square test values and correlations will be employed with the associated p-values calculated. The p-value signifies significance with an associated value of “$p<0.05$”.

4.2 Statistical analysis and findings

This section provides the statistical insights of the study to understand the intricate relationship between demographic indicators with the cybersecurity behaviour of South African e-commerce users. Insights into the demographic data (age, gender, and educational level) of the participants. The statistical analysis includes factor analysis, reliability statistics, rotated component matrix and correlation analysis, together these assist in providing detailed analysis of the various dimensions impacting cybersecurity behaviour within the South Africa e-commerce context.

4.2.1 *Reliability statistics*

To ensure the reliability of this study, Cronbach alpha was utilised to ascertain the different measurements of the questions in the survey. Reliability is the measure of how the scores obtained in the study can be reproduced if the study was carried out again and at different times (Creswell & Guetterman, 2020).

Reliability coefficient scores of equal to or greater than 0.70 were deemed to be desirable.

The table below depicts the relevant reliability scores (Cronbach alpha) as reflected in the study.

Table 3: Cronbach's Alpha Scores

	Section	Number of Items	Cronbach's Alpha
C	Personal Cybersecurity Practices	9	0.897
D	Self-Efficacy in Cybersecurity	7	0.873
E	Online Risk Awareness	6	0.761
F	Proactive Security Measures	4	0.798
G	Adherence to Security Advice	3	0.712
H	Engagement with Cybersecurity Information	5	0.722
All items included		34	0.921

The reliability scores for all sections exceed the recommended Cronbach's alpha value. This indicates a degree of acceptable, consistent scoring for these sections of the research.

4.2.2 *Factor analysis*

Factor analysis, a statistical method employed to explore the underlying structure of a set of variables, is instrumental in identifying latent constructs that explain patterns of correlations within psychological, sociological, and business research. By reducing many variables into fewer factors, this technique facilitates the interpretation of data, enhancing the understanding of the dimensions that constitute complex constructs. The application of factor analysis ensures the construct validity of a questionnaire by confirming that items grouped under a specific factor indeed measure the same underlying concept. Moreover, it aids in refining instruments and scales by eliminating redundant or irrelevant items, thereby improving the reliability and validity of the measures. In essence, factor analysis is a cornerstone in the development and validation of measurement instruments, providing a robust foundation for empirical research and theory development.

The matrix table is preceded by a summarised table that reflects the results of Kaiser-Meyer-Olkin (KMO) and Bartlett's Test. The KMO Measure of Sampling Adequacy shows a score foreach of the variables that is as a result of underlying factors. is a statistic that indicates the proportion of variance in the variables that might be caused by underlying factors. Scores that are close to 1.0 are show that the factor analysis could be beneficial whilst scores of below 0.50 depicts a factor analysis that might not be valuable.

The other test utilised for this study was the Bartlett's test of sphericity. It is used to check if the hypothesis that the correlation matrix is an identity matrix, which would provide evidence that the variables in question are not correlated which means they cannot be used for structure detection. Generally, values that have a significance level of less than 0.05 show that factor analysis of the data would be valuable.

Factor analysis is done only for the Likert scale items. Certain components divided into finer components. This is explained below in the rotated component matrix.

Table 4: KMO and Bartlett's test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.908
	Approx. Chi-Square	5236.257
	Degrees of	561
	Sig.	< 0.001

All of the conditions are satisfied for factor analysis. That is, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy value should be greater than 0.500 and the Bartlett's Test of Sphericity sig. value should be less than 0.05.

4.2.3 *Rotated component matrix*

Table 5: Rotated component matrix

	Component					
	1	2	3	4	5	6
Not regularly updating my apps and software on my computer, tablet, smartwatch, smartphone can make me more vulnerable to cyber-attacks	0.810	0.124	-0.027	0.178	0.023	0.119
Having my computer, smartphone, smartwatch or tablet infected by a virus is a serious concern for me	0.775	0.056	0.056	0.145	-0.027	0.016
The potential of someone misusing my personal data obtained from e-commerce sites is a major concern for me	0.719	0.128	0.249	0.218	0.063	0.084
I believe that using a public Wi-Fi to transact on e-commerce platforms significantly increases the risk of cybercriminals gaining unauthorised access to my personal information	0.706	0.294	0.254	0.235	0.036	0.061
Understanding e-commerce platform's privacy and security policies helps to ensure the security of my personal information	0.627	0.264	0.019	0.021	0.251	0.213
Using legal and updated software and applications for e-commerce activities helps to protect me from cybercriminals	0.617	0.154	0.015	0.191	0.449	0.034
Using a reputable antivirus software can effectively protect me from cyber threats while engaging in e-commerce activities	0.588	0.214	-0.083	0.098	0.472	-0.042
Keeping abreast of the latest cybersecurity tips specifically related to e-commerce enhances my online shopping safety	0.546	0.296	0.070	0.061	0.194	0.138
Using the same password on multiple e-commerce platforms increases my risk of potential harm resulting from cyberthreats leading to financial loss	0.506	0.294	0.408	0.072	0.220	-0.024
I am confident of identifying and avoiding suspicious activities when doing online shopping	0.062	0.822	0.040	0.089	0.202	0.053
I am confident of recognising a suspicious email without help from anyone	0.153	0.750	0.100	0.338	0.050	0.091
I am confident of recognising a fake e-commerce website address without help from anyone	0.155	0.702	0.102	0.416	0.024	0.124
I am confident that I can configure and manage privacy settings on my social media platforms to control who can access my private information	0.220	0.692	-0.038	0.165	0.054	0.090
I am confident of recognising if my computer, tablet, smartwatch or smartphone is infected by a malware such as a virus, worm etc	0.388	0.566	-0.034	0.404	0.018	0.129
Checking if the sender and subject of emails makes sense is effective in preventing me from being a victim of a cybercriminals	0.339	0.548	0.129	0.055	0.195	0.172
Using two-factor authentication on e-commerce platforms significantly increases my security when shopping online	0.325	0.526	0.274	-0.134	0.196	0.148
I believe that my financial and personal information is at risk of being compromised when shopping online	-0.084	-0.081	0.795	0.044	0.073	0.012

There is a good possibility that my sensitive personal details (passwords, credit / debit card details, username, address etc) could be stolen by unauthorised users	-0.189	0.067	0.710	0.006	-0.067	0.044
Cybercriminals are likely to use my social media information to try and access my e-commerce accounts	0.347	0.168	0.640	0.028	-0.030	0.167
There is a good likelihood that I will receive a malicious attachment via email, WhatsApp, SMS or social media	0.181	0.157	0.628	0.163	0.059	0.006
I am concerned about the security of my accounts specifically on e-commerce platforms	0.172	-0.089	0.611	0.219	0.142	0.000
Sharing my geographic location, children's names, date of birth, Identity numbers etc on public platforms can seriously compromise my security on e-commerce platforms	0.287	0.201	0.466	-0.204	0.213	-0.004
I check my browsers (Chrome, Opera, Microsoft Edge, Safari etc) privacy control and security settings regularly	0.330	0.316	-0.037	0.707	-0.018	0.113
I regularly update my awareness and knowledge about cyber threats targeting e-commerce platforms	0.220	0.219	0.134	0.706	0.121	0.177
I regularly change my password, PIN, pattern or passcode on my smart devices	0.058	0.099	0.185	0.628	0.009	0.164
When browsing e-commerce websites, I mouse over links to see where they go before clicking them	0.364	0.361	0.042	0.559	-0.018	0.132
Following advise received through the public media like newspapers, television, internet and radio will prevent me from being a cybercrime victim when shopping online	-0.066	0.026	0.074	-0.081	0.813	0.164
Complying with the information security policies of e-commerce platforms will help to keep me safe from cybercriminals	0.242	0.150	0.029	0.108	0.762	0.078
Regular password changes to my e-commerce accounts will help to protect me from cybercriminals	0.241	0.185	0.193	0.029	0.601	-0.005
Social media platforms constantly remind me on the latest safe cybersecurity practices	0.198	0.093	-0.004	-0.039	0.013	0.791
I get reminders and notifications from the e-commerce platforms to regularly change my log in password	0.081	0.020	-0.045	0.144	-0.013	0.747
My friends, family or work colleagues sometimes share cybersecurity information with me	-0.173	0.086	0.158	0.266	0.151	0.589
Public articles about cybercrimes and security breaches in the e-commerce sector motivate me to adopt safer online behaviour	0.126	0.361	0.190	0.133	0.209	0.506
I constantly come across cybersecurity information (awareness campaigns) through the media like newspapers, television, internet, billboards and radio	0.238	0.263	0.012	0.284	0.084	0.484

- Extraction Method: Principal Component Analysis.
- Rotation Method: Varimax with Kaiser Normalisation*
- * Rotation converged in 7 iterations.

Principal component analysis employed Varimax with Kaiser Normalization as the rotation method, simplifying factor interpretation by minimizing high-loading

variables on each of the factors. The orthogonal rotation method assists in the examination of inter-correlations between the variables, where similar loadings of questions imply measurement along a common factor. Variables loading at or above 0.5, or the highest loading in cases of cross-loading, effectively contribute to measuring various components.

4.2.4 *Identified themes*

The exploratory factor analysis conducted on the Likert scale data revealed several factors or ‘themes’ that were indicative of distinct patterns in cybersecurity behaviour. These themes represent groups of related survey items that loaded highly on the same factor, suggesting they measure a common underlying construct.

This section includes all the identified themes that emerged because of the analysis of the study respondents in relation to their cybersecurity behaviour. The identified themes help to enhance the understanding of the various factors impacting e-commerce users in respect to cybersecurity behaviour in the context of South Africa.

Personal cybersecurity practices: This component includes behaviours and concerns that reduce vulnerability to cyber-attacks, such as updating apps and using antivirus software.

Self-efficacy in cybersecurity: This theme captures an individual's confidence in their ability to identify and avoid cybersecurity threats without external assistance.

Online risk awareness: This component reflects the awareness of risks associated with online financial and personal information, and the belief that this information could be compromised.

Proactive security measures: This component is related to proactive behaviours such as regularly checking browser security settings and updating knowledge about cyber threats.

Adherence to security advice: Here, the theme is concerned with following advice from various sources to prevent cybercrime victimisation.

Engagement with cybersecurity information: This component involves the frequency and impact of receiving cybersecurity information from social platforms and media, as well as from personal connections.

4.2.5 *Correlation analysis*

Bivariate correlation was also performed on the data. The results are shown below. The results indicate the following patterns. Positive values indicate a directly proportional relationship between the variables and a negative value indicates an inverse relationship. All significant relationships are indicated by a * or **.

Table 6: Correlation analysis

		Personal Cybersecurity Practices	Self-Efficacy in Cybersecurity	Online Risk Awareness	Proactive Security Measures	Adherence to Security Advice	Engagement with Cybersecurity Information
Personal Cybersecurity Practices	Pearson Correlation	--					
	N	316					
Self-Efficacy in Cybersecurity	Pearson Correlation	0,609**	--				
	Sig. (2-tailed)	0.000					
	N	316	316				
Online Risk Awareness	Pearson Correlation	0,342**	0,266**	--			
	Sig. (2-tailed)	0.000	0.000				
	N	316	316	316			
Proactive Security Measures	Pearson Correlation	0,542**	0,630**	0,247**	--		
	Sig. (2-tailed)	0.000	0.000	0.000			
	N	316	316	316	316		
Adherence to Security Advice	Pearson Correlation	0,417**	0,335**	0,240**	0,183**	--	
	Sig. (2-tailed)	0.000	0.000	0.000	0.001		
	N	316	316	316	316	316	
Engagement with Cybersecurity Information	Pearson Correlation	0,350**	0,459**	0,200**	0,459**	0,263**	--
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	
	N	316	316	316	316	316	316

**. Correlation is significant at the 0.01 level (2-tailed).

The correlation matrix provided indicates several general trends in the relationships between different dimensions of cybersecurity behaviour and attitudes.

There is a notably strong positive correlation between "Personal Cybersecurity Practices" and "Self-Efficacy in Cybersecurity" as well as between "Self-Efficacy in Cybersecurity" and "Proactive Security Measures". This suggests that individuals who have confidence in their cybersecurity abilities tend to engage more in personal cybersecurity practices and proactive measures. This is a common trend as self-efficacy is often associated with higher engagement in protective behaviours.

Most dimensions show moderate to strong positive correlations with one another. This interconnectedness indicates that good practices or attitudes in one area of cybersecurity are likely to be associated with good practices or attitudes in another.

All the correlations presented are significant at the 0.01 level, indicating a high level of confidence in the relationships between these dimensions. The consistency of significance across different dimensions suggests that these are not isolated findings, but rather indicative of broader patterns within the data.

Both "Engagement with Cybersecurity Information" and "Proactive Security Measures" are strongly correlated with "Self-Efficacy in Cybersecurity", which implies that those who are more informed and engaged with cybersecurity content may also feel more competent in their cybersecurity abilities and are thus more likely to take proactive steps.

There is a moderate positive correlation between "Adherence to Security Advice" and "Personal Cybersecurity Practices", which could mean that individuals who adhere to security advice are also likely to practice better personal cybersecurity.

"Online Risk Awareness" has a positive correlation with "Engagement with Cybersecurity Information", indicating that awareness of online risks is associated with greater engagement with cybersecurity information.

These trends are consistent with what might be expected in cybersecurity behaviours—knowledge and engagement in one area reinforce and enhance practices in other areas. The strong correlation between self-efficacy and proactive measures underscores the importance of confidence and perceived ability in performing cybersecurity-related actions. It also highlights potential areas for intervention; for example, increasing self-efficacy might be a strategy to improve overall cybersecurity behaviour.

4.3 Demographic data

This section summarises the demographic characteristics of the respondents. This section records critical demographic particulars, thereby establishing a backdrop against which the ensuing analysis is positioned. It serves a dual purpose: firstly, to facilitate a nuanced comprehension of the demographic diversity within the respondent cohort; and secondly, to explore potential correlations between demographic characteristics and the primary outcomes of interest.

4.3.1 *Demographic distribution by age and gender*

This section provides a detailed overview of the demographic composition of the study participants by gender and age.

Table 7: Gender distribution by age

Age (years)		Gender			Total
		Male	Female	Non-binary	
18 - 20	Count	7	16	0	23
	% within Age (years)	30.4%	69.6%	0.0%	100.0%
	% within Gender	5.9%	8.2%	0.0%	7.3%
	% of Total	2.2%	5.1%	0.0%	7.3%
21 - 25	Count	7	26	2	35
	% within Age (years)	20.0%	74.3%	5.7%	100.0%
	% within Gender	5.9%	13.3%	100.0%	11.1%
	% of Total	2.2%	8.2%	0.6%	11.1%
26 - 30	Count	12	30	0	42
	% within Age (years)	28.6%	71.4%	0.0%	100.0%
	% within Gender	10.2%	15.3%	0.0%	13.3%
	% of Total	3.8%	9.5%	0.0%	13.3%
31 - 35	Count	15	24	0	39
	% within Age (years)	38.5%	61.5%	0.0%	100.0%
	% within Gender	12.7%	12.2%	0.0%	12.3%
	% of Total	4.7%	7.6%	0.0%	12.3%
36 - 40	Count	18	17	0	35
	% within Age (years)	51.4%	48.6%	0.0%	100.0%
	% within Gender	15.3%	8.7%	0.0%	11.1%
	% of Total	5.7%	5.4%	0.0%	11.1%
41 - 45	Count	26	29	0	55
	% within Age (years)	47.3%	52.7%	0.0%	100.0%
	% within Gender	22.0%	14.8%	0.0%	17.4%
	% of Total	8.2%	9.2%	0.0%	17.4%
46 - 50	Count	14	18	0	32
	% within Age (years)	43.8%	56.3%	0.0%	100.0%
	% within Gender	11.9%	9.2%	0.0%	10.1%
	% of Total	4.4%	5.7%	0.0%	10.1%
51 - 55	Count	10	11	0	21
	% within Age (years)	47.6%	52.4%	0.0%	100.0%
	% within Gender	8.5%	5.6%	0.0%	6.6%
	% of Total	3.2%	3.5%	0.0%	6.6%
56 - 60	Count	4	15	0	19
	% within Age (years)	21.1%	78.9%	0.0%	100.0%
	% within Gender	3.4%	7.7%	0.0%	6.0%
	% of Total	1.3%	4.7%	0.0%	6.0%
> 60	Count	5	10	0	15
	% within Age (years)	33.3%	66.7%	0.0%	100.0%
	% within Gender	4.2%	5.1%	0.0%	4.7%
	% of Total	1.6%	3.2%	0.0%	4.7%
Total	Count	118	196	2	316
	% within Age (years)	37.3%	62.0%	0.6%	100.0%
	% within Gender	100.0%	100.0%	100.0%	100.0%
	% of Total	37.3%	62.0%	0.6%	100.0%

Overall, the ratio of males to females is approximately 2:3 (37.3%: 62.0%), with less than 1% identifying as non-binary ($p < 0.001$).

The general trend analysis of the gender distribution by age, as detailed in the provided table, allows for the extraction of several key insights regarding the demographic composition of the study's participants. This analysis not only sheds light on the gender and age dynamics within the sample but also offers a foundation for understanding potential implications these demographics may have on the study's findings.

Across the age spectrum, there is a consistent trend of female respondents outnumbering their male counterparts. This is particularly pronounced in the younger age groups (18-25 years and 56-60 years), where females account for a significant majority. This trend could suggest a greater female interest or participation in the context of the study or reflect broader societal trends in gender dynamics within the population sampled.

The age group of 36-40 years stands out with most male respondents (51.4%), a unique deviation from the overall trend where females predominantly exceed males. This indicates specific age-related demographic characteristics that may need to be considered when analysing data and drawing conclusions, especially regarding age-specific behaviours or attitudes that the study aims to explore.

The overall representation of non-binary individuals in the study is minimal (0.6%), with presence only in the 21-25 years age group. This low representation underscores the need for a more inclusive demographic engagement in future research to better understand the spectrum of gender identities.

A significant portion of the study's participants are under the age of 40, with a notable decrease in respondents as age increases beyond this point. This trend suggests that younger individuals are more represented in the sample, which could influence the study's applicability to older populations.

The detailed breakdown within each age group reveals nuanced trends, such as the relatively balanced gender distribution in the 41-45- and 46-50-years age groups, and the stark gender disparities in the 56-60 years age group. These variations highlight the importance of considering age and gender as interrelated factors that could affect the study's outcomes.

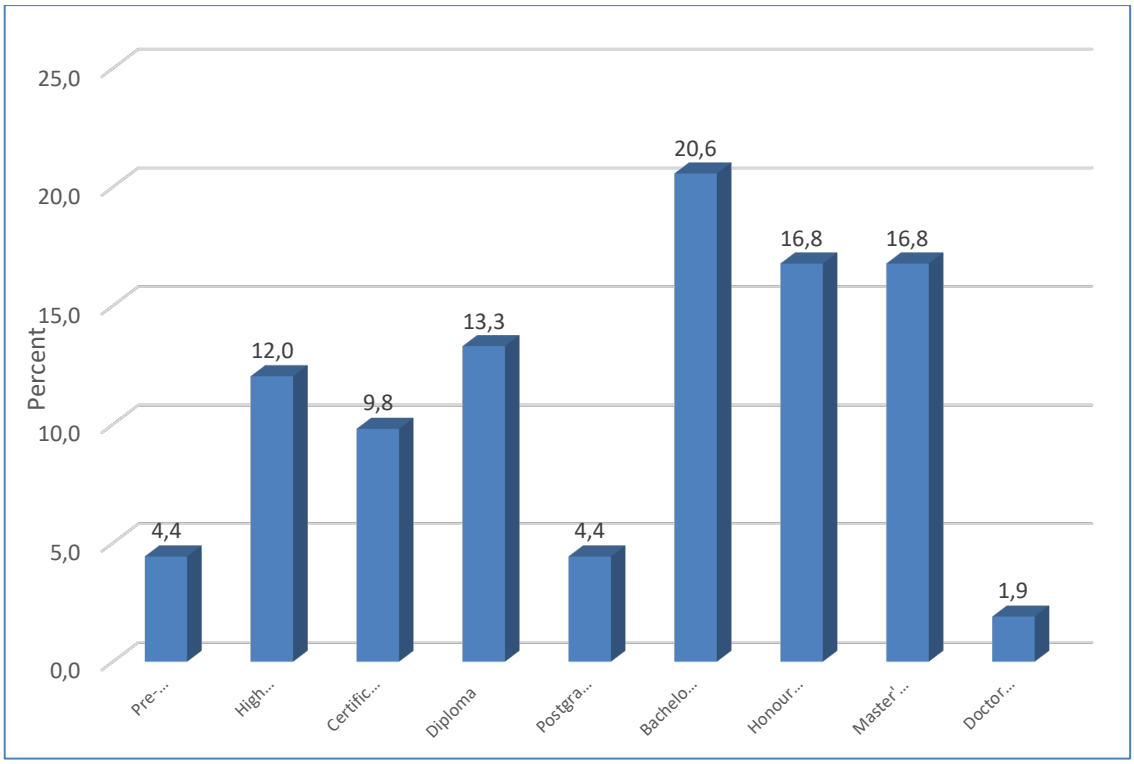
In conclusion, the general trend analysis reveals a complex interplay between age and gender within the sample, with significant implications for the interpretation of the study's results. The predominance of female respondents, the unique gender distribution in specific age groups, and the concentration of younger participants underscore the need to contextualize findings within these demographic realities. Such insights are crucial for ensuring the validity and relevance of the research conclusions, necessitating a careful consideration of how these demographic trends may influence the phenomena under investigation.

4.3.2 *Demographic distribution by education level*

In this section, the results of the statistical analysis of the educational level of the participants will be showcased. Descriptive statistics will be used to provide more intricate details of the sample utilised in the study with a focus to their educational level.

The figure below indicates the education levels of the respondents.

Figure 5: Educational levels



The bar chart offers a visual representation of the educational qualifications of respondents, revealing distinct patterns in the highest educational level qualification obtained.

The chart indicates that a significant majority of respondents, 83.6%, possess qualifications beyond high school, underscoring a high level of educational achievement within the group. This suggests that the respondents are likely to have a strong foundation of advanced knowledge, which could correlate with other factors such as employment levels or specialised skills.

It is also notable that over a third of the respondents (35.7%) have attained a postgraduate degree (encompassing postgraduate diplomas, master's, and doctorate degrees). This level of higher education could be indicative of a sample with a propensity towards professional or academic careers where such qualifications are requisite.

A bachelor’s degree is the most common level of education attained, with 20.6% of respondents, suggesting that this level of qualification is a significant

educational milestone for the group. It serves as a potential gateway to either the workforce or further academic pursuits.

Conversely, the doctorate level has the lowest percentage, at 1.9%, reflecting the typical pyramid structure of educational attainment where each successive academic echelon is achieved by progressively fewer individuals.

Diplomas and certificates also constitute a notable portion of the respondents' qualifications, with 13.3% and 9.8% respectively. These figures highlight a commitment to vocational and continued education, which may be aligned with specific professional requirements or personal development goals.

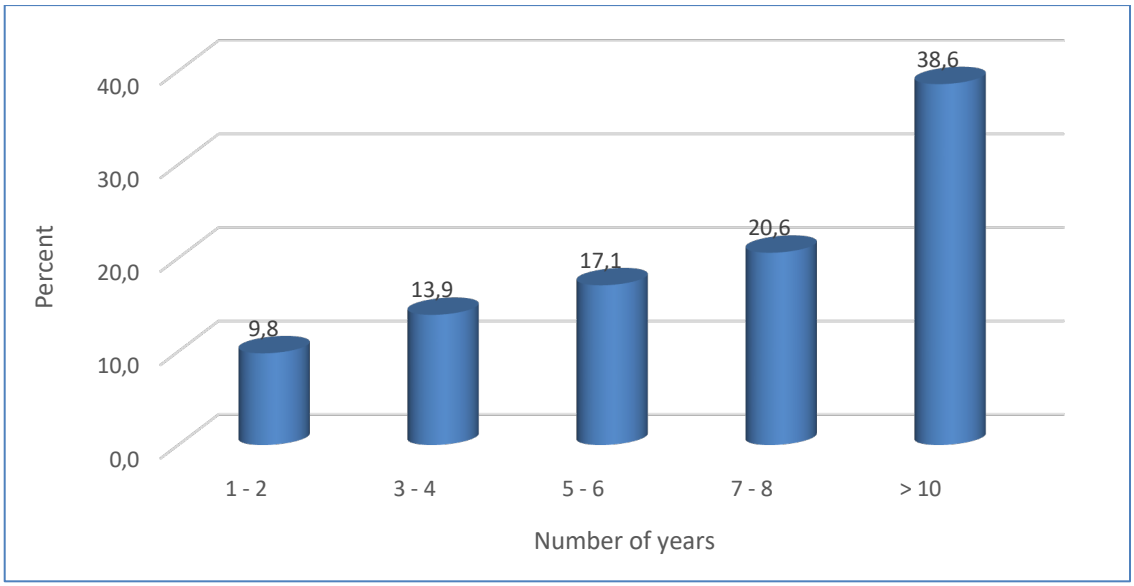
In summary, the chart portrays a respondent pool predominantly skewed towards higher education, which may significantly influence the competencies, perspectives, and opportunities of the individuals represented. The data suggests a trend of advanced education that may reflect the specific demographic or professional context of the respondents.

4.4 E-commerce and e-commerce experience

This section aims to explore the multifaceted dimensions of e-commerce, examining how technological advancements, consumer preferences, and market dynamics interact to shape the online shopping experience.

The figure below reflects the length of time respondents have been using e-commerce platforms.

Figure 4: E-commerce experience

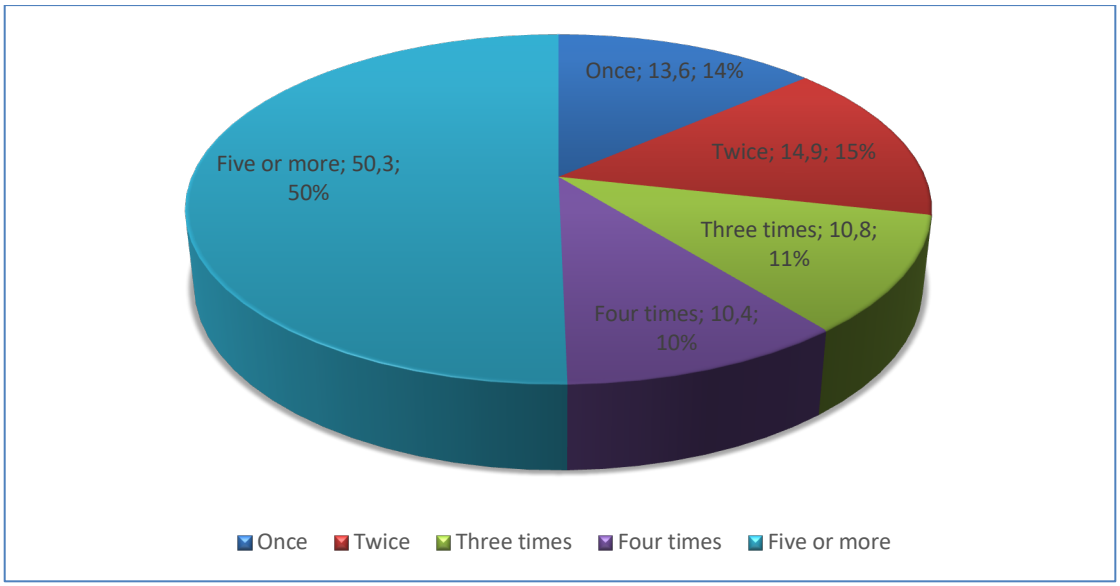


A substantial proportion of the respondents (76.3%) have been using e-commerce platforms for at least 5 years, indicating a significant level of familiarity and potentially greater dependency on these platforms for their shopping needs ($p < 0.001$). The remaining categories display a gradual decrease in percentages with decreasing years of use.

This distribution suggests that the user base of e-commerce platforms is mature, with a considerable number of respondents having over a decade of experience in online shopping. This may reflect broader trends in the adoption of e-commerce, signalling a shift in consumer behaviour towards the digital acquisition of goods and services. Moreover, the data may indicate that e-commerce is not a nascent phenomenon but rather a well-established facet of modern retail that has been growing over the past decade.

The figure below indicates the monthly average of use of e-commerce platforms.

Figure 5: E-commerce monthly average use

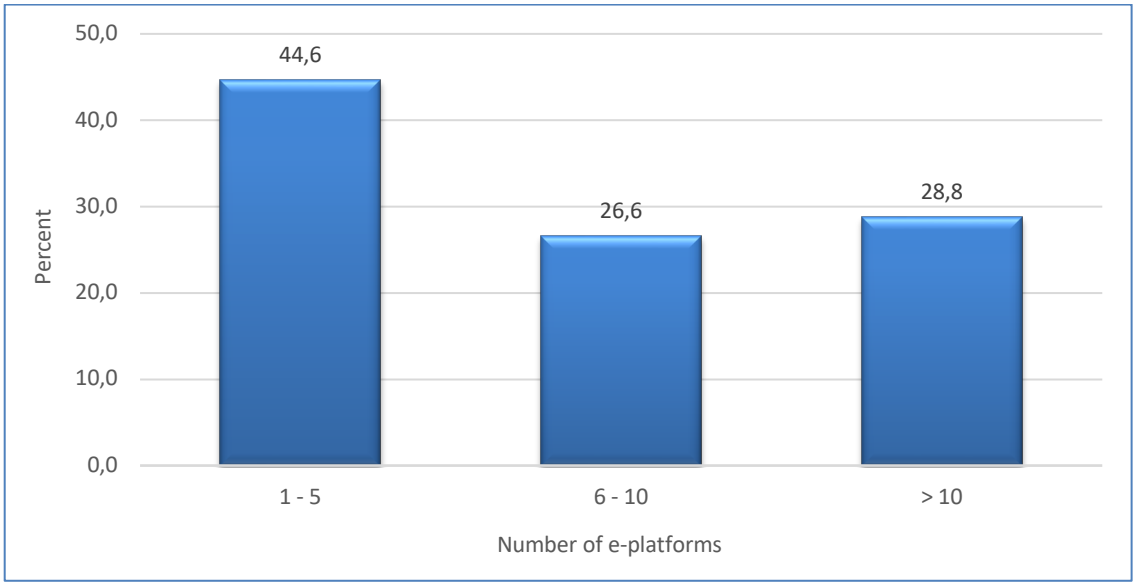


The largest segment, accounting for just over half of the respondents (50.3%), indicates that most users make a purchase on e-commerce platforms once a month. This is followed by those who use these platforms five or more times a month, making up 14.9% of respondents, suggesting a smaller yet significant cohort of highly frequent users ($p < 0.001$).

14,9% of the users engage with e-commerce platforms twice a month, while those using them three times and four times a month represent 10.8% and 10.4% of respondents, respectively. These figures reflect a diverse range of consumer behaviours, from moderate to high-frequency users, highlighting the varied reliance on digital shopping platforms.

The figure below indicates the number of different e-commerce platforms that respondents have used over the past two years.

Figure 6: Number of e-commerce platforms



The most common category, with 44.6% of respondents, is those who have used between 1 and 5 different platforms. This suggests a moderate level of platform diversity, with users likely showing loyalty to a select few services or possibly indicating a market with a few dominant players. The second category represents individuals who have used 6 to 10 different e-commerce platforms, constituting 26.6% of the respondents. This indicates a more exploratory consumer segment that may be open to trying out different platforms, possibly to take advantage of a broader range of products, services, or deals. Finally, the category of respondents who have engaged with more than 10 different e-commerce platforms accounts for 28.8% ($p < 0.001$). This is a significant proportion and suggests a segment of the market that is highly explorative and comfortable navigating across a wide array of digital shopping experiences. This could reflect a consumer drive for variety, better prices, or specific features that are spread across multiple platforms.

Overall, the data reflect a significant spread in the adoption of diverse e-commerce platforms, with a notable number of respondents exploring a wide range of options available to them. This spread has implications for understanding consumer loyalty, the competitiveness of the e-commerce

marketplace, and the effectiveness of multi-platform strategies for e-commerce businesses.

4.5 Scoring pattern analysis

The section that follows analyses the scoring patterns of the respondents per variable per section. The results are first presented using mean scores for the variables that constitute each section. Results are then further analysed according to the importance of the statements.

To determine whether the scoring patterns per statement were significantly different per statement, a binomial test was done, with a cut-off value being the middle value (3.0). The null hypothesis claims that similar numbers of respondents scored above 3.0 (agreement) as there were who scored less than 3.0 (disagreement). The alternate states that there is a significant difference between the levels of agreement and disagreement.

The highlighted significant values (p-values) are less than 0.05 (the level of significance), it implies that the distributions were not similar. That is, the differences between the way respondents scored were significant.

4.5.1 *Personal cybersecurity practices*

This section deals with Personal Cybersecurity Practices, aiming to gauge the attitudes and behaviours of individuals regarding their cybersecurity measures, especially in the context of e-commerce activities. The data presented summarises responses with various metrics. These statements explore various aspects of cybersecurity practices, ranging from the updating of apps and software to the use of antivirus software and the significance of using unique passwords across e-commerce platforms.

The table below summarises the scoring patterns:

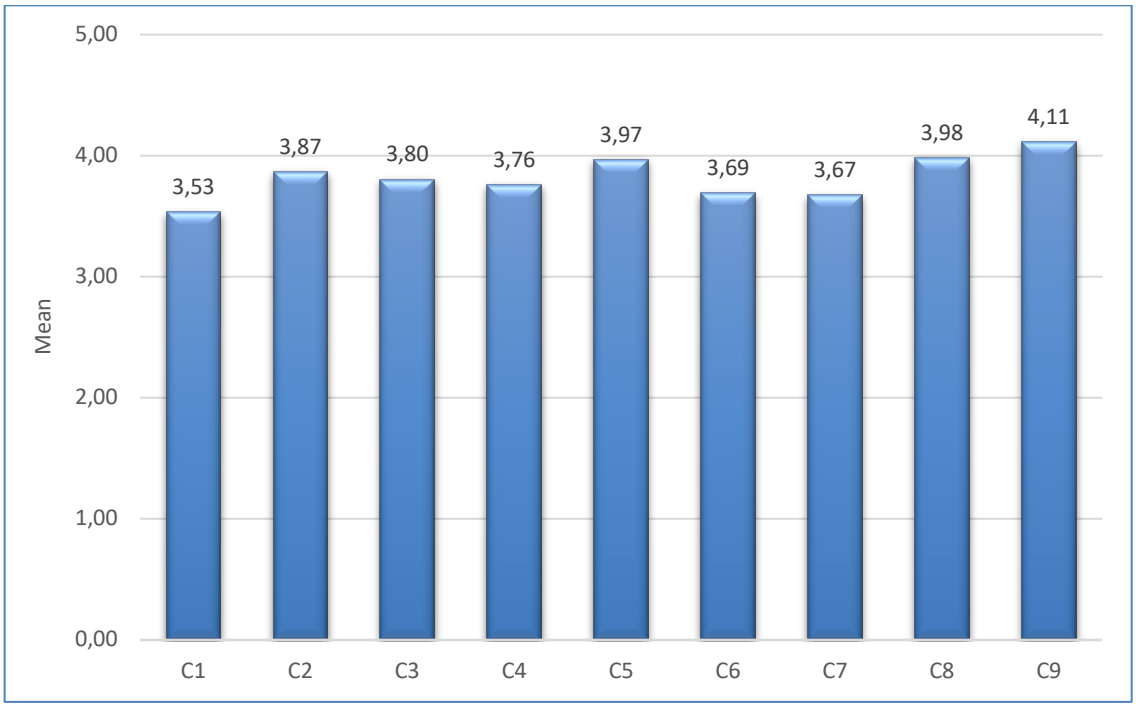
Table 8: Scoring patterns (personal cybersecurity practice)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
C1	Not regularly updating my apps and software on my computer, tablet, smartwatch, smartphone can make me more vulnerable to cyber-attacks	316	3.53	1.19	4.00	2.50	5.00	5.00	1.00	0.053
C2	Having my computer, smartphone, smartwatch or tablet infected by a virus is a serious concern for me	316	3.87	1.09	4.00	3.00	5.00	5.00	1.00	< 0.001*
C3	The potential of someone misusing my personal data obtained from e-commerce sites is a major concern for me	316	3.80	1.03	4.00	3.00	5.00	5.00	1.00	< 0.001*
C4	I believe that using a public Wi-Fi to transact on e-commerce platforms significantly increases the risk of cybercriminals gaining unauthorised access to my personal information	316	3.76	1.16	4.00	3.00	5.00	5.00	1.00	< 0.001*
C5	Understanding e-commerce platform's privacy and security policies helps to ensure the security of my personal information	316	3.97	0.82	4.00	3.00	5.00	5.00	2.00	< 0.001*
C6	Using legal and updated software and applications for e-commerce activities helps to protect me from cybercriminals	316	3.69	0.93	4.00	3.00	4.00	5.00	1.00	< 0.001*
C7	Using a reputable antivirus software can effectively protect me from cyber threats while engaging in e-commerce activities	316	3.67	0.97	4.00	3.00	4.00	5.00	1.00	< 0.001*
C8	Keeping abreast of the latest cybersecurity tips specifically related to e-commerce enhances my online shopping safety	316	3.98	0.90	4.00	4.00	5.00	5.00	1.00	< 0.001*
C9	Using the same password on multiple e-commerce platforms increases my risk of potential harm resulting from cyberthreats leading to financial loss	316	4.11	0.88	4.00	4.00	5.00	5.00	1.00	< 0.001*

*Indicates significant difference i.e. the differences in the responses were significant

All statements show (significantly) higher levels of agreement whilst other levels of agreement are lower (but still greater than levels of disagreement). There are no statements with higher levels of disagreement (means significantly less than 3.0). The significance of the differences is tested and shown in the table above. A cursory analysis of the table reveals several critical insights into the personal cybersecurity practices among the respondents.

Figure 7: Mean scores (personal cybersecurity practices)



The means of the responses predominantly exceed the midpoint (3.0 on a scale of 1 to 5), indicating a general trend of high concern and awareness about cybersecurity threats among participants. This is particularly evident in statements like C9, "Using the same password on multiple e-commerce platforms increases my risk of potential harm resulting from cyberthreats leading to financial loss," which has the highest mean score of 4.11, suggesting a strong consensus on the risks of reusing passwords.

Statements such as C5, "Understanding e-commerce platform's privacy and security policies helps to ensure the security of my personal information," and C8, "Keeping abreast of the latest cybersecurity tips specifically related to e-commerce enhances my online shopping safety," both show high mean scores (3.97 and 3.98 respectively). This underscores the perceived importance of being informed and proactive in safeguarding personal information online.

The minimal variation in the high levels of agreement across different statements (as indicated by the low standard deviations for some statements, e.g., C5 with a

standard deviation of 0.82) suggests a uniform understanding and concern about cybersecurity threats and the effectiveness of various protective measures.

Focusing on the statement C9, which deals with the use of the same password on multiple e-commerce platforms, it is evident that this practice is widely recognized as a significant risk factor for cybersecurity threats. This is supported by a substantial body of literature that highlights the dangers of password reuse, including increased vulnerability to credential stuffing attacks, where attackers use stolen account credentials to gain unauthorized access to a user's other accounts (Das, Bonneau, Caesar, Borisov, & Wang, 2014).

Furthermore, the high level of agreement with statements C5 and C8 indicates a strong recognition of the importance of being informed and proactive about cybersecurity measures. This aligns with the Protection Motivation Theory (Rogers, 1975), which suggests that individuals are motivated to adopt protective behaviours when they perceive a high severity of and vulnerability to threats, and when they believe in the efficacy of the recommended protective actions. The significant agreement with these statements reflects a recognition of the effectiveness of understanding security policies and staying informed about cybersecurity as critical components of online safety.

In conclusion, the data from Section C indicates a high level of concern and awareness among participants regarding personal cybersecurity practices, especially in the context of e-commerce. The uniform agreement across various cybersecurity measures suggests a widespread recognition of the importance of proactive behaviours in mitigating cyber threats. Theoretical frameworks such as the Protection Motivation Theory provide a valuable lens through which to understand these trends, highlighting the role of perceived threats and efficacy beliefs in motivating cybersecurity behaviours. This analysis underscores the critical need for continued education and awareness efforts to enhance personal cybersecurity practices among individuals engaging in e-commerce activities.

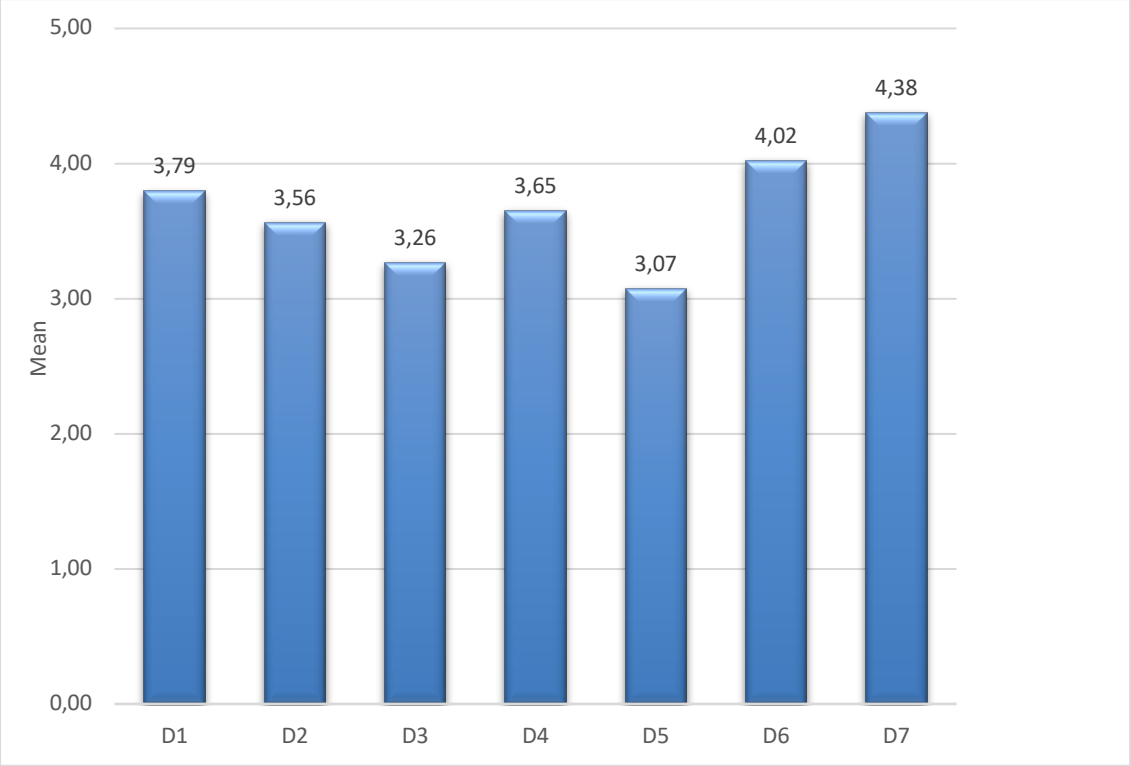
4.5.2 *Self-efficacy in cybersecurity*

This section deals with the findings as they relate to their confidence to practice safe online behaviour as they make use of e-commerce platforms. The results will help to shed light on how the reported confidence levels of the individual and their corresponding ability to keep their data and transaction safe while transacting online.

Table 9: Scoring patterns (self-efficacy in cybersecurity)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
D1	I am confident of identifying and avoiding suspicious activities when doing online shopping	316	3.79	0.92	4.00	3.00	4.00	5.00	1.00	< 0.001
D2	I am confident of recognising a suspicious email without help from anyone	316	3.56	1.13	4.00	3.00	4.00	5.00	1.00	< 0.001
D3	I am confident of recognising a fake e-commerce website address without help from anyone	316	3.26	1.19	3.00	2.00	4.00	5.00	1.00	0.955
D4	I am confident that I can configure and manage privacy settings on my social media platforms to control who can access my private information	316	3.65	1.09	4.00	3.00	4.00	5.00	1.00	< 0.001
D5	I am confident of recognising if my computer, tablet, smartwatch or smartphone is infected by a malware such as a virus, worm etc	316	3.07	1.26	3.00	2.00	4.00	5.00	1.00	0.028
D6	Checking if the sender and subject of emails makes sense is effective in preventing me from being a victim of a cybercriminals	316	4.02	0.81	4.00	4.00	5.00	5.00	1.00	< 0.001
D7	Using two-factor authentication on e-commerce platforms significantly increases my security when shopping online	316	4.38	0.75	5.00	4.00	5.00	5.00	2.00	< 0.001

Figure 8: Mean scores (self-efficacy in cybersecurity)



The data presents an insightful overview of the participants' self-reported confidence levels in managing cybersecurity threats:

Most of the statements report means above the midpoint of 3.0, indicating a generally high level of confidence among respondents in their cybersecurity competencies. Notably, the statement D7, "Using two-factor authentication on e-commerce platforms significantly increases my security when shopping online," exhibits the highest mean score of 4.38, highlighting a strong consensus on the efficacy of two-factor authentication as a security measure.

While overall confidence levels are high, there is noticeable variability. For instance, statement D3, "I am confident of recognising a fake e-commerce website address without help from anyone," has a mean score of 3.26, close to the neutral point, and a binomial test p-value of 0.955, indicating less confidence in this specific area compared to others. This suggests that while respondents feel generally competent in cybersecurity practices, their confidence varies depending on the complexity of the task.

The high mean score of 4.02 for statement D6, "Checking if the sender and subject of emails makes sense is effective in preventing me from being a victim of a cybercriminal," underscores a strong belief in proactive measures like scrutinizing email senders and subjects to avoid phishing attacks.

Focusing on D5, "I am confident of recognising if my computer, tablet, smartwatch, or smartphone is infected by malware such as a virus, worm, etc.," which has one of the lower mean scores (3.07), it's notable that while there's a general confidence in dealing with cybersecurity issues, detecting malware infections presents a challenge for some. This reflects findings in cybersecurity literature that emphasize the subtlety and sophistication of modern malware, which can often evade detection by users without specialized knowledge or tools (Gopinath & Sethuraman, 2023).

In contrast, the strong confidence expressed in D7 about the efficacy of two-factor authentication aligns with current cybersecurity recommendations that highlight two-factor authentication as one of the most effective defences against unauthorized access (Cao et al., 2023). This reflects a broader understanding and acceptance of two-factor authentication as a critical security measure.

The analysis reveals a pattern of self-efficacy in cybersecurity among participants. There is a generally high level of confidence across most areas, with specific strengths in recognizing phishing attempts and the value of two-factor authentication. However, challenges remain in areas requiring more technical knowledge, such as recognizing malware infections and fake e-commerce websites. These findings underscore the importance of targeted cybersecurity education and training that addresses these knowledge gaps, enhancing individuals' confidence and competence in navigating the evolving landscape of cyber threats. Theoretical models of self-efficacy suggest that such educational interventions can significantly enhance individuals' perceived self-efficacy, leading to more effective and proactive cybersecurity behaviours (Kaufmann et al., 2022).

4.5.3 *Online risk awareness*

In this section, the findings related to the pivotal construct of online risk awareness are presented as collected from the study participants. The questions which formed part of the online questionnaire seek to get an understanding of the individual's perception of cyberthreats to their financial and personal information whilst transacting on e-commerce platforms. The results as presented based on the self-reporting of the individuals. Each of the responses to the survey questions is statistically analysed through the standard deviations, mean scores, medians etc., including binominal test p-values to validate statistical significance of the user perceptions.

Table 10: Scoring patterns (online risk awareness)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
E1	I believe that my financial and personal information is at risk of being compromised when shopping online	316	3.76	1.02	4.00	3.00	4.00	5.00	1.00	< 0.001
E2	There is a good possibility that my sensitive personal details (passwords, credit / debit card details, username, address etc) could be stolen by unauthorised users	316	3.76	1.05	4.00	3.00	4.00	5.00	1.00	< 0.001
E3	Cybercriminals are likely to use my social media information to try and access my e-commerce accounts	316	3.41	1.18	4.00	2.00	4.00	5.00	1.00	0.160
E4	There is a good likelihood that I will receive a malicious attachment via email, WhatsApp, SMS or social media	316	3.89	0.90	4.00	3.00	4.00	5.00	1.00	< 0.001
E5	I am concerned about the security of my accounts specifically on e-commerce platforms	316	3.62	1.06	4.00	3.00	4.00	5.00	1.00	< 0.001
E6	Sharing my geographic location, children's names, date of birth, Identity numbers etc on public platforms can seriously compromise my security on e-commerce platforms	316	4.22	0.76	4.00	4.00	5.00	5.00	1.00	< 0.001

The analysis of Section E reveals key trends regarding online risk awareness among the survey participants.

The data indicates a general acknowledgment of the risks associated with online activities. For example, both E1, "I believe that my financial and personal information is at risk of being compromised when shopping online," and E2, "There is a good possibility that my sensitive personal details could be stolen by unauthorized users," have mean scores of 3.76. This suggests a high level of concern among respondents about the security of their personal and financial information online.

The concern for specific risks, such as the potential for geographic location and other personal details to compromise security on e-commerce platforms (E6), is particularly pronounced, with a mean score of 4.22. This indicates a strong awareness of how certain types of shared information can significantly increase online risks.

While there is a generally high level of concern across all areas, there is some variability in the perceived level of threat. For instance, the concern about cybercriminals using social media information to access e-commerce accounts (E3) has a slightly lower mean score of 3.41 and a binomial test p-value of 0.160, suggesting a less unanimous agreement on this risk compared to others.

Focusing on E6, the high mean score reflects a particularly acute awareness of the risks associated with sharing personal information such as geographic location, children's names, dates of birth, and identity numbers on public platforms. This concern is well-founded, as literature in cybersecurity highlights how such information can be exploited by cybercriminals to carry out identity theft, social engineering attacks, and other forms of cyberattacks (van Schaik et al., 2017). The high level of awareness around this issue underscores the importance of privacy management and cautious sharing practices on social media and other public platforms.

The findings from Section E underscore a significant level of online risk awareness among the participants, with a particularly strong concern for the

security of personal and financial information on e-commerce platforms. The data reflects a nuanced understanding of the various risks associated with online activities, indicating a recognition of the complex landscape of cybersecurity threats (Diniz et al., 2014; Silaule et al., 2022). This awareness is crucial for the development of effective risk management strategies, emphasizing the need for ongoing education and proactive measures to safeguard against online threats. Theoretical frameworks such as the Health Belief Model can provide insight into how risk perception motivates individuals to adopt protective behaviours online (Ng et al., 2009). Enhancing online risk awareness and promoting informed cybersecurity practices are essential steps in mitigating the risks posed by cybercriminals and ensuring the safety of individuals' personal and financial information in the digital age (Dodel & Mesch, 2017; Koloseni et al., 2019).

4.5.4 *Proactive security measures*

In this section the participants responses to how they respond to secure online practices proactively to protect themselves from cyberthreats as they transact on e-commerce platforms. The findings are a culmination of the self-reported responses to questions related to management of e-commerce passwords, keeping abreast of cyberthreats etc. The findings are statistically analysed and for variability and statistical significance to understand how they impact the cybersecurity behaviour of the respondents.

Table 11: Scoring patterns (proactive security measures)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
F1	I check my browsers (Chrome, Opera, Microsoft Edge, Safari etc) privacy control and security settings regularly	316	2.66	1.34	2.00	1.00	4.00	5.00	1.00	< 0.001
F2	I regularly update my awareness and knowledge about cyber threats targeting e-commerce platforms	316	3.09	1.27	3.00	2.00	4.00	5.00	1.00	0.063
F3	I regularly change my password, PIN, pattern or passcode on my smart devices	316	2.82	1.24	3.00	2.00	4.00	5.00	1.00	< 0.001
F4	When browsing e-commerce websites, I mouse over links to see where they go before clicking them	316	2.79	1.36	3.00	2.00	4.00	5.00	1.00	< 0.001

The responses from Section F provide insight into the frequency and diligence with which participants undertake specific proactive cybersecurity measures.

The data illustrates a range of engagement levels with proactive security measures. Notably, none of the measures listed achieve a mean score above the midpoint of 3.0, except for F2, "I regularly update my awareness and knowledge about cyber threats targeting e-commerce platforms," which has a mean score of 3.09. This suggests a relatively higher engagement in staying informed about cyber threats than in other proactive behaviours, though not significant.

The lowest mean score is observed for F1, "I check my browsers' privacy control and security settings regularly," with a mean of 2.66. This indicates that checking browser settings is not a regularly practiced behaviour among the respondents, suggesting a potential area for improvement in personal cybersecurity practices.

Other practices such as regularly changing passwords (F3) and verifying links before clicking (F4) also have mean scores below 3.0, indicating that these recommended cybersecurity practices are not consistently adopted by the survey participants.

The relatively low mean score for F1 highlights a notable gap in cybersecurity practices, given the critical importance of browser security settings in protecting against various online threats. Regularly checking and adjusting these settings is a fundamental aspect of safeguarding personal information and ensuring secure online transactions. The underutilization of this measure suggests a need for increased awareness and education on the importance of browser settings as a frontline defence in cybersecurity.

Similarly, the practices of regularly changing passwords and verifying links before clicking, represented by F3 and F4 respectively, are essential components of a robust cybersecurity posture. The lukewarm engagement with these measures underscores a broader challenge in promoting consistent adherence to cybersecurity best practices among the public.

The analysis of Section F reveals a critical insight into the proactive security measures taken by individuals, highlighting a general trend of insufficient engagement with recommended cybersecurity practices. This finding underscores the need for heightened awareness and education efforts aimed at encouraging more rigorous and consistent adoption of proactive cybersecurity measures, especially in the realm of e-commerce. Given the increasing sophistication of cyber threats, fostering a culture of proactive cybersecurity behaviour is paramount. Drawing on the Theory of Planned Behaviour (Ajzen, 1991), which suggests that intention is influenced by attitudes, subjective norms, and perceived behavioural control, targeted interventions can be designed to modify these factors positively. Enhancing individuals' attitudes towards cybersecurity, increasing social pressure to engage in secure online behaviours, and improving perceived control over cybersecurity practices through education and resources are vital steps toward mitigating cyber threats and enhancing online safety.

4.5.5 *Adherence to security advice*

This section delves into the self-reported responses of the participants on their willingness to adhere to safe and secure online practices whilst transacting om e-commerce platforms. Due to the evolving nature of cyberthreats, the ability of e-commerce users to follow recommended safe online practices is pivotal in keeping them safe. Responses to questions like following the e-commerce platforms security policies, following advice received in the media provide useful insights into the cybersecurity behaviour of the participants.

Table 12: Scoring patterns (adherence to security advice)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
G1	Following advise received through the public media like newspapers, television, internet, and radio will prevent me from being a cybercrime victim when shopping online	316	3.83	0.82	4.00	3.00	4.00	5.00	1.00	< 0.001
G2	Complying with the information security policies of e-commerce platforms will help to keep me safe from cybercriminals	316	3.86	0.84	4.00	3.00	4.00	5.00	1.00	< 0.001
G3	Regular password changes to my e-commerce accounts will help to protect me from cybercriminals	316	4.15	0.76	4.00	4.00	5.00	5.00	2.00	< 0.001

The collected data explains the participants' perceptions regarding the effectiveness of adhering to security advice in mitigating cybercrime risks:

The mean scores for all statements in this section are above the midpoint of 3.0, indicating a strong belief among the respondents in the value of following security advice. Specifically, G3, "Regular password changes to my e-commerce accounts will help to protect me from cybercriminals," has the highest mean score of 4.15, suggesting a particularly strong consensus on the importance of regular password updates as a cybersecurity measure.

Both G1, regarding advice received through public media, and G2, regarding compliance with e-commerce platforms' security policies, have mean scores above 3.8 (3.83 and 3.86 respectively). This reflects a high level of trust in the security recommendations provided by both public media and the security policies of e-commerce platforms.

The relatively low standard deviations (below 1.0 for all statements) indicate a consistent belief among respondents in the efficacy of these security practices. This consistency suggests a widespread acknowledgment of the role that adherence to security advice plays in safeguarding against cyber threats.

The strong belief in the effectiveness of regular password changes (G3) is well-supported by cybersecurity research, which consistently highlights the importance of password management as a critical component of online security (Buil-Gil et al., 2021). Regularly updating passwords is a key deterrent against brute-force attacks, credential stuffing, and other password-related breaches (Kennison et al., 2021).

Furthermore, the high level of trust in security advice from public media (G1) and compliance with e-commerce platforms' policies (G2) underscores an important aspect of cybersecurity culture: the reliance on authoritative and expert sources for guidance in navigating the complex landscape of online threats. This trust reflects an awareness of the dynamic nature of cyber threats and the necessity of staying informed through reliable channels.

The findings highlight a strong belief among survey participants in the protective value of adhering to security advice, whether it comes from public media, e-commerce platforms, or best practices such as regular password changes. This trust in authoritative advice is crucial for fostering a culture of cybersecurity awareness and proactive behaviour (Bahl et al., 2021; D'adamo et al., 2021). However, it also underscores the responsibility of these sources to provide accurate, relevant, and timely information to the public. The high levels of adherence and trust suggest that targeted, clear, and actionable security advice can significantly impact individuals' cybersecurity practices and their ability to protect themselves from cyber threats (Daengsi et al., 2022). Incorporating insights from behavioural theories, such as the Health Belief Model could further enhance the effectiveness of cybersecurity advice by tailoring messages to address individuals' perceived threats, benefits, barriers, and cues to action, thereby promoting more secure online behaviours (Koloseni et al., 2019).

4.5.6 *Engagement with cybersecurity information*

This section pertains to understanding how the study participants source their cybersecurity information and their motivations to actively look for recommended safe online behaviour. The findings focus primarily on how the participants engage with various communication platforms, sharing with cybersecurity information with friends and family.

Table 13: Scoring patterns (engagement with cybersecurity information)

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
H1	Social media platforms constantly remind me on the latest safe cybersecurity practices	316	3.12	1.18	3.00	2.00	4.00	5.00	1.00	0.129
H2	I get reminders and notifications from the e-commerce platforms to regularly change my log in password	316	2.78	1.09	3.00	2.00	4.00	5.00	1.00	< 0.001
H3	My friends, family or work colleagues sometimes share cybersecurity information with me	316	3.40	1.14	4.00	3.00	4.00	5.00	1.00	0.028
H4	Public articles about cybercrimes and security breaches in the e-commerce sector motivate me to adopt safer online behaviour	316	3.72	0.89	4.00	3.00	4.00	5.00	1.00	< 0.001
H5	I constantly come across cybersecurity information (awareness campaigns) through the media like newspapers, television, internet, billboards and radio	316	3.21	1.18	3.00	2.00	4.00	5.00	1.00	0.694

The analysis of the responses from Section H offers insights into the participants' exposure to and interaction with cybersecurity information.

The data indicates a moderate level of engagement with cybersecurity information across various channels. Notably, H4, "Public articles about cybercrimes and security breaches in the e-commerce sector motivate me to adopt safer online behaviour," has the highest mean score of 3.72, suggesting that exposure to information on cybercrimes and security breaches significantly influences participants' cybersecurity behaviours.

There is variability in the effectiveness and frequency of cybersecurity information sources. While social media platforms (H1) and media like newspapers and television (H5) are noted as sources of cybersecurity information, with mean scores of 3.12 and 3.21 respectively, the impact and frequency of these reminders appear to be less consistent compared to the influence of public articles on cybercrimes (H4).

The mean score of 3.40 for H3, "My friends, family or work colleagues sometimes share cybersecurity information with me," highlights the role of personal networks as a significant channel through which cybersecurity information is disseminated and discussed.

The relatively high impact of public articles about cybercrimes (H4) on motivating safer online behaviour underscores the importance of public awareness campaigns and reporting on cybersecurity issues. This finding aligns with the notion that heightened awareness of the consequences of cyber threats can motivate individuals to adopt better security practices, a principle supported by the Protection Motivation Theory (Rogers, 1983), which posits that awareness of a threat, coupled with the efficacy of recommended preventive behaviours, can motivate action.

Conversely, the lower mean score for H2, "I get reminders and notifications from the e-commerce platforms to regularly change my login password," suggests a potential gap in the proactive delivery of cybersecurity information and reminders from e-commerce platforms. Enhancing the frequency and visibility of such

reminders could be a critical step in encouraging better password management practices among users.

The findings from Section H highlight a moderate engagement with cybersecurity information among participants, influenced by various information sources, including public articles, social media, personal networks, and media campaigns. The data underscores the significant role that public reporting on cybercrimes and breaches, as well as personal networks, play in shaping cybersecurity behaviours. This suggests that a multifaceted approach to cybersecurity awareness, leveraging both mass media and personal communication channels, could enhance the overall cybersecurity posture of individuals. Implementing more aggressive and targeted cybersecurity information dissemination strategies, particularly by e-commerce platforms, could further reinforce safe online behaviours. This approach aligns with theories of behaviour change, suggesting that increased exposure to relevant information can influence individuals' risk perceptions and motivate proactive security behaviours, thereby contributing to a more secure online environment.

4.5.7 *Summarised dimension scores*

The table below is a summary of the overall mean dimension scores.

Table 14: Summarised dimension scores

		Count	Mean	Standard Deviation	Median	Percentile 25	Percentile 75	Maximum	Minimum	Binomial Test p-value (cut-off = 3.0)
H1	Social media platforms constantly remind me on the latest safe cybersecurity practices	316	3.12	1.18	3.00	2.00	4.00	5.00	1.00	0.129
H2	I get reminders and notifications from the e-commerce platforms to regularly change my log in password	316	2.78	1.09	3.00	2.00	4.00	5.00	1.00	< 0.001
H3	My friends, family or work colleagues sometimes share cybersecurity information with me	316	3.40	1.14	4.00	3.00	4.00	5.00	1.00	0.028
H4	Public articles about cybercrimes and security breaches in the e-commerce sector motivate me to adopt safer online behaviour	316	3.72	0.89	4.00	3.00	4.00	5.00	1.00	< 0.001
H5	I constantly come across cybersecurity information (awareness campaigns) through the media like newspapers, television, internet, billboards and radio	316	3.21	1.18	3.00	2.00	4.00	5.00	1.00	0.694

The dimension of adherence to security advice scores the highest mean of 3.95, indicating a strong belief among participants in the efficacy of following security advice. This dimension exhibits a relatively low standard deviation (0.64), suggesting a consistent agreement across respondents on the importance of adhering to recommended security practices.

Both the self-efficacy in cybersecurity and online risk awareness dimensions score moderately high means of 3.68 and 3.78, respectively. These scores reflect a good level of confidence among the respondents in being able to respond safely when faced with online security threats in their ability to manage cybersecurity threats and having an awareness of the risks associated with online activities.

The proactive security measures dimension scores the lowest mean of 2.86, indicating a gap in the regular adoption of proactive security behaviours. This lower score, coupled with a higher standard deviation (1.03), suggests variability in how participants engage with proactive cybersecurity practices.

Engagement with cybersecurity information has a mean score of 3.24, pointing to a moderate level of interaction with cybersecurity information through various channels. This suggests there is room for increasing the frequency and effectiveness of cybersecurity information dissemination to further engage the public.

The overall mean score across all dimensions is 3.59, with a binomial test p-value of < 0.001, indicating a statistically significant tendency towards positive cybersecurity attitudes and behaviours among the participants. However, the range of means from the lowest (2.86 for Proactive Security Measures) to the highest (3.95 for Adherence to Security Advice) highlights areas for improvement, especially in fostering more proactive security measures.

The summarised dimension scores provide valuable insights into the cybersecurity landscape as perceived by the survey participants. While there is a strong adherence to security advice and a moderate level of self-efficacy, risk awareness, and engagement with cybersecurity information, there is a notable need for improvement in proactive security measures. These findings underscore

the importance of targeted interventions to enhance the cybersecurity posture of individuals, such as increased education and awareness campaigns, more engaging and accessible cybersecurity information, and encouraging the adoption of proactive security behaviours. Addressing these areas can help to build a more resilient and informed online community, better equipped to navigate the complexities of cybersecurity threats.

4.6 Testing of hypotheses

This study focuses on the impact of the demographic factors (age, gender, and educational level) and its effect on the cybersecurity behaviour on South African e-commerce users, if any. As this was a newly developed construct, the overall mean score was considered as a fair reflective measure of the respondent scoring. The impact of the demographic factors was tested using the Independent Samples Kruskal Wallis test, for the first 3 hypotheses. The null hypothesis claims that there is no difference in the central measure across the different categories of the variables.

4.6.1 *Hypothesis 1*

There is a significant relationship between cybersecurity behaviour and age in South African e-commerce users.

Table 15: Overall score comparison (gender)

Null Hypothesis	Test	Sig.	Decision
The distribution of Overall is the same across categories of Age (Years)	Independent-Samples Kruskal-Wallis Test	0.037	Reject the null hypothesis

The p-value indicates that there is a significant difference between the ages relating to cybersecurity behaviour.

Table 16: Mean scores (age)

Age	18 - 20	21 - 25	26 - 30	31 - 35	36 - 40	41 - 45	46 - 50	51 - 55	56 - 60	> 60
Mean	3.12	3.59	3.68	3.77	3.78	3.73	3.54	3.43	3.49	3.17

The pairwise comparisons are shown below:

Table 17: Pairwise comparison (age)

Sample 1 - Sample 2	**Test Statistic**	**Sig.**
18 – 20 - > 60	-13,594	0,653
18 – 20 - 51 - 55	-51,808	0,060
18 – 20 - 56 - 60	-64,208	0,023
18 – 20 - 46 - 50	-67,776	0,007
18 – 20 - 21 - 25	-72,489	0,003
18 – 20 - 26 - 30	-83,213	<0.001
18 – 20 - 41 - 45	-96,870	<0.001
18 – 20 - 31 - 35	-102,043	<0.001
18 – 20 - 36 - 40	-107,489	<0.001
> 60 - 51 - 55	38,214	0,215
> 60 - 56 - 60	50,614	0,108
> 60 - 46 - 50	54,182	0,058
> 60 - 21 - 25	58,895	0,036
> 60 - 26 - 30	69,619	0,011
> 60 - 41 - 45	83,276	0,002
> 60 - 31 - 35	88,449	0,001
> 60 - 36 - 40	93,895	<0.001

51 - 55 - 56 - 60	-12,400	0,668
51 - 55 - 46 - 50	15,968	0,533
51 - 55 - 21 - 25	20,681	0,411
51 - 55 - 26 - 30	31,405	0,198
51 - 55 - 41 - 45	45,061	0,054
51 - 55 -31 - 35	50,234	0,042
51 - 55 - 36 - 40	55,681	0,027
56 – 60 - 46 - 50	3,568	0,893
56 – 60 - 21 - 25	8,281	0,750
56 – 60 - 26 - 30	19,005	0,451
56 – 60 - 41 - 45	32,662	0,178
56 – 60 - 31 - 35	37,835	0,138
56 – 60 - 36 - 40	43,281	0,096
46 – 50 - 21 - 25	4,713	0,833
46 – 50 - 26 - 30	15,437	0,471
46 – 50 - 41 - 45	29,093	0,151
46 – 50 - 31 - 35	34,266	0,115
46 – 50 - 36 - 40	39,713	0,075
21 – 25 - 26 - 30	-10,724	0,607
21 – 25 - 41 - 45	-24,381	0,216
21 – 25 - 31 - 35	-29,553	0,164
21 – 25 - 36 - 40	-35,000	0,108
26 – 30 - 41 - 45	-13,657	0,465
26 – 30 - 31 - 35	-18,830	0,353

26 – 30 - 36 - 40	-24,276	0,245
41 – 45 - 31 - 35	5,173	0,786
41 – 45 - 36 - 40	10,619	0,590
31 – 35 - 36 - 40	-5,447	0,798

4.6.2 *Hypothesis 2*

There is no significant difference in cybersecurity behaviour across gender disparities of e-commerce users in South Africa.

Table 18: Overall score comparison (gender)

Null Hypothesis	Test	Sig.	Decision
The distribution of Overall is the same across categories of Gender	Independent-Samples Kruskal-Wallis Test	< 0.001	Reject the null hypothesis

The p-value indicates that there is a significant difference between the genders relating to cybersecurity behaviour.

Table 19: Mean scores (gender)

Gender	Mean
Male	3.70
Female	3.53
Non-binary	3.40

The pairwise comparisons are shown below:

Table 20: Pairwise comparison (gender)

Sample 1 - Sample 2	Female-Male	Non-binary-Male	Non-binary-Female
Test Statistic	27,193	31,818	4,625
Sig.	0,010	0,625	0,943

4.6.3 *Hypothesis 3*

There is a significant relationship between cybersecurity behaviour and educational level in South African e-commerce users.

Table 21: Overall score comparison (educational level)

Null Hypothesis	Test	Sig.	Decision
The distribution of Overall is the same across categories of Highest education level	Independent-Samples Kruskal-Wallis Test	< 0.001	Reject the null hypothesis.

The p-value indicates that there is a significant difference between the educational level in relation to cybersecurity behaviour.

Table 22: Mean scores (educational level)

Educational Level	Mean
Pre-matric	2.73
High School (Matric)	3.34
Certificate	3.36
Diploma	3.48
Postgraduate Diploma	3.61
Bachelor's Degree	3.76
Honours Degree	3.78
Master's Degree	3.82

Doctorate Degree	3.90

The pairwise comparisons are shown below:

Table 23: Pairwise Comparison (educational level)

Sample 1-Sample 2	Test Statistic	Sig.
Pre-matric - High School (Matric)	-63,274	0,026
Pre-matric - Certificate	-66,498	0,024
Pre-matric - Diploma	-80,417	0,004
Pre-matric - Postgraduate Diploma	-97,357	0,005
Pre-matric - Bachelor's Degree	-128,135	<0.001
Pre-matric - Honours Degree	-133,558	<0.001
Pre-matric - Master's Degree	-138,879	<0.001
Pre-matric - Doctorate Degree	-155,810	<0.001
High School (Matric) - Certificate	-3,223	0,884
High School (Matric) - Diploma	-17,142	0,401
High School (Matric) - Postgraduate Diploma	-34,083	0,232
High School (Matric) - Bachelor's Degree	-64,861	<0.001
High School (Matric) - Honours Degree	-70,284	<0.001
High School (Matric) - Master's Degree	-75,604	<0.001
High School (Matric) - Doctorate Degree	-92,535	0,021
Certificate - Diploma	-13,919	0,519
Certificate - Postgraduate Diploma	-30,859	0,293
Certificate - Bachelor's Degree	-61,637	0,002
Certificate - Honours Degree	-67,060	0,001

Certificate - Master's Degree	-72,381	<0.001
Certificate - Doctorate Degree	-89,312	0,028
Diploma - Postgraduate Diploma	-16,940	0,547
Diploma - Bachelor's Degree	-47,718	0,008
Diploma - Honours Degree	-53,141	0,005
Diploma - Master's Degree	-58,462	0,002
Diploma - Doctorate Degree	-75,393	0,058
Postgraduate Diploma - Bachelor's Degree	-30,778	0,252
Postgraduate Diploma - Honours Degree	-36,201	0,186
Postgraduate Diploma - Master's Degree	-41,522	0,130
Postgraduate Diploma - Doctorate Degree	-58,452	0,189
Bachelor's Degree - Honours Degree	-5,423	0,748
Bachelor's Degree - Master's Degree	-10,744	0,524
Bachelor's Degree - Doctorate Degree	-27,674	0,477
Honours Degree - Master's Degree	-5,321	0,764
Honours Degree - Doctorate Degree	-22,252	0,571
Master's Degree -Doctorate Degree	-16,931	0,666

4.6.4 *Hypothesis 4*

The combined impact of age, gender, and educational level can significantly predict cybersecurity behaviour in South African users.

This hypothesis tested whether the combination of the 3 demographic factors (age, gender, and educational level) had any effect on cybersecurity behaviour. To test this hypothesis, a univariate general linear model was used with the

overall mean score as the dependent variable, and the interaction term as the independent variable.

Table 24: Multifactor analysis: overall score by age, gender, educational level

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
A1 * A2 * A3	51,632	111	0,465	2,123	<0.001

Dependent Variable: Overall

R Squared = 0,536 (Adjusted R Squared = 0,283)

A1 = Gender, A2 = Age (years), A3 = Educational level

The combination of the demographic factors did significantly affect cybersecurity behaviour.

4.6.5 *Conclusions*

The results from the detailed study on the cybersecurity behaviour of e-commerce users divulge that there is a significant relationship between the demographic indicators of age, gender, educational level, and the combination of these three demographic indicators. The null hypothesis was rejected in each of the four instances showing that there is a meaningful relationship in the cybersecurity of e-commerce users in South Africa in reference to age, gender, education level and combination of the three demographic indicators.

This chapter has presented the key findings from the conducted quantitative survey, highlighting the demographic profile of the respondents and their responses. These findings provide a detailed view of the data collected, providing a solid basis for further analysis. The next chapter will discuss these findings in detail, interpreting the results on the basis study's research objectives and the context of the theoretical frameworks discussed in the previous chapter.

CHAPTER 5. DISCUSSION OF RESULTS

5.1 Introduction

In this chapter, we delve into the findings as presented in the previous chapter for the study to examine the impact of demographic indicators of age, gender, and education level on the cybersecurity behaviour of e-commerce users in South Africa. This section seeks to shed light on the identified patterns and provide insights that may assist to shape policy, cybersecurity interventions and any other initiatives within the South African context. The chapter will extend further to discuss identified patterns or trends on the research objectives as they relate to the identified patterns and trends on age, gender, and educational level factors on the cybersecurity behaviour of individuals.

5.2 Inclusion criteria

The study included results from respondents that voluntarily agreed to take part in the survey. Also, only the respondents who indicated that they had used e-commerce platforms in South Africa before were considered for this study.

5.3 Overview of key findings

The examination of cybersecurity behaviour amongst the South African e-commerce users provided some patterns shaped by the age, gender, and educational level. Through the statistical analysis of the data collected from the survey, yielded significant statistical differences for age, gender, educational level with p-values of 0.037, 0.01 and 0.01 respectively.

5.4 Discussion of hypothesised relationships

5.4.1 *To investigate how varying age groups impact cybersecurity behaviour amongst South African e-commerce users.*

The research objective aimed to understand how different age groups impact the cybersecurity behaviour of South African e-commerce users. This objective was guided by a hypothesis proposing a significant relationship between age and cybersecurity behaviour, patterns related to age had a p-value of 0.037 indicating a significant relationship between age and cybersecurity behaviour. The statistical analysis supported this hypothesis:

H1: *There is a significant relationship between cybersecurity behaviour and age in South African e-commerce users.*

The study's findings on understanding the relationship between the age of South African e-commerce users and cybersecurity behaviour has divulged some new perspectives and detailed interplay of these variables in the context of South Africa e-commerce. The various mean scores for each of the age groups and the statistical analysis outcomes helps to further confirm the significance of the findings in relation to the previously understood perspectives.

The outcome of the study with a focus to the relationship between age and cybersecurity behaviour confirms the current understanding within some of the existing literature. Gillam and Foster (2020) found a significant relationship between age and cybersecurity behaviour with a p-value of 0.045. However, some of the differences to note was that the referenced study had exactly half of its participants over the age of 50 whilst this current study had about 17%.

Contrary to the findings of this present study, where the youngest age group had the lowest mean score of 3.12 representing the lowest level of cybersecurity behaviour among the respondents. In a study conducted in 2014, which might yield different results if it were to be conducted now, found that the younger age groups were more likely to exhibit responsible cybersecurity behaviour online (Miltgen & Peyrat-Guillard, 2014). Also presenting alternative findings to the

notion that younger users are less likely to engage in safer cybersecurity behaviour than the older users as they perceive online platforms as a risky place (Jiang et al., 2016). This study's cybersecurity behaviour mean score show variations across the age groups, the findings are not allowed with the view that younger users are exhibit higher levels of cybersecurity behaviour. The mean score showed variations with each group but did not show a linear decrease of cybersecurity level with the older age groups.

In zooming into the impact of age on cybersecurity behaviour, this study found that age alone might not be a determinant factor of cybersecurity behaviour as shown by the insignificant statistical differences across some of the age groups. These findings may help in contributing and challenging some of the existing understanding of the impact of age on cybersecurity behaviour especially with a South Africa and e-commerce context.

5.4.2 *To investigate how gender influences the cybersecurity behaviour of South African e-commerce users*

The research objective aimed to understand how gender disparities impact the cybersecurity behaviour of South African e-commerce users. The research focused on the male, female and non-binary genders. Conducting a statistical analysis shed light on this relationship with the findings showing that the stated hypothesis was not supported with no significant difference between male and female e-commerce users. The non-binary group comprised a limited representation (0.6%) of the study participants but still showed cybersecurity behaviour consistent with the male and female participants thereby reaffirming that the initial hypothesis was not supported.

H2: *There is no significant difference in cybersecurity behaviour across gender disparities of e-commerce users in South Africa.*

The findings of this study are consistent with earlier studies to understand the cybersecurity behaviour of online users when using smartphones. Statistically significant differences were found between males and females in India when it comes to cybersecurity behaviour with males showing higher levels of

cybersecurity behaviour than females (Shah & Agarwal, 2020). This study found that cybersecurity behaviour of males was higher with mean scores of 3.70 in contrast to women's 3.53 with non-binary individuals scoring 3.40. With a p-value of 0.943 (non-binary and females) and 0.625 (non-binary and males) showing no significant difference between the genders but there exists significant difference between males and females (p-value of 0.010). Women are more likely to be vulnerable to online cyberattacks than males confirming the findings of this study (Gillam & Foster, 2020). A study in the US found significant differences in safe cybersecurity behaviour between males and females (Anwar et al., 2017). Further cementing the understanding of the current literature, females are exhibited lower cybersecurity behaviour than males in another US based study (Goel et al., 2017). When it comes to elements of what constitutes safe cybersecurity behaviour like not using basic and common passwords, in a study at a public university gender was found to be a predictor of cybersecurity behaviour. The study found that man practiced safer cybersecurity behaviours than women (Gratian et al., 2018).

On the flipside, in a study conducted in the health sector, females exhibited safer cybersecurity behaviours compared to their male counterparts (Rowan & Dehlinger, 2014).In a later study conducted by Daengsi et al. (2022) on the cybersecurity practices of Thai employees of a financial institution in response to cyberthreats, the female employees exhibited better levels of cybersecurity behaviour than males. The study attributed this to possible cultural practices in Thailand where women are naturally more cautious and risk averse, pointing out that studies in other countries could potentially result in different findings.

The findings highlight the need to consider gender differences among South African e-commerce users when implementing cybersecurity interventions. Females tend to show unsafe cybersecurity behaviour in relative to the male counterparts when utilising e-commerce platforms and targeted interventions are essential in South Africa.

5.4.3 *To investigate how the cybersecurity behaviour of South African e-commerce users varies based on their educational level*

The research objective aimed to understand how the education levels of South African e-commerce users impacted their cybersecurity behaviour. The study included a range of qualifications from pre-matric to doctorate degrees covering the formal qualifications available in South Africa. Interestingly, the results showed a consistent upward trend on the mean scores of 2.73 for pre-matric with those having doctorate degree scoring the highest mean score of 3.90. With p-values of 0.001, confirming the validity of the findings and cementing the relationship that exist between cybersecurity behaviour and educational level. The analysis of the study confirms the stated hypothesis below emphasising the important role that access to educational opportunities could help to enhance recommended cybersecurity behaviour.

H2: *There is a significant relationship between cybersecurity behaviour and educational level in South African e-commerce users.*

This study confirmed the existing literature that education level influences the cybersecurity behaviour of individuals. This finding documented in other geographic locations and different contexts also holds true for e-commerce users in South Africa. The mean scores showed a linear progressive pattern of increasing cybersecurity levels from the lowest education level to the highest education level.

In a recent study of university students and employed graduates across 2 cities in China, found that users with a higher education level (graduates) were had a better cybersecurity behaviour level than final year students with first to third year students had the lowest (Hong et al., 2023). The educational level of individuals has a significant impact on the ability of an individual to conduct safe cybersecurity practice (Chua et al., 2018). Education level of individuals was positively correlated to the cybersecurity behaviour of individuals based on study conducted in the US of users who have not finished high school to those who have graduated from college (Aivazpour & Rao, 2020). In the same vein, Goel et

al. (2017)pointed out that more educated individuals are less likely to be vulnerable to online cyberattacks like phishing.

These findings help to add to the existing body of knowledge by confirming that the educational level of individuals is pivotal in how they conduct themselves on e-commerce platforms in South Africa. This further prompts for more targeted cybersecurity interventions for those who are less educated as they tend to be more vulnerable when using e-commerce platforms.

5.4.4 *To investigate how the combined impact of age, gender and educational level serves as a predictor of cybersecurity behaviour among South African e-commerce users*

The research objective aimed to examine how the interaction of the demographic indicators of age, gender, and educational level combined would predict the cybersecurity behaviour of South African e-commerce users. Statistical analysis showed an F-statistic of 2.123 with a p-value of <0.01 providing an indication that the interplay of the demographic indicators holds statistical significance in predicting the cybersecurity behaviour of e-commerce users in South Africa. mean scores of 2.73 for pre-matric with those having doctorate degree scoring the highest mean score of 3.90. With p-values of 0.001, confirming the validity of the findings and cementing the relationship that exist between cybersecurity behaviour and educational level. The findings strongly support the stated hypothesis below indicating that the combined impact of age, gender and educational level serves as a significant predictor of cybersecurity behaviour among South African e-commerce users.

H3: *The combined impact of age, gender, and educational level can significantly predict cybersecurity behaviour in South African users.*

The results show an R squared value of 0.536 which indicates that the combined factors of age, genders and educational level represent about 54% of the variability in the cybersecurity behaviour of e-commerce users in South Africa.

The current literature has often emphasised the need to understand various factors to get a better understanding of the behaviour of individuals (Hong et al., 2023). The findings based on the univariate general linear model showed that a combination of age, gender and the highest education level was significant predictor of the individuals cybersecurity behaviour. Fatokun et al. (2019) based on a study done in Malaysia pointed out that all the three demographic indicators of age, gender and education level were important to consider when predicting the cybersecurity behaviour of individuals.

Our results further emphasise the fact that understanding the combined interplay of all the combined demographic indicators is pivotal in understanding and coming up with relevant interventions in respect to South African e-commerce.

In conclusion, this chapter has discussed the study's findings in relation to the research objectives and stated hypotheses, providing an in-depth understanding of the observed patterns in cybersecurity behaviour among South African e-commerce users. By linking the empirical results to the theoretical framework and existing literature, the discussion has highlighted the study's contributions to the field. The final chapter will now conclude the study by summarising the findings as they pertain to the research objectives, discussing their implications, and offering recommendations for future research and practical applications.

CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter aims to provide conclusion for this study by revisiting the objectives of the research into examining the cybersecurity behaviour of individual users in the contexts of e-commerce platforms in South Africa. The purpose of the study was to understand the dynamic interplay of demographic indicators (age, gender, and educational level) influencing user actions and responses when utilising e-commerce. The key conclusion derived from the study will be outlined in this section with key insights of the study also articulated clearly. Also, offer practical interventions to help in improving the cybersecurity behaviour of South African e-commerce users the theoretical results and findings will be used to provide actionable recommendations.

6.2 Deductions

In total, a total of 382 responses were received for the survey, incomplete responses and those that did not meet the study criteria were excluded leaving 316 to be analysed. Females made up most of the respondents with 62%, males contributed 37.3% and non-binary respondents contributed a relatively low proportion of 0.6%. Among the female respondents, the most common age group was 36-40 years making up 5.7% of the sample whilst the 26 -30 age group contributed 9.5% to the sample with the highest proportion. Non-binary respondents were present only in 1 age group of 21-25. Respondents with a bachelor's degree make up most of the sample with a proportion of 20.6%. On the other hand, respondents with doctorate degrees contributed 1.9% which was the lowest proportion. 83.6% of the respondents have attained a qualification beyond matric i.e. have more than a high school qualification. The demographic statistics provide the basis used to provide results and conclusions for examining the dynamics of this study.

After completing the exploration journey of the study, the findings allow for the deduction of important insights to help address the research objectives. The statistical analysis of the collected data rejected the null hypothesis of all the demographic variables of age, gender, educational level, and the combined impact of all three provides a perspective of the interplay of these variables with the cybersecurity online practices of users. The study concluded that age, gender, education level and their combination have a significant impact on the cybersecurity behaviour of e-commerce users in South Africa.

6.3 Conclusions regarding the hypothesis

6.3.1 *Conclusions regarding Hypothesis 1*

The first hypothesis pertained examining if there was a significant relationship between cybersecurity behaviour and age in the context of South African e-commerce users. The findings of the study provided some useful insights into understanding the impact of age in the cybersecurity behaviour of users. The results led to the rejection of the null hypothesis indicating that age is a significant factor in predicting the users' practices and responses to cybersecurity practices. This conclusion about the impact of age was signified by the Independent Samples Kruskal-Wallis test with a p-value of 0.037 which is less than 0.05 indicating that there is a significant difference across age groups in cybersecurity behaviour. By zooming more into the findings, the age group 41 – 45 exhibited the highest mean score which might be attributed to the possibility that in a South African context the users might have had more access to recommended cybersecurity practices through the workplace, internet based-sources and peers within their social circles. On the contrary, the 18-20 age group scored the lowest among the age groups which be related to their inexperience and the challenges to financially afford platforms like the internet, subscription based print and visual based media.

6.3.2 *Conclusions regarding Hypothesis 2*

The second hypothesis pertained to investigating if there is a significant relationship between cybersecurity and gender and valuable insights were derived based on the collected data and statistical analysis conducted. The results of the Independent Samples Kruskal-Wallis test showed that there is statistically significant difference between gender and the cybersecurity behaviour of South African e-commerce users. The p-value was 0.001 and thereby the null hypothesis was rejected.

Male respondents scored the highest mean scores on cybersecurity behaviour of 3.70 with females following closely behind with a mean score of 3.53 and lastly non-binary had 3.40 albeit them contributing a small sample of 0.6%. Based on the pairwise comparison analysis done between males and females ($p = 0.010$) indicates that males in the context of e-commerce in South Africa show a better engagement to cybersecurity behaviour than their female counterparts. Non-binary users showed no statistically significant differences in comparison to their male ($p = 0.625$) and females ($p = 0.943$) indicating that their cybersecurity behaviour is comparable to males and females.

The implication of these findings shows that gender should be considered when coming up with cybersecurity measures for South African e-commerce users. Females have a relatively lower mean score as compared to males and this could call for more gender targeted cybersecurity interventions, awareness campaigns and training. As for the non-binary users who have exhibited cybersecurity behaviour more closely aligned to both males and females, further investigation with more focus on this group might help to provide better trends and patterns impacting their cybersecurity practices.

This study provides further evidence that in South Africa, understanding and customising any initiatives to help in protecting the general populace from online cyberthreats requires gender focused interventions. As the e-commerce industry technology platforms continually evolve with so are the cyberthreats potentially targeting the e-commerce users, the relevant authorities need to provide more focus and bias to protect female users.

6.3.3 *Conclusions regarding Hypothesis 3*

The investigation into the impact of educational level on the cybersecurity behaviour of e-commerce users provided some compelling findings. The outcome of the statistical analysis of the collected data led to the rejection of the null hypothesis, indicating that there is statistically significant variance in the cybersecurity behaviour of South African e-commerce users based on their educational level. The resulting mean scores for each educational level attained by the users from pre-matric, matric, certificate, diploma, bachelor's degree, honours degree, postgraduate diploma, master's degree to doctorate degrees indicate the varying nature of South African e-commerce users.

On closer examination of the statistical findings a clear pattern emerges showing that in general e-commerce users who have a higher educational level tend to have a higher cybersecurity behaviour level. The highest mean scores were observed on the respondents who had attained a master's degree (3.82) and doctorate degree (3.90) showing a heightened awareness and cybersecurity level in relative to other users. On the other end of the spectrum, the e-commerce users who have not yet attained matric (2.73) and those with a high school matric (3.34) scored the lowest mean scores indicating a lower level of cybersecurity behaviour.

A pairwise comparison was done on the study further cementing the findings indicating that there is a significant difference between almost all the educational levels of the respondents. This result further emphasises the pivotal nature of educational achievement of users in predicting the cybersecurity behaviour of e-commerce users in South Africa.

In conclusion, the results of the study provide further evidence that there is a significant relationship between cybersecurity behaviour with the user's highest educational level attained. In a South African context, the relevant authorities would need to consider any cybersecurity related interventions with solutions that take into consideration the educational levels of the individuals.

6.3.4 *Conclusions regarding Hypothesis 4*

The study also investigated the combined impact of age, gender, and educational level on the cybersecurity behaviour of e-commerce users in South Africa. The statistical analysis of the collected data has yielded results providing a more detailed understanding of this complex dynamics of the collective demographic indicators and cybersecurity behaviour. The outcome of the study rejected the null hypothesis.

The evidence from the study shows that the demographic indicators of age, gender, and educational level together have an impact on the cybersecurity behaviour of users. This finding provides a different perspective to our understanding of the different factors affecting cybersecurity behaviour, showing that understanding the different demographic indicator's influence as isolated factors might not provide a complete picture of this relationship.

Conclusions regarding this hypothesis further emphasise that any practical interventions in South Africa within the e-commerce context requires that the relevant role players consider the demographic indicators jointly. A holistic view of the demographic indicators together will provide more effective and impactful interventions in enhancing the safe online practices on e-commerce platforms in South Africa.

6.4 Recommendations

The study has helped to shed light into various pivotal factors that have an impact on the cybersecurity behaviour in a specific geographical location of South Africa in the context of e-commerce platforms. As a result of this study various recommendations can be made to possibly help improve in the creation of relevant and effective interventions to assist in elevating the cybersecurity behaviour levels of users.

Customised and fit for purpose educational content and programmes may need to be developed with a specific focus on specific age groups. This means the educational programmes need to be adapted for each age group taking into

cognisance the different cybersecurity levels of each group. A possible collaboration with high schools, colleges, Technikons and universities driven by government departments and private players to include the educational curriculum with cybersecurity educational content.

Various campaigns targeted at the different genders tailored to each of the male, female and non-binary users. The various campaigns can be more effective if they address the specific concerns of the different gender groups. Utilising the various popular social media channels to target specific genders such as Facebook, Pinterest, Instagram, YouTube, X and Tumblr.

Practical educational interventions targeted at users based on their different educational levels. Collaborating with government institutions, private sector employers and the various institutions of learning is recommended as platforms to access users with cybersecurity awareness focused interventions. Also utilising social media platforms like LinkedIn can provide a more accessible and convenient way to introduce these interventions to professional audience. Simple and easy to understand user interfaces for conveying the message would likely enhance understanding among the users.

The findings from this study have practical implications for e-commerce platforms. Different user demographics, such as age and educational level, exhibit varied cybersecurity behaviours. E-commerce platforms can use these insights to develop tailored security measures, like targeted security reminders and personalised security settings. By enhancing user-specific security features, platforms can create a safer online environment and promote greater trust and engagement among users.

The study also offers valuable insights for cybersecurity professionals. The diverse cybersecurity behaviours across demographics suggest the need for targeted awareness campaigns. Professionals can design training programs that cater specifically to different user groups, focusing on fundamental or advanced cybersecurity practices based on the audience’s needs. Customised efforts can improve the effectiveness of educational programmes and contribute to a more secure experience for South Africa e-commerce users.

It is recommended that a multi-pronged approach between non-profit organisations, government and the private sector is paramount in developing relevant cybersecurity related policies to align with the best practice and global standards. This intervention may force the e-commerce platforms to enact relevant measures to prioritise the cybersecurity of their customers and enhance security on these platforms.

6.5 Limitations

Whilst this research has produced some valuable insights in the exploration of cybersecurity behaviour of e-commerce users in South Africa, however there are certain limitations that might influence how the results of this study can be interpreted and used to inform potential practical interventions.

This study was focused only on South African e-commerce users and due consideration must be applied if these results are to be extended to other countries. Also, the cybersecurity behaviour was analysed within the context of e-commerce users and any other platforms or context might yield different results.

The data collected in this study was based on self-reported data which might open the possibility of bias in the responses. This might be because of the participants responding based on what they perceive as the acceptable practice and not necessarily what they do.

Whilst this study focused on age, gender, and educational level as the demographic indicators to explore, these are not the only variables that could potentially impact the cybersecurity behaviour of e-commerce users. Income, technology related qualifications, employment status, race, country legislation and policies are some of the factors that were not investigated in this study.

6.6 Suggestions for further research

Valuable insights have been obtained from this study however there are several other potential opportunities that can be further investigated to provide and enhance the understanding of the complex dynamics of cybersecurity behaviour

of South African e-commerce users. This section aims to provide some indications for researchers to consider in plugging some of the gaps in the current literature.

A study on how the user experience and user interface design of e-commerce platforms impact the user's propensity to practice safe cybersecurity behaviour. A detailed investigation of this impact might help to shed more light on other factors that influence the cybersecurity behaviour of users on e-commerce platforms.

A cross-sectional research design was utilised for this study and potential valuable insights could be obtained if a longitudinal research design was employed. This would provide data collected over a longer period capturing the variability of the continuously evolving nature of cyberthreats, e-commerce trends and cultural norms.

Future research could expand upon this work by exploring additional demographic factors such as income level, digital literacy, employment status, and geographic location within South Africa. These factors may significantly impact cybersecurity behaviour and the ability to implement security measures. Also, investigating the role of cultural attitudes towards privacy and security, as well as the influence of social networks and peer groups on cybersecurity practices, could provide a more comprehensive understanding of the cybersecurity behaviour under investigation.

South Africa has a rich history of diverse cultures and religions (Xhosa, Zulu, Afrikaans, Tswana, Hindu, Muslim etc) within with its borders. Valuable insights might be obtained from understanding the common and different patterns that might shape the cybersecurity behaviour of e-commerce users.

Additionally, comparative analyses with other countries or regions could offer a broader perspective on global cybersecurity behaviour. Such studies could explore how differences in economic development, and regulatory environments affect users' cybersecurity practices in diverse contexts.

Non-binary users contributed just 0.6% to the sample used for this study. A detailed study focusing on non-binary e-commerce users to elicit their potential unique preferences and online practices in response to cyberthreats could help in understanding of this field further.

Future research could benefit from integrating or comparing alternative theories, such as the Theory of Planned Behaviour and the Technology Acceptance Model, to gain a more comprehensive understanding of cybersecurity behaviour. Additionally, exploring how contextual factors, like organizational culture or national policies, influence cybersecurity practices could provide insights beyond the individual focus of the PMT and HBM. Such research would assist in expanding the theoretical basis of the study.

To further leverage on these findings, several future research directions are proposed. Future studies could explore the role of digital literacy in cybersecurity behaviour, examining how technical knowledge affects users' ability to respond to threats. Research could also investigate how socio-economic status impacts access cybersecurity behaviour on e-commerce platforms. Cross-cultural studies could shed more light on how cultural practices influence online security behaviours.

By incorporating these additional factors and perspectives, future research could enhance the quality of findings and contribute to a more detailed and holistic view of cybersecurity behaviour across different populations and environments.

6.7 Conclusion

In conclusion, this study focused on understanding the impact of age, gender, and educational level on the cybersecurity behaviour of e-commerce users in South Africa. The results of the study for all three demographic indicators, the null hypothesis was rejected indicating the role each of these variables plays in the cybersecurity practices of users. Each of the demographic indicators provided some unique patterns and trends which in culmination presents a complex picture of understanding the cybersecurity behaviour of e-commerce users in South Africa. A combination of the three indicators also resulted in the null hypothesis

being rejected leading to a conclusion that understanding the influence of the combined indicators might help to provide a more detailed picture of this field.

This study provides some insights that may assist role players in the cybersecurity space, e-commerce industry, legislators, educators, and media players with input to help shape their respective interventions. The outcomes of this study could also help with a base that can be utilised by researchers to further explore this important field in our society. The dynamic and evolving nature of e-commerce platforms, social media trends, policies, social norms and cyberthreats altogether makes up a cocktail of variables that need to be continually monitored to provide a conducive environment that is safe for users to utilise the increasingly important e-commerce platforms.

In summary, this final chapter has highlighted the study's main findings, emphasized their impact on cybersecurity, and given practical recommendations for stakeholders. By bringing together the insights from the research, it provides a clear conclusion on the importance of understanding cybersecurity behaviour among South African e-commerce users. For more detailed information and additional analysis used in this study, readers can refer to the appendices after this chapter.

REFERENCES

Ahmad, S., Jha, S., Alam, A., Alharbi, M., & Nazeer, J. (2022). Analysis of Intrusion Detection Approaches for Network Traffic Anomalies with Comparative Analysis on Botnets (2008-2020). In *Security and Communication Networks* (Vol. 2022). https://doi.org/10.1155/2022/9199703

Aivazpour, Z., & Rao, V. S. (2020). Information disclosure and privacy paradox: The role of impulsivity. *Data Base for Advances in Information Systems*, *51*(1). https://doi.org/10.1145/3380799.3380803

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

Alhashem, M., Nabi, M. K., Pant, R., Inkesar, A., Khan, N., & Khan, M. A. (2023). Exploring the Factors Affecting Online Trust in B2C E-Commerce Transactions in India: an Empirical Study. *International Journal of Professional Business Review*, *8*(12), e03945. https://doi.org/10.26668/businessreview/2023.v8i12.3945

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052589

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behaviour*, *104*. https://doi.org/10.1016/j.chb.2019.106184

An, Q., Hong, W. C. H., Xu, X. S., Zhang, Y., & Kolletar-Zhu, K. (2023). How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, *22*(2), 305–317. https://doi.org/10.1007/s10207-022-00637-z

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3). https://doi.org/10.2307/25750694

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviours. *Computers in Human Behaviour*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Apau, R., & 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), 228–254. https://doi.org/10.5281/zenodo.3697886

Badotra, S., & Sundas, A. (2021). A systematic review on security of E-commerce systems. *International Journal of Applied Science and Engineering*, *18*(2), 1–19. https://doi.org/10.6703/IJASE.202106_18(2).010

Bahl, A., Sharma, A., & Asghar, M. R. (2021). Vulnerability disclosure and cybersecurity awareness campaigns on twitter during COVID -19. *SECURITY AND PRIVACY*, *4*(6). https://doi.org/10.1002/spy2.180

Balasudarsun, N. L., Sathish, M., Venkateswaran, P. S., Rameshwaran, B., Sonal, D., & Mohd, N. (2022). Predicting Consumers' Online Grocery Purchase Intention Within Middle-Class Families. *Webology*, *19*(1). https://doi.org/10.14704/web/v19i1/web19239

Bamberg, S., Masson, T., Brewitt, K., & Nemetschek, N. (2017). Threat, coping and flood prevention – A meta-analysis. *Journal of Environmental Psychology*, *54*, 116–126. https://doi.org/10.1016/j.jenvp.2017.08.001

Bartczak, K. (2021). Cybersecurity as the Main Challenge to the Effective Use of Digital Technology Platforms in E-Commerce. In *European Research Studies Journal: Vol. XXIV*.

Begum, M., Masud, M. M., Alam, L., Mokhtar, M. Bin, & Amir, A. A. (2022). The Adaptation Behaviour of Marine Fishermen towards Climate Change and

Food Security: An Application of the Theory of Planned Behaviour and Health Belief Model. *Sustainability (Switzerland)*, *14*(21). https://doi.org/10.3390/su142114001

Belli, L. (2021). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication*, *28*. https://doi.org/10.23962/10539/32208

Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers and Electrical Engineering*, *96*. https://doi.org/10.1016/j.compeleceng.2021.107546

Branch, L. E., Eller, W. S., Bias, T. K., Mccawley, M. A., Myers, D. J., Gerber, B. J., & Bassler, J. R. (2016). Trends in Malware Attacks against United States Healthcare Organizations. In *Global Biosecurity* (Vol. 1, Issue 1).

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims and Offenders*, *16*(3). https://doi.org/10.1080/15564886.2020.1814468

Cao, Y., Li, F., Zhang, Q., Yang, S., & Wang, Y. (2023). Towards Nonintrusive and Secure Mobile Two-Factor Authentication on Wearables. *IEEE Transactions on Mobile Computing*, *22*(5). https://doi.org/10.1109/TMC.2021.3133275

Carapeto, R., & Calil, A. L. (2022). Cybersecurity regulation in Brazil and Latin America: an overview. *International Cybersecurity Law Review*, *3*(2), 385–410. https://doi.org/10.1365/s43439-022-00055-w

Carico, R. R., Sheppard, J., & Thomas, C. B. (2021). Community pharmacists and communication in the time of COVID-19: Applying the health belief model. In *Research in Social and Administrative Pharmacy* (Vol. 17, Issue 1). https://doi.org/10.1016/j.sapharm.2020.03.017

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behaviour on social networking sites: The case of Facebook users. *European Journal of Information Systems*, *24*(1), 93–106. https://doi.org/10.1057/ejis.2013.31

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

Colley, A., & Maltby, J. (2008). Impact of the Internet on our lives: Male and female personal perspectives. *Computers in Human Behaviour*, *24*(5), 2005–2013. https://doi.org/10.1016/j.chb.2007.09.002

Coman, I. A., Xu, S., & Yamamoto, M. (2023). COVID-19 Vaccine Hesitancy: Disadvantaged Groups' Experience with Perceived Barriers, Cues to Action, and Attitudes. *American Journal of Health Promotion*, *37*(4), 488–498. https://doi.org/10.1177/08901171221136113

Conner, M., & Sparks, P. (2015). The theory of planned behaviour and the reasoned action approach. In *Predicting and changing health behaviour: Research and practice with social cognition models*.

Creswell, J. W., & Guetterman, T. c. (2020). *Educational Research planning, conducting, and evaluating quantitative and qualitative research sixth edition*.

D'adamo, I., González-Sánchez, R., Medina-Salgado, M. S., & Settembre-Blundo, D. (2021). Methodological perspective for assessing european consumers' awareness of cybersecurity and sustainability in e-commerce. *Sustainability (Switzerland)*, *13*(20). https://doi.org/10.3390/su132011343

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and

Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

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

De Wet, W., Koekemoer, E., & Nel, J. A. (2016). Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, *42*(1). https://doi.org/10.4102/sajip.v42i1.1330

Diniz, G., Muggah, R., & Glenny, M. (2014). *Deconstructing cyber security in brazil: Threats and Responses*.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behaviour: A health belief model approach. *Computers in Human Behaviour*, *68*. https://doi.org/10.1016/j.chb.2016.11.044

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviours: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers and Security*, *86*, 75–91. https://doi.org/10.1016/j.cose.2019.05.023

Dorce, L. C., da Silva, M. C., Mauad, J. R. C., de Faria Domingues, C. H., & Borges, J. A. R. (2021). Extending the theory of planned behaviour to understand consumer purchase behaviour for organic vegetables in Brazil: The role of perceived health benefits, perceived sustainability benefits and perceived price. *Food Quality and Preference*, *91*. https://doi.org/10.1016/j.foodqual.2021.104191

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). PUBLIC PERCEPTIONS OF CYBERSECURITY: A SOUTH AFRICAN CONTEXT. In *Southern African Journal of Criminology* (Vol. 31, Issue 3).

El Aassal, A., Baki, S., Das, A., & Verma, R. M. (2020). An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs. *IEEE Access*, *8*, 22170–22192. https://doi.org/10.1109/ACCESS.2020.2969780

Elrhim, M. A., & Elsayed, A. (2020). The Effect of COVID-19 Spread on the E-Commerce Market: The Case of the 5 Largest E-Commerce Companies in the World. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3621166

ENISA, & EGA. (2021). *RAISING AWARENESS OF CYBERSECURITY: A Key Element of National Cybersecurity Strategies*. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

Evanschitzky, H., Bartikowski, B., Baines, T., Blut, M., Brock, C., Kleinlercher, K., Naik, P., Petit, O., Rudolph, T., Spence, C., Velasco, C., & Wünderlich, N. V. (2020). Digital Disruption in Retailing and Beyond. *Journal of Service Management Research*, *4*(4), 187–204. https://doi.org/10.15358/2511-8676-2020-4-187

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviours of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1). https://doi.org/10.1088/1742-6596/1339/1/012098

Gcaza, N., & von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviours by U.S. workers: An exploratory study. *Computers in Human Behaviour*, *108*. https://doi.org/10.1016/j.chb.2020.106319

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1). https://doi.org/10.17705/1jais.00447

Gopinath, M., & Sethuraman, S. C. (2023). A comprehensive survey on deep learning based malware detection techniques. In *Computer Science Review* (Vol. 47). https://doi.org/10.1016/j.cosrev.2022.100529

Government Gazette. (2015). The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015. *Government Gazette*, *39475*.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Computers and Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Harerimana, A., & Mtshali, N. G. (2021). Using Mobile Technologies among Undergraduate Nursing Students for Academic Purposes in Tertiary Education: A Quantitative Survey. In *CIN - Computers Informatics Nursing* (Vol. 39, Issue 5). https://doi.org/10.1097/CIN.0000000000000694

Hofstee, E. (2018). Constructing a good dissertation. In *Constructing a Good Dissertation A Practical Guide to Finishing a Master's, MBA or PhD on Schedule*.

Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, *28*(1), 439–470. https://doi.org/10.1007/s10639-022-11121-5

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioural habits: Insights from situational support. *Journal of Information Security and Applications*, *57*. https://doi.org/10.1016/j.jisa.2020.102710

INTERPOL. (2021). *AFRICAN CYBERTHREAT ASSESSMENT REPORT 2021: INTERPOL'S KEY INSIGHT INTO CYBERCRIME IN AFRICA*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved

=2ahUKEwiQy-XVycaEAxWQbPEDHXFZBXgQFnoECBAQAQ&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F16759%2Ffile%2FAfricanCyberthreatAssessment_ENGLISH.pdf&usg=AOvVaw3wl6pEW7imKb0QSn5twzq6&opi=89978449

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers and Security*, *66*. https://doi.org/10.1016/j.cose.2017.01.010

Jewel Jean-Pierre, J., Academic Officer, C., Sue Subocz, P., & Jermaine Jewel Jean-Pierre, by. (2008). *BA*.

Jiang, M., Tsai, H. yi S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

Johnson, O., & Iyamu, T. (2019). Framework for the adoption of e-commerce: A case of South African retail grocery sector. *Electronic Journal of Information Systems in Developing Countries*, *85*(5). https://doi.org/10.1002/isd2.12095

Kartiwi, M., Hussin, H., Suhaimi, M. A., Mohamed Jalaldeen, M. R., & Amin, M. R. (2018). Impact of external factors on determining E-commerce benefits among SMEs in Malaysia. *Journal of Global Entrepreneurship Research*, *8*(1). https://doi.org/10.1186/s40497-018-0105-7

Kaufmann, L., Ninaus, M., Weiss, E. M., Gruber, W., & Wood, G. (2022). Self-efficacy matters: Influence of students' perceived self-efficacy on statistics anxiety. *Annals of the New York Academy of Sciences*, *1514*(1), 187–197. https://doi.org/10.1111/nyas.14797

Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behaviour Reports*, *4*. https://doi.org/10.1016/j.chbr.2021.100132

Keshri, A. K., Mishra, B. K., & Rukhaiyar, B. P. (2020). When rumors create chaos in e-commerce. *Chaos, Solitons and Fractals*, *131*. https://doi.org/10.1016/j.chaos.2019.109497

Kim, J., Yang, K., Min, J., & White, B. (2022). Hope, fear, and consumer behavioural change amid COVID-19: Application of protection motivation theory. *International Journal of Consumer Studies*, *46*(2), 558–574. https://doi.org/10.1111/ijcs.12700

Koloseni, D. N., Lee, C. Y., & Gan, M. L. (2019). Understanding information security behaviours of Tanzanian government employees: A health belief model perspective. *International Journal of Technology and Human Interaction*, *15*(1). https://doi.org/10.4018/IJTHI.2019010102

Kortjan, N., & Von Solms, R. (2014). *A conceptual framework for cyber-security awareness and education in SA*.

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behaviour. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Kumbhar, M., & Gavekar, V. (2017). A Study of Cyber Crime Awareness for Prevention and its Impact. *International Journal of Recent Trends in Engineering and Research*, *3*(10), 240–246. https://doi.org/10.23883/ijrter.2017.3480.jtu50

Lavrakas, P. (2012). Encyclopedia of Survey Research Methods. In *Encyclopedia of Survey Research Methods*. https://doi.org/10.4135/9781412963947

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behaviour*, *126*. https://doi.org/10.1016/j.chb.2021.106979

LexisNexis. (2020). *THE NEW CYBERCRIME LANDSCAPE: GLOBAL RISKS, REGIONAL TRENDS, INDUSTRY OPPORTUNITIES*.

Lim Ka Yong, nd, Majesty Yeap Xiao Li, rd, & Yeo Hui Qi, th. (2020). *Cyber Attacks in the Era of Covid-19 and Possible Solution Domains*. https://doi.org/10.20944/preprints202009.0630.v1

Makame, W. H., Kang, J., & Park, S. (2014). Factors influencing electronic commerce adoption in developing countries: The case of Tanzania. In *J.Bus.Manage* (Issue 2).

Maon, S. N., Hassan, N. M., Jailani, S. F. A. K., & Kassim, E. S. (2021). Gender Differences in Digital Competence Among Secondary School Students. *International Journal of Interactive Mobile Technologies*, *15*(4), 73–84. https://doi.org/10.3991/IJIM.V15I04.20197

Mashiane, T., & Kritzinger, E. (2019). Cybersecurity behaviour: A conceptual taxonomy. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11469 LNCS*, 147–156. https://doi.org/10.1007/978-3-030-20074-9_11

Mbatha, B., & Ngwenya, B. (2018). Obstacles to the adoption of e-commerce by tourism SME service providers in South Africa: the case of selected SMEs in Pretoria. *African Journal of Business and Economic Research*, *13*(3), 153–173. https://doi.org/10.31920/1750-4562/2018/v13n3a8

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). Insight into the cyberthreat landscape in South Africa. In *Accenture*.

McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. *Information and Computer Security*, *29*(5), 850–865. https://doi.org/10.1108/ICS-07-2020-0125

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries.

European Journal of Information Systems, *23*(2), 103–125. https://doi.org/10.1057/ejis.2013.17

Minnaar, A. (2014). 27 “CRACKERS”, CYBERATTACKS AND CYBERSECURITY VULNERABILITIES: THE DIFFICULTIES IN COMBATTING THE “NEW” CYBERCRIMINALS. In *Southern African Journal of Criminology Special Edition* (Issue 2).

Mıhcı Türker, P., & Kılıç Çakmak, E. (2019). An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents. *Computers in the Schools*, *36*(4), 293–318. https://doi.org/10.1080/07380569.2019.1677433

Molinillo, S., Aguilar-Illescas, R., Anaya-Sánchez, R., & Liébana-Cabanillas, F. (2021). Social commerce website design, perceived value and loyalty behaviour intentions: The moderating roles of gender, age and frequency of use. *Journal of Retailing and Consumer Services*, *63*. https://doi.org/10.1016/j.jretconser.2020.102404

Morrison, B. A., Coventry, L., & Briggs, P. (2020). Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.00623

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance & Cybersecurity*. https://doi.org/10.5171/2017.800299

Musakwa, I. S., & Petersen, F. (2023). *South African Journal of Information Management*. https://doi.org/10.4102/sajim

Ng, B. Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users’ computer security behaviour: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nganga, M. (2022). Concern over increase in cyber crime as SA ranked sixth worldwide for cybercrimes. *IOL*. https://www.iol.co.za/weekend-

argus/news/concern-over-increase-in-cyber-crime-as-sa-ranked-sixth-worldwide-for-cybercrimes-ac5b74e6-0736-484e-8c36-cb49ae809c02

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys*, *54*(11s). https://doi.org/10.1145/3514229

Paganin, G., Margheritti, S., Farhane-Medina, N. Z., Simbula, S., & Mazzetti, G. (2023). Health, Stress and Technologies: Integrating Technology Acceptance and Health Belief Models for Smartphone-Based Stress Intervention. *Healthcare (Switzerland)*, *11*(23). https://doi.org/10.3390/healthcare11233030

Peng, S. Y. (2023). Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions. *AJIL Unbound*, *117*, 122–127. https://doi.org/10.1017/aju.2023.18

Pickering, B., Boletsis, C., Halvorsrud, R., Phillips, S., & Surridge, M. (2021). It's Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12788 LNCS*, 337–352. https://doi.org/10.1007/978-3-030-77392-2_22

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*. https://doi.org/10.23962/10539/32213

Rahayu, R., & Day, J. (2015). Determinant Factors of E-commerce Adoption by SMEs in Developing Country: Evidence from Indonesia. *Procedia - Social and Behavioural Sciences*, *195*. https://doi.org/10.1016/j.sbspro.2015.06.423

Rathore, H., Mohamed, A., & Guizani, M. (2020). A survey of blockchain enabled cyber-physical systems. In *Sensors (Switzerland)* (Vol. 20, Issue 1). MDPI AG. https://doi.org/10.3390/s20010282

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications*, *56*. https://doi.org/10.1016/j.elerap.2022.101207

Roos, L., & Jordaan, A. (2006). *Access to information and communication: estimating the determinants of Internet usage in South Africa*.

Rosário, A., & Raimundo, R. (2021). Consumer marketing strategy and e-commerce in the last decade: A literature review. In *Journal of Theoretical and Applied Electronic Commerce Research* (Vol. 16, Issue 7, pp. 3003–3024). MDPI. https://doi.org/10.3390/jtaer16070164

Rowan, M., & Dehlinger, J. (2014). Observed gender differences in privacy concerns and behaviours of mobile device end users. *Procedia Computer Science*, *37*, 340–347. https://doi.org/10.1016/j.procs.2014.08.050

Safa, N. S., & Von Solms, R. (2016). Customers repurchase intention formation in e-commerce. *SA Journal of Information Management*, *18*(1). https://doi.org/10.4102/sajim.v18i1.712

Saunders, M., & Lewis, P. (2012). Doing Research in Business and Management CourseSmart eTextbook. *Ingentaconnect.Com*.

Schaefer, S., & Bulbulia, A. (2021). *Digital Commerce Acceleration Increased online purchases present new opportunities for digital commerce players*.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, *263*(4). https://doi.org/10.1088/1757-899X/263/4/042043

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information and Computer Security*, *28*(2), 293–318. https://doi.org/10.1108/ICS-04-2019-0041

Shenjere, F., & Middelberg, S. L. (2023). Analysing the impact of COVID-19 on the digital strategies of South African retailers. *Journal of Economic and Financial Sciences*, *16*(1). https://doi.org/10.4102/jef.v16i1.864

Silaule, C. B., Makhubele, L. M., & Mamorobela, S. P. (2022). A model to reduce insider cybersecurity threats in a South African telecommunications company. *SA Journal of Information Management*, *24*(1). https://doi.org/10.4102/sajim.v24i1.1573

Stitch. (2024). *Consumer_perspectives_South_Africa_e-commerce*. https://stitch.money/downloads/Consumer_perspectives_South_Africa_e-commerce.pdf

Tan, W. (2022). Research Methods: A Practical Guide For Students And Researchers: Second Edition. In *Research Methods: A Practical Guide For Students And Researchers: Second Edition*. https://doi.org/10.1142/10699

Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, *3*. https://doi.org/10.1016/j.promfg.2015.07.181

Thompson, N., & Brindley, J. (2020). Who are you talking about? Contrasting determinants of online disclosure about self or others. *Information Technology and People*, *34*(3), 999–1017. https://doi.org/10.1108/ITP-04-2019-0197

Tsai, F. J., Hu, Y. J., Chen, C. Y., Tseng, C. C., Yeh, G. L., & Cheng, J. F. (2021). Using the health belief model to explore nursing students' relationships between COVID-19 knowledge, health beliefs, cues to action, self-efficacy, and behavioural intention: A cross-sectional survey study. *Medicine (United States)*, *100*(11), E25210. https://doi.org/10.1097/MD.0000000000025210

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour.

Computers in Human Behaviour, *75*. https://doi.org/10.1016/j.chb.2017.05.038

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vaportzis, E., Clausen, M. G., & Gow, A. J. (2017). Older adults perceptions of technology and barriers to interacting with tablet computers: A focus group study. *Frontiers in Psychology*, *8*(OCT). https://doi.org/10.3389/fpsyg.2017.01687

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

Wilcox, H., & Bhattacharya, M. (2020). A human dimension of hacking: Social engineering through social media. *IOP Conference Series: Materials Science and Engineering*, *790*(1). https://doi.org/10.1088/1757-899X/790/1/012040

World Economic Forum. (2024). The Global Risks Report 2024 - 19th Edition. In *Energy Conversion and Management* (Vol. 52, Issue 2). https://www.weforum.org/publications/global-risks-report-2024/

Yoon, H. S., & Occeña, L. G. (2015). Influencing factors of trust in consumer-to-consumer electronic commerce with gender and age. *International Journal of Information Management*, *35*(3). https://doi.org/10.1016/j.ijinfomgt.2015.02.003

Yue, H. (2022). Research on E-Commerce Data Standard System in the Era of Digital Economy From the Perspective of Organizational Psychology. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.900698

Zhang, X., Han, X., Dang, Y., Meng, F., Guo, X., & Lin, J. (2017). User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance. *Informatics for*

Health and Social Care, *42*(2), 194–206. https://doi.org/10.1080/17538157.2016.1200053

Zhu, B., Kowatthanakul, S., & Satanasavapak, P. (2020). Generation Y consumer online repurchase intention in Bangkok: Based on Stimulus-Organism-Response (SOR) model. *International Journal of Retail and Distribution Management*, *48*(1), 53–69. https://doi.org/10.1108/IJRDM-04-2018-0071

APPENDIX A – Participant Information Letter

Dear Sir / Madam,

My name is Weston Mberikwazvo, and I am a Masters student in Digital Business at the University of the Witwatersrand, Johannesburg. As part of my studies, I must undertake a research project, and I am investigating the effect of demographic indicators on cybersecurity behaviour amongst e-commerce users in South Africa under the supervision of Dr Kiru Pillay. The aim of this research project is to find out if age, gender, and education level has an impact on cybersecurity behaviour of e-commerce platforms.

As part of this project, I would like to invite you to take part in this survey. This activity will take approximately 15 minutes to complete. Participating in the survey will be considered as consent for using the provided data.

There will be no personal costs to you if you participate in this project, you will not receive any direct benefits from participation but there are no disadvantages or penalties if you do not choose to participate or if you withdraw from the study. You may withdraw at any time or not answer any question if you do not want to. The questionnaire will be completely confidential and anonymous as I will not be asking for your name or any identifying information, and the information you give to me will be held securely and not disclosed to anyone else. I will be using a pseudonym (false name) to represent your participation in my final research report. If you experience any distress or discomfort at any point in this process, we will stop the interview or resume another time.

If you have any questions during or afterwards about this research, feel free to contact me on the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of this report, kindly provide your email at the end of the survey. If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za

Yours sincerely,

Weston Mberikwazvo

Researcher:

Weston Zorodzai Mberikwazvo, 1789533@students.wits.ac.za, +27 61 264 2961

Supervisor:

Dr. Kiru Pillay, kiru2010@gmail.com, +27 82 602 7261

APPENDIX B – Survey Instrument

By consenting to take part in the survey you agree to the following:

You are at least 18 years of age; Your participation in the study is voluntary; You are aware that you may terminate your participation in the study at any time for any reason.

- Yes, I consent
- No, I do not consent

6.1 Electronic Commerce (hereafter referred to as e-commerce) refers to the use of electronic devices such as computers, tablets, smartwatches, or smartphones connected to a network (mainly internet) to obtain information, buy, or sell product, services, data, or funds.

Common examples include but are not limited to the following:

- Takealot
- Facebook Marketplace
- Instagram
- Shein
- Shopify
- Gumtree
- Superbalist
- Zando
- makro.co.za
- game.co.za
- checkers.co.za
- bidorbuy.co.za
- woolworths.co.za
- Online Banking Websites

6.2 I have participated in e-commerce platforms by buying products or services in South Africa.

- Yes
- No

6.3 What is your gender?

- Female
- Male
- Non-binary / third gender

6.4 How old are you?

- 18 to 20 Years
- 21 to 25 Years

- 26 to 30 Years
- 31 to 35 Years
- 36 to 40 Years
- 41 to 45 Years
- 46 to 50 Years
- 51 to 55 Years
- 56 to 60 Years
- 61 Years and Above

6.5 What is your highest education level (obtained)?

- Pre-matric
- High School (Matric)
- Certificate
- Diploma
- Bachelor's Degree
- Honours Degree
- Postgraduate Diploma
- Master's Degree
- Doctorate Degree

6.6 How long have you been using e-commerce platforms?

- 1 to 2 years
- 3 to 4 years
- 5 to 6 years
- 7 to 8 years
- More than 10 years

6.7 On average, how many times do you make use of e-commerce platforms in a month?

- Once
- Twice
- Three times
- Four times
- More than five times

6.8 How many different e-commerce platforms have you used over the past two years?

- 1 to 5
- 6 to 10
- More than 10

6.9 I am likely to use e-commerce platforms in the future.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.10 I regularly change my password, PIN, pattern, or passcode on my smart devices.

- Strongly Disagree

- Disagree
- Neutral
- Agree
- Strongly Agree

6.11 I sometimes use public wi-fi hotspots when shopping online.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.12 When browsing e-commerce websites, I mouse over links to see where they go before clicking them.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.13 I regularly update my awareness and knowledge about cyberthreats targeting e-commerce platforms.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.14 I check my browsers (Chrome, Opera, Microsoft Edge, Safari etc.) privacy control and security settings regularly.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.15 There is a good possibility that my sensitive personal details (passwords, credit / debit card details, username, address etc.) could be stolen by unauthorised users.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.16 There is a good likelihood that I will receive a malicious attachment via email, WhatsApp, SMS, or social media.

- Strongly Disagree
- Disagree
- Neutral
- Agree

- Strongly Agree

6.17 Cybercriminals are likely to use my social media information to try and access my e-commerce accounts.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.18 I believe that my financial and personal information is at risk of being compromised when shopping online.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.19 I am concerned about the security of my accounts specifically on e-commerce platforms.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.20 Sharing my geographic location, children's names, date of birth, Identity numbers etc on public platforms can seriously compromise my security on e-commerce platforms.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.21 Using the same password on multiple e-commerce platforms increases my risk of potential harm resulting from cyberthreats leading to financial loss.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.22 Having my computer, smartphone, smartwatch, or tablet infected by a virus is a serious concern for me.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.23 I believe that using a public wi-fi to transact on e-commerce platforms significantly increases the risk of cybercriminals gaining unauthorised access to my personal information.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.24 The potential of someone misusing my personal data obtained from e-commerce sites is a major concern for me.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.25 Checking if the sender and subject of emails makes sense is effective in preventing me from being a victim of a cybercriminals.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.26 Not regularly updating my apps and software on my computer, tablet, smartwatch, smartphone can make me more vulnerable to cyber-attacks.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.27 Keeping abreast of the latest cybersecurity tips specifically related to e-commerce enhances my online shopping safety.

- Strongly Disagree
- Disagree

- Neutral
- Agree
- Strongly Agree

6.28 Using two-factor authentication on e-commerce platforms significantly increases my security when shopping online.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.29 Understanding e-commerce platform's privacy and security policies helps to ensure the security of my personal information.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.30 I constantly come across cybersecurity information (awareness campaigns) through the media like newspapers, television, internet, billboards, and radio.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.31 My friends, family or work colleagues sometimes share cybersecurity information with me.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.32 Social media platforms constantly remind me on the latest safe cybersecurity practices.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.33 I get reminders and notifications from the e-commerce platforms to regularly change my log in password.

- Strongly Disagree
- Disagree

- Neutral
- Agree
- Strongly Agree

6.34 Public articles about cybercrimes and security breaches in the e-commerce sector motivate me to adopt safer online behaviour.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.35 I am confident of recognising a fake e-commerce website address without help from anyone.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.36 I am confident of recognising a suspicious email without help from anyone.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.37 I am confident of recognising if my computer, tablet, smartwatch, or smartphone is infected by a malware such as a virus, worm etc.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.38 I am confident that I can configure and manage privacy settings on my social media platforms to control who can access my private information.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.39 I am confident of identifying and avoiding suspicious activities when doing online shopping.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.40 Following advise received through the public media like newspapers, television, internet, and radio will prevent me from being a cybercrime victim when shopping online.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.41 Complying with the information security policies of e-commerce platforms will help to keep me safe from cybercriminals.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.42 Regular password changes to my e-commerce accounts will help to protect me from cybercriminals.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.43 Using legal and updated software and applications for e-commerce activities helps to protect me from cybercriminals.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6.44 Using a reputable antivirus software can effectively protect me from cyber threats while engaging in e-commerce activities.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

APPENDIX C – Ethics Approval

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

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

Ethics Clearance Certificate

Ethics protocol number: WBS/DB1789533/128
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

This certificate is only valid if accompanied by formal permission from the relevant stakeholder(s).

Project title	The impact of demographic indicators on cybersecurity behaviour of e-commerce users in South Africa
Investigator / Researcher	Mr Weston Zorodzai Mberikwazvo
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.
Issue Date of Certificate	2022-12-20
	Text
Expiry date	Date of submission of the project / research report
Chairperson	Prof Anthony Stacey ☎ +27 11 717 3587 +27 82 880 4531 ✉ anthony.stacey@wits.ac.za

---

Declaration by Researcher

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

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

Signature

28 / 12 / 2022
Date: