USING PROTECTION MOTIVATION THEORY TO EVALUATE THE IMPACT OF CYBERSECURITY PRACTICES ON USER EXPERIENCE WITH E-COMMERCE PLATFORMS AMONG INTERNET CAFÉ USERS IN GQEBERHA

By

Segun Musa Obisesan

Student Number: 24O7469

Thesis submitted in fulfilment of the requirements for the award of the Degree of

Master of Commerce

In

Information Systems

Faculty of Commerce

Of

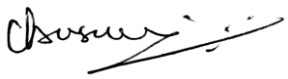
Rhodes University

Supervisor: Dr Moses Moyo

Date of Submission: September 2025

DECLARATION

I ***Segun Musa Obisesan*** hereby declare that this thesis titled: ***Using Protection Motivation Theory to Evaluate The Impact of Cybersecurity Practices on User Experience with E-Commerce Platforms Among Internet Café Users in Gqeberha*****,** submitted for the fulfilment of the degree of Master of Commerce in the Department of Information Systems at Rhodes University, has never been previously submitted to any other universities and it is my original work. The researcher is entirely aware of the plagiarism procedure of Rhodes University, and I have made required efforts to follow the established regulations. Also, all the cited and consulted sources have been duly acknowledged in the reference lists.



29 August 2025

_____ _____

Signature ***Date***

Segun Musa Obisesan

ABSTRACT

Online shopping has become deeply embedded in modern society, despite the growth of cybersecurity concerns linked with e-commerce platforms, particularly among users accessing public internet café through unsecured connections. Limited research has examined how cybersecurity practices affect e-commerce platform users' experiences in insecure public internet cafés. This study used the Protection Motivation Theory (PMT) to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha. The study population consists of e-commerce platform users mainly online shoppers from the internet cafés, with purposive sampling used to select three busy internet cafés located at the centre of Gqeberha city. The study utilised explanatory sequential mixed-methods, using probability sampling to administer 100 questionnaires and purposive sampling to select 7 participants for in-depth interviews for both quantative and qualitative phases. Quantitative data were analysed using Statistical Package for the Social Sciences version 29 with descriptive and inferential statistics, while qualitative data were thematically analysed using ATLAS.ti 25 following Braun and Clarke's six-phase.

The findings reveal high perceived severity and vulnerability regarding cybersecurity risks, such as phishing, smishing, and One-Time Password (OTP) attacks, which cause financial losses among e-commerce platform users in public internet cafés. Users' disregard for security practices led to negative experiences. E-commerce platform users with cybersecurity knowledge and shopping experiences demonstrated high self-efficacy and response efficacy in adopting cybersecurity practices, such as two-factor authentication, password managers, verification processes, and virtual card payment, to prevent fraud while shopping in internet cafés. Security measures' visibility on the e-commerce platforms improves user trust and self-efficacy. The study further concluded that a lack of cybersecurity knowledge led to low self-efficacy and response efficacy to follow security practices, making users vulnerable to online attacks and causing dissatisfaction. The study concluded that a lack of instructions and high perceived response costs, like inconvenience or time delay, were key challenges, affecting cybersecurity practices. The study recommended educating users on implementing security best practices such as using password managers, virtual cards and site verification. E-commerce platforms supported education is necessary to keep users

informed about security measures, and biometric verification should be implemented on e-commerce platforms**.** This study was restricted by the sample size for both qualitative and quantitative phases, and the sites where it was conducted in Gqeberha. Further studies could explore PMT constructs and cybersecurity practices across other cities of the Eastern Cape and other South African provinces, expanding the geographical coverage

KEYWORDS: user experience, e-commerce platform users, e-commerce platform, cybersecurity threats, cybersecurity practices, self-efficacy, response efficacy, response costs, perceived severity, perceived vulnerability.

POTENTIAL PUBLICATIONS

Publications produced from this thesis:

1. Obisesan S.M. & Dr Moyo M. (2024) Using the protection motivation theory to understand the impact of user cybersecurity practices on the utilisation of e-commerce platforms by online shoppers: A scoping review (Submitted to Southern African Business Review).

2. Obisesan S.M. & Dr Moyo M. (2025) Assessing cybersecurity practices among online shoppers using internet cafes in Gqeberha (submitted to Information Security for South Africa Conference).

ACKNOWLEDGEMENTS

First, I would like to express my gratitude to Almighty God for His mercy, love, and wisdom, which have invigorated me throughout this project and enabled me to complete my master's thesis successfully.

I want to especially thank my supervisor, Dr Moses Moyo, for his leadership, constant support, and expertise in guiding me throughout this journey. I genuinely appreciate his professionalism and supervisory input, which I have received and I owe the success of this thesis to his supervisory feedback and guidance.

I would also like to extend my gratitude to all the clients and users in the selected internet cafés who took the time to participate in completing the questionnaires and interviews.

I want to thank my loving parents, especially my mother, Mulikatu Obisesan. Your son will always make you proud of all the incalculable investment you have made in me. Furthermore, my covenant brother, Ayo, thank you for your financial support. And to all my siblings for your seasonal prayers. I appreciate those prayers so much.

LIST OF TABLES

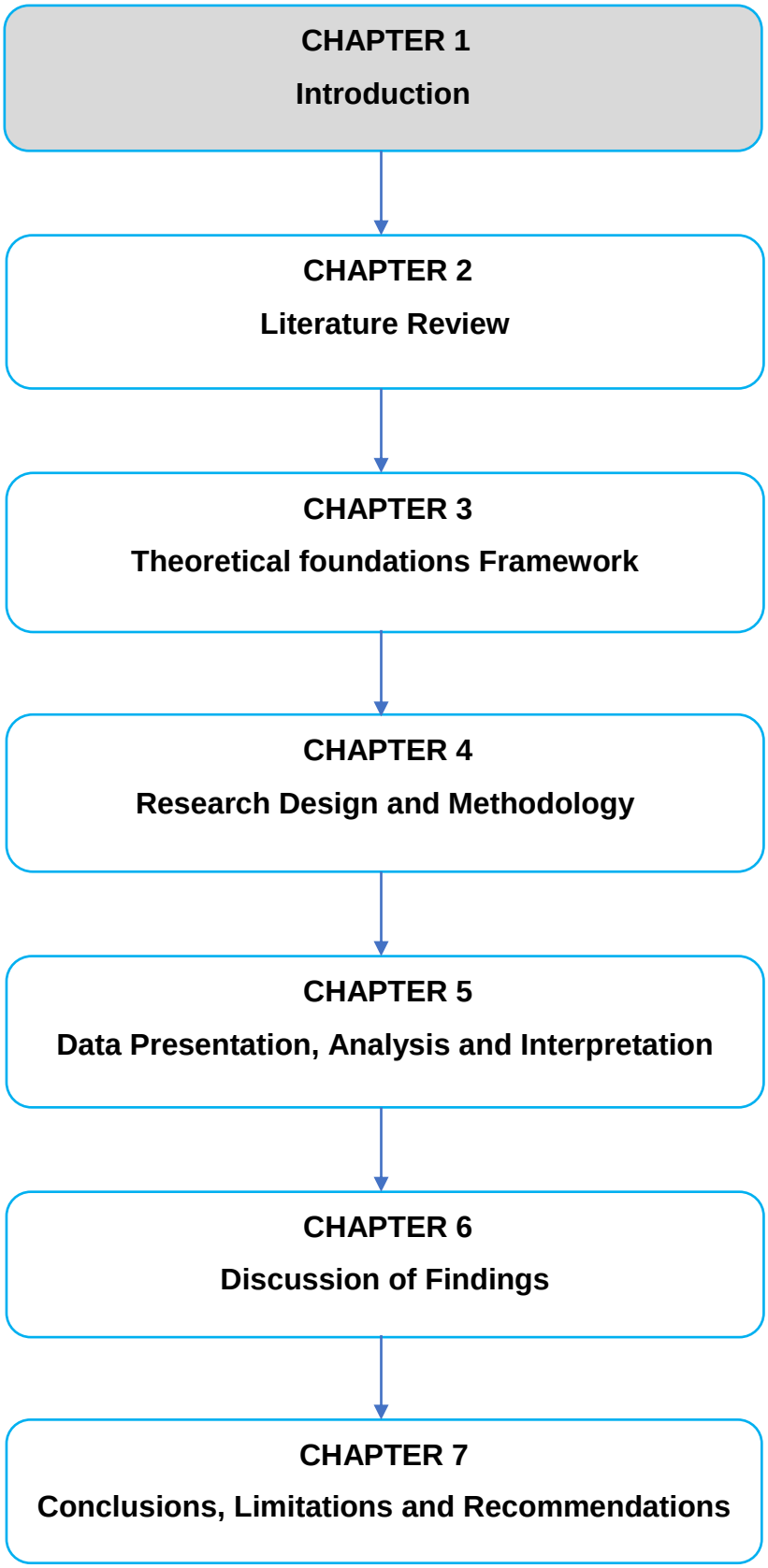
LIST OF FIGURES

LIST OF ACRONYMS USED

ACRONYM	MEANING
PMT	Protection Motivation Theory
ISO	International Organisation for Standardisation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
XSS	Cross-site Scripting
DDoS	Distributed Denial of Service
MITM	Man-in-the-middle
URL	Uniform Resource Locator
MFA	multifactor authentication
ITU	International Telecommunication Union
CIA	Confidentiality, Integrity and Availability
ROM	Research Onion Model
RTA	Reflexive Thematic Analysis
CMV	Common Method Variance
OTP	One-Time Password

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION



1.1. Background to the Problem

Electronic commerce (e-commerce) has become the cornerstone of the modern digital economy, as evidenced by its rapid expansion globally (Daramola & Etim, 2022; Jain et al., 2021). For instance, as of 2023, recent studies emphasise that e-commerce have doubled its volume to $ 4.2 billion (Paun et al., 2024). The global e-commerce markets such as Alibaba, Amazon and other platforms are expected to reach $4.89 trillion by 2027 in terms of money, and pricey. This continues to become major players in the adoption of online shopping platforms (Parvez, 2023; Paun et al., 2024). Similarly, in South Africans the growth of e-commerce is projected to increase from 11.7 million users in 2022 to 21.6 million by 2029, with 122,000 e-commerce platform users shopping online monthly on 142 e-commerce platforms such as Takealot.com, Amazon, Bidorbuy, Home-choice and other platforms (Cowling, 2024; Daramola & Etim, 2022; GoDigital Western Cape, 2023).

Literature reveals that e-commerce in South Africa has experienced a 300% rise since 2022, largely due to its accessibility to users who intend to shop from homes, workplaces and internet cafes (Henry, 2023; Ofori-Sasu et al., 2024)**.** However, online transactions in an unsecured public network are highly vulnerable to cybercriminal activities, posing significant risks to e-commerce platform users and leading to potential negative experiences (Al Shakosh, 2024; Prasad & Rohokale, 2020). E-commerce involves using the Internet, web-based platforms, and mobile applications to facilitate digital transactions between organisations and individuals (Laudon & Traver, 2020). Despite the benefits of e-commerce, users are often overshadowed by the reported cybersecurity breaches on these platforms (O'Shea, 2019; Wahab et al., 2023).

The digital landscape is evolving rapidly, making cybersecurity a key concern, especially in e-commerce, where user trust and security practices shape the overall user experience. Despite rising awareness efforts around cybersecurity threats, some e-commerce platform users, such as online shoppers, continue to conduct sensitive online transactions through insecure internet cafés (Aliyu, 2019; Munyendo et al., 2023; Ojo, 2021). This raises important questions about the behavioural and cognitive factors influencing risky online behaviour and shopping experiences. Cybersecurity

risks in e-commerce platforms significantly impact user experiences in unprotected public networks (Mafuya, 2022; Shakela & Jazri, 2019). Literature reveals various endless challenges from cybersecurity threats, such as social engineering and identity theft, which were experienced by users as a result of shopping online on e-commerce platforms in public internet cafés (Idayani et al., 2024; Liu et al., 2022; Ojo, 2021). According to Brederode (2023) more than 11.8% of e-commerce platform users shopping online on desktop computers reported an increase in online attacks such as account theft or financial risks in 2022, when creating new accounts for e-commerce transactions in the internet café environment (Brederode, 2023; Munyendo et al., 2023). According to Hotjar (2022), user experiences in e-commerce refer to the satisfaction users derive from interacting with an online shopping platform. User experiences encompass a person's perceptions and responses from the actual or anticipated use of a system or service during online transactions (Hinderks et al., 2022). Studies report that e-commerce platform users' experiences with e-commerce platforms influence their intentions either to complete online transactions or withdraw during the process, particularly on platforms susceptible to cyberattacks in an unprotected internet café setting (Al Shakosh, 2024; Ojo, 2021; Wahab et al., 2023).

Cybersecurity involves protecting cyberspace and its assets from threats that exploit vulnerabilities, leading to unauthorised access to sensitive data and financial loss or unintended experiences (Varachia, 2022; Von Solms & Von Solms, 2018). Cybersecurity awareness refers to e-commerce platform users' knowledge of online threats and adopting security practices to mitigate these risks, enabling safer online interactions in internet café settings (Al Shakosh, 2024; Spanning, 2022). Cybersecurity awareness leads to good cybersecurity practices. User cybersecurity practices refer to the actions and behaviours individuals adopt to protect themselves from cybersecurity threats, such as strong passwords, enabling two-factor authentication and avoiding suspicious links that help to prevent unauthorised access to their sensitive information and reduce online risks in a highly sensitive internet café environment (Ahmed, 2024; Cisco, 2024; Richard, 2023). However, 86% of e-commerce platform users, especially online shoppers in South Africa, are exposed to cyberattacks due to insufficient cybersecurity measures, especially among those with

low digital literacy who shop online in public internet cafés (Aliyu, 2019; Davison, 2023; Kshetri, 2019). While e-commerce platforms can enhance their platform's security, users' cybersecurity practices remain essential for the safe use during online transactions (Davison, 2023; Soava et al., 2022). Poor cybersecurity practices leave e-commerce platform users vulnerable to phishing and digital fraud, which are exploited by cybercriminals (Ncubukezit, 2022; Varma et al., 2023).

Moreover, in 2021, South Africa was ranked sixth globally in cybercrime, with an average of 97 victims per hour, many of whom were e-commerce platform users (Davison, 2023). Over 21.6 million users are at risk of cyberattacks, potentially costing more than R2 billion in two years (Cowling, 2024; News24, 2020). Online identity theft has surged by 337%, with users frequently targeted by phishing or malicious links (Adisa, 2023; Moonstone, 2024; Parker, 2020), often due to poor cybersecurity practices among e-commerce platform users (Davison, 2023; Varma et al., 2023). Moreover, literature shows that many e-commerce platform users lack fundamental cybersecurity knowledge, exposing them to common cyber threats on unprotected connections (Ojo, 2021; Strzelecki and Rizun, 2022). This can erode user trust and instil fear, negatively affecting their willingness and satisfaction to use e-commerce platforms for online shopping activities (Kakar et al., 2020; Mofokeng, 2021).

Literature stresses that e-commerce platform users' behaviours and lack of concerns about cybersecurity practices, such as repeated use of login credentials, contributed to the rising cyberattacks and incidents on e-commerce platforms in an unprotected public internet café environment (Liu et al., 2022; Makhitha & Ngobeni, 2024; Munyendo et al., 2023). Studies show that e-commerce platform users who feel immune to cyber threats often neglect security practices, making them easy targets for cyberattacks (Grobler et al., 2021; Lim, 2021; Sulaiman et al., 2022). Furthermore, e-commerce platforms face significant threats due to users' ignorance of online risks and the ever-evolving nature of cybercrimes (Khan, 2019; Liu et al., 2022). Victims of cyber incidents are less likely to return to platforms due to fears of data breaches or perceived threats on an unsecure connection (Hariharan et al., 2023). Also, cybersecurity issues such as fake websites and third-party vulnerabilities exacerbate distrust (Mitra et al., 2022; Subramani et al., 2022). However, users with cybersecurity

awareness are more likely to adopt safety security practices, increasing trust and engagement on e-commerce platforms in the internet café (Ahmad et al., 2023; Alontaga, 2018).

Studies reveal that the interplay between e-commerce platform users' awareness and technical measures can substantially influence their behaviour during online transactions on e-commerce platforms (Kelley, 2018; Liu et al., 2022; Moustafa et al., 2021). While technical measures such as encryption, SSL protocols, and multifactor authentication are designed to secure data, they require specialised knowledge, which many users are ignorant of (Mehraj et al., 2021; Newhouse et al., 2019). According to Munyendo et al. (2023), a lack of basic cybersecurity knowledge among e-commerce platform users about the technical protections put in place on the platforms is a cause for concern. The effectiveness of these technical defences largely depends on e-commerce platform users' understanding and behaviour in supporting technical measures (Moustafa et al., 2021). Sam et al. (2019) reported that 52% of users in the Eastern Cape, particularly in Gqeberha, lack the essential cybersecurity skills needed to protect their online transactions from identity theft and financial loss, thereby exposing themselves to cyber threats in an unsecured public environment (Semrush, 2024). Therefore, considering the diverse landscape of e-commerce platform users in Gqeberha, it is evident that a study examining e-commerce platform users' adoption of cybersecurity practices will provide valuable insight. Especially in the context of the Protection Motivation Theory (PMT) constructs, it can offer clear guidance and encourage secure behaviour, making cybersecurity practices more accessible for e-commerce platform users in the region.

1.2. Problem Statement

In the Eastern Cape, many users continue to rely on internet cafés for their online transactions, which raises significant concerns about cybersecurity risks such as phishing and identity theft (Moonstone, 2024; Nkadimeng, 2019). While mobile apps are generally more secure than website platforms, the extent to which users are aware of the vulnerabilities associated with public networks and their actual cybersecurity practices remains largely unclear (Khipu Networks, 2023; Munyendo et al., 2023).

Despite the growing number of e-commerce platform users, little research has explored how these cybersecurity habits affect users' overall shopping experiences (Aseri, 2021; Butler & Butler, 2019). This gap necessitates further investigation, particularly considering the growing dependence on e-commerce platforms and the ongoing cybersecurity threats. Therefore, this study aims to fill this gap by applying the PMT to assess the impact of cybersecurity practices on user experiences.

1.3. Goals of the Research

The main objective of this study is: To use the PMT to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha. Therefore, the sub-objectives of the study will be:

1. To determine cybersecurity threats that e-commerce platform users who use internet cafés for business transactions perceive as influencing their online shopping behaviour;
2. To examine how basic cybersecurity measures implemented in e-commerce platforms impact user satisfaction and overall shopping experiences in the internet café;
3. To determine how the perceptions of cybersecurity threats among e-commerce platform users who use internet cafés influence their perceived effectiveness of cybersecurity practices when conducting business transactions on e-commerce platforms; and
4. To recommend cybersecurity practices that e-commerce platform users can adopt to enhance their experiences while accessing e-commerce platforms in internet cafés.

1.4. Main Research Question

This main research question of the study is: *How can the Protection Motivation Theory (PMT) be employed to assess the effectiveness of cybersecurity practices and their impact on online shopping experiences with e-commerce platforms among internet café users in Gqeberha?*

1.4.1 Sub Questions

1. *What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?*

   This question aims to identify specific cybersecurity threats perceived by e-commerce platform users, especially online shoppers in internet cafés and examine how they influence their online shopping behaviour. This information can help the development of user-centred security measures on e-commerce platforms, tailored for users in shared or public internet café environments.

2. *How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?*

   This question investigates how fundamental cybersecurity measures, such as secure passwords, two-factor authentication and identifying suspicious links, affect user satisfaction and shopping experiences among e-commerce platform users in internet cafés. It seeks to determine whether these measures boost users' confidence and enjoyment while shopping online in public spaces. The findings could enhance knowledge of cybersecurity measures to promote positive experiences, especially in higher-risk environments like internet cafés.

3. *How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?*

   The purpose of this question is to explore the relationship between e-commerce platform users' perceptions of cybersecurity threats and their confidence in the effectiveness of cybersecurity practices while conducting online transactions in internet cafés. This could reveal potential gaps in user knowledge and practices that can inform strategies to enhance user education and promote more effective cybersecurity practices tailored for users in shared internet environments.

4. *What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping?*
   This question aims to identify specific cybersecurity practices that e-commerce platform users can implement while accessing e-commerce platforms in public environments, such as internet cafés, to improve their safety and overall shopping experiences. This understanding could empower e-commerce platform users' knowledge of cybersecurity practices that enhance their security habits. The insights gained will help inform e-commerce platform users on effective strategies to mitigate risks associated with online shopping in a shared internet café environment, ultimately fostering a more secure and satisfying shopping experience.

1.5. Delimitation of this Study

Several vital factors limit this study to remaining focused and managing its scope. It is geographically restricted to Gqeberha in the Eastern Cape, to ensure that the findings reflect the unique cybersecurity challenges and experiences specific to this area. The population of this study consists of e-commerce platform users, exclusively online shoppers using Internet cafes for their online transactions and shopping purposes. The study focuses specifically on online shoppers and does not deal with the vendors. Individuals unfamiliar with both online shopping and mobile e-commerce applications outside internet cafés are excluded. Furthermore, it focuses on assessing cybersecurity practices and their impact on e-commerce platform users' experiences rather than exploring from a technical or organisational security measures standpoint. It will not examine other factors, such as website usability or logistics, unless directly related to cybersecurity practices and the PMT.

1.6. Research Methodology

The study used a pragmatic philosophy and explanatory sequential mixed-methods research methodology, guided by the Research Onion Model (ROM) by Saunders et al. (2019). Data collection and analysis were planned, using an explanatory sequential design consisting of two phases: a quantitative phase and a qualitative phase. The

quantitative phase assessed the impact of cybersecurity practices on online shoppers' experiences, while the qualitative phase explored users' perceptions, experiences, and behaviours (Creswell, 2021, 2013; Creswell & Poth, 2016). Chapter 4 explains in detail the ethical concerns and research methodology for this study.

1.7. Population, Sample Dimension and Sampling techniques

This study population contains internet café users in Gqeberha, Eastern Cape, specifically targeting individuals aged 18 and above who have used e-commerce platforms for online shopping or related activities. The study used two samples: a probability sampling of 88-100 participants from three internet cafés namely Internet café A (North), Internet café B (Central) and Internet café C (North) from which quantitative data was collected for the quantitative phase (Taherdoost, 2016a), and a purposive sample of 4-10 participants from the initial group for in-depth interviews to gather qualitative data for the qualitative phase (Creswell, 2021; Palinkas et al., 2015). The study used a questionnaire for quantitative data collection and in-depth interviews for qualitative data collection. A detailed discussion of the population and sampling procedures is presented in Chapter 4.

1.8. Data Collection and Analysis Techniques

Quantitative data was gathered through a questionnaire with Likert scale questions administered in an internet café setting, and SPSS Version 29 was used to analyse quantitative data presented the results as descriptive and inferential statistics. Qualitative data was collected through semi-structured interviews with responses recorded and transcribed verbatim, then analysed thematically using ATLAS.ti 25, following Braun and Clarke's six-phase process (Braun and Clarke, 2022, 2019). Chapter 4 explains in details the data collection and analysis for this study.

1.9. Significance of the Study

This study addresses a critical gap in e-commerce research by examining how cybersecurity practices influence online shoppers’ experiences, explicitly focusing on e-commerce platform users in Gqeberha, Eastern Cape. With the rapid expansion of

e-commerce, many e-commerce platform users lack essential cybersecurity practices needed to protect themselves, engaging in risky behaviours such as weak password practices that heighten their vulnerability to cyber threats. Although studies acknowledged these challenges, they do not examine how adopting protective behaviours, such as self-efficacy and response efficacy, can improve cybersecurity practices and online shopping experiences on these platforms. By applying the PMT framework, this study assessed cybersecurity practices that e-commerce platform users perceive as most effective in safeguarding online transactions and enhancing their shopping experiences. This study has theoretical, methodological and business contributions.

1.10. Research Contribution

This study contributes to the academic literature by applying Protection Motivation Theory (PMT) to e-commerce platform users' experiences and cybersecurity practices, thereby bridging existing research gaps and laying the groundwork for future studies on cybersecurity practices, user experiences, user-centred research, and behavioural theories. It provides insights into how they perceive and respond to cybersecurity threats in the internet café environment, helping to recommend effective cybersecurity practices for e-commerce platform users. The findings of this study can help e-commerce platforms design more effective and user-friendly cybersecurity practices and gain a competitive edge. It offers valuable information for developing cybersecurity policies that enhance e-commerce platform users' experiences in a public-access internet café environment. The methodology provides a comprehensive framework that other researchers can adapt and apply in similar contexts, enhancing the rigour and depth of research in understanding e-commerce platform user experiences and cybersecurity practices.

1.11. Ethical Consideration

The researcher applied for ethical clearance from the University's Ethical Committee before collecting data. Participants were given informed consent after explaining the study's objectives, ensuring they can withdraw without coercion at any time, and that their data remains confidential. The researcher also obtained permission from internet café managers to engage their clients and present the consent letters for approval.

1.12. Terms and Defintions

TERMS	DEFINITIONS
Cybersecurity	Cybersecurity safeguards the interests and assets of individuals, societies, and nations from risks associated with the digital environment, including protecting those operating in cyberspace and their assets (Boban, 2024; Von Solms & Von Solms, 2018).
User cybersecurity practices	User cybersecurity practices refer to the actions and behaviours individuals adopt to protect themselves from cybersecurity threats to enhance their online security (Dodge et al., 2023; Herath et al., 2022; Matlala, 2023)
Cybersecurity Threats	Cybersecurity threats encompass a range of attacks on the e-commerce ecosystem, such as malware, client/server security threats, identity theft, phishing and other attacks on personal data (Andreianu, 2023; Kshetri, 2021; Liu et al., 2022; Mitra et al., 2022).
Cybercrime	Cybercrime is a criminal activity where computers or networks are the primary means for committing offences or violating laws, rules, or regulations (Kshetri, 2021)**.**
E-commerce	E-commerce refers to conducting business online using computing devices and communication platforms (Wahab et al., 2023).
Cybersecurity awareness	Cybersecurity awareness refers to an individual's knowledge, understanding and responsible action to prevent security incidents in the digital environment (Spanning, 2022; Verusboc, 2022).
User Experiences	User experience refers to a person's perceptions and responses resulting from the actual or anticipated use of a product, system, or service (Hinderks et al., 2022).
Cyberspace	Cyberspace is a realm of virtual environments where users store, share and create digital information while communicating online through physical infrastructure (Craigen et al., 2014; Kshetri, 2021).
E-commerce platforms	E-commerce platforms are digital systems that enable online buying and selling activities, offering tools for product listing, payment management, inventory tracking, and transaction processing through websites or apps such as Amazon, Takealot, eBay and others (Daramola & Etim, 2022)
E-commerce platform users	E-commerce platform users refer to online shoppers or individuals who engage in online shopping, transactions, and interactions on digital platforms. These users rely on internet-enabled devices or systems to access e-commerce sites or apps for convenience and variety of shopping (Khan, 2019; Laudon & Traver, 2020)

1.13. Thesis structure and Layout

This thesis will consist of seven chapters, as illustrated in Figure 1. Each chapter addresses a detailed area of this study and is briefly explained in the layout of the thesis.

Chapter 1	**Introduction**
	This chapter introduces the study and explains the research context. It further outlines the research problem, objectives, questions, delimitation and the significance of conducting this research.
Chapter 2	**Literature Review**
	This chapter examines existing literature on cybersecurity threats, common cybersecurity threats and cybersecurity practices. It examines user experiences and perceptions, as well as shopping behaviour in the context of e-commerce and Internet cafés, utilising both preliminary and secondary sources such as journals and books.
Chapter 3	**Theoretical Foundations Framework**
	The chapter explores protection motivation theory and its application in cybersecurity, user experiences, cybersecurity practices and e-commerce.
Chapter 4	**Research Design and Methodology**
	This chapter details the research methodology, including research design, strategy, population, sampling procedure, data collection method, and analysis.
Chapter 5	**Data Presentation, Analysis and Interpretation**
	This chapter presents the data analysis, the presentation of results and interpretations for this study. It begins with the quantitative results, followed by qualitative themes collected from the questionnaires and semi-structured interviews.
Chapter 6	**Discussion of Findings**
	This chapter discusses the findings for this research, explaining its relation to PMT constructs and comparing them to previous research.
Chapter 7	**Conclusions, Limitations and Recommendations**
	This chapter highlights the study's contributions and shortcomings, and concludes with recommendations for future researchers.

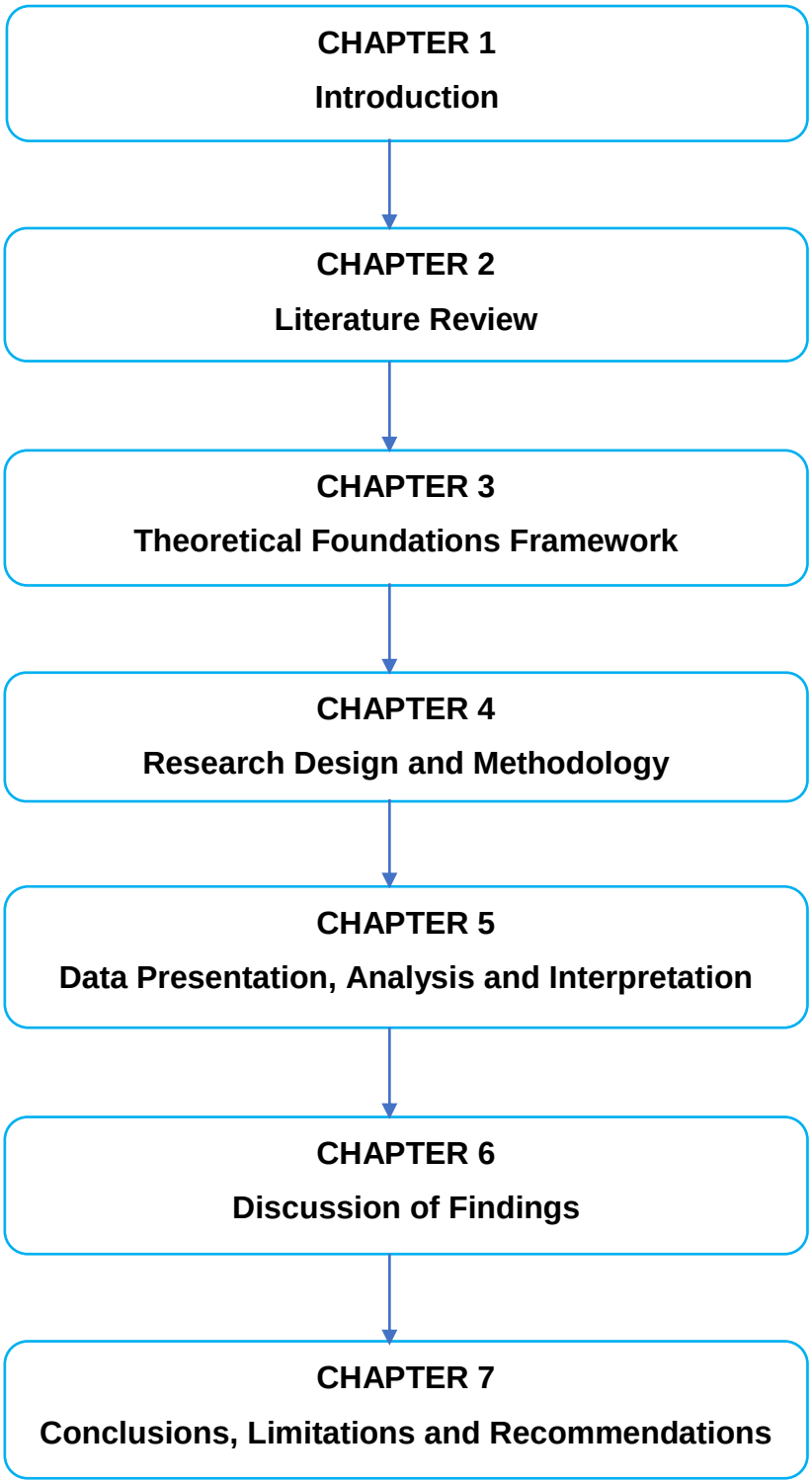


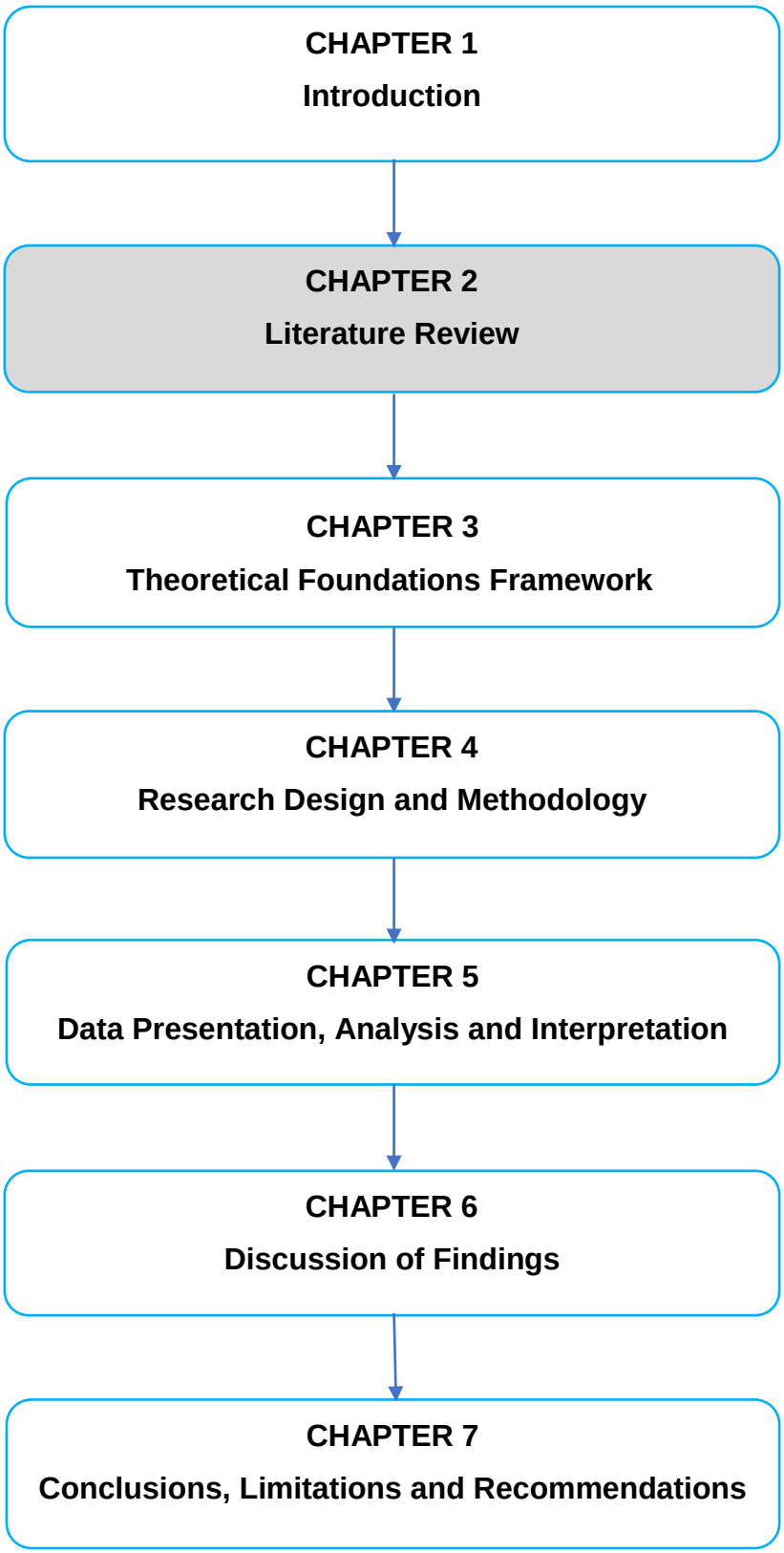
Figure 1.1: Thesis structure and layout

1.14. Synopsis for the Chapter

Many e-commerce platform users shop online from workplaces, residences, and internet cafes. At the same time, a more significant number of these users in the Eastern Cape lack the basic skills and awareness to safeguard their online transactions against cybersecurity threats such as identity theft and financial loss. Using public environments such as internet cafés for online transactions raises concerns regarding cybersecurity risks. The extent of user awareness of public network vulnerabilities, their cybersecurity practices and security habits affecting overall shopping experiences remains undetermined, highlighting a gap in cybersecurity practices as online fraud outpaces public awareness. Therefore, this study aims to utilise the PMT to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha, Eastern Cape.

This chapter delineated the research context and justified the importance of this study. The background problem was identified, highlighting the importance of cybersecurity practices for e-commerce platform users who rely on the public Internet for online shopping. A explanatory sequential mixed-method research design was employed using quantitative and qualitative methods. This study contributes to appropriate cybersecurity practices perceived to enhance online shopping experiences among users. The study was conducted with e-commerce platform users in Gqeberha, Eastern Cape. Chapters 2 and 3 presents literature review for this study.

CHAPTER 2: LITERATURE REVIEW



2.1. Introduction

The research context and problem statement were explained in Chapter 1. The study key objective was clarified as: *"to use the PMT to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha"*. This chapter presents literature review on key concepts central to this study. The literature presented in this chapter will address cybersecurity threats, common cybersecurity threats and cybersecurity practices in relation to e-commerce platform users' experiences, perceptions and shopping behaviour within the e-commerce and internet café context.

2.2. Cybersecurity and Information Security

Cybersecurity and information security have always been an ongoing debate among scholars in the Information Systems field, which often use them interchangeably (Kunal et al., 2022; Taherdoost, 2022a; Von Solms & Von Solms, 2018). Cybersecurity can be traced back to the 1980s, when it evolved from information security, which encompasses digital assets and device security in the minds of people and their visual communication. Also, information security spans centuries, evolving from ancient bureaucracies to modern digital systems (Ramsay et al., 2020; Taherdoost, 2022a; Von Solms & Von Solms, 2018). While some scholars and practitioners use the terms cybersecurity and information security interchangeably, there is a growing consensus that cybersecurity signifies an extensive and modern approach to addressing digital threats across interconnected systems, whereas information security remains a foundational concept, which is less generally used in modern discourse (Kunal et al., 2022; Taherdoost, 2022a). Moreover, the difference between information security and cybersecurity is that information security focuses on protecting information data assets, while cybersecurity is restricted to the information in cyberspace. For this study, both terms are concerned with data security, and they play an important role in the protection of digital assets and address confidentiality, integrity, and availability (CIA) against different types of threats (Alexei & Alexei, 2023; Bada et al., 2019; Von Solms & Von Solms, 2018). Hence, cybersecurity is considered appropriate as it involves the protection of digital information in cyberspace or the Internet from diverse

types of cybersecurity threats faced by e-commerce platform users in the internet cafés.

2.3. Cybersecurity

The definition of cybersecurity varies across different interpretations by many authors, depending on the context of its application; however, understanding its progression is essential. According to Alexei and Alexei (2023) and Von Solms and Von Solms (2018), cybersecurity is a part of information security focusing on the protection of confidentiality, integrity, and availability (CIA) against online threats arising from digital information assets connected via the Internet from being compromised. Cybersecurity is the security of individuals and businesses, protecting them against security breaches or incidents that can affect their information systems (Gunawan & Wendy, 2019). Cybersecurity is the collection of tools, security safeguards, risk management approaches, training, best practices, guidelines and technologies which can be used to protect cyberspace and users' assets (Kshetri, 2021, pg.9). In this study, cybersecurity refers to the protection of confidentiality, integrity and availability (CIA) against online threats which arises from individual digital data or assets such as e-commerce platform users connected through the Internet from being compromised (Gunawan & Wendy, 2019; Von Solms & Von Solms, 2018). According to Ahmad et al. (2023), the growth of e-commerce platforms through digital interconnectivity introduces significant cybersecurity challenges that threaten digital platforms and e-commerce platform users' information. To ensure users' safety on e-commerce platforms, it is essential to implement security measures that strengthen online protection against cybersecurity threats (Boban, 2024).

2.4. User Cybersecurity Practices

Although user cybersecurity practices is an emerging concept, various studies have examined cybersecurity practices from users' perspectives, identifying factors that influence users' cybersecurity behaviours (Herath et al., 2022; Jamil, 2023; Matlala, 2023; Richard, 2023). According to Rao (2023) and Richard (2023), cybersecurity practices refer to adopting effective practices or habits, such as creating unique passwords and avoiding suspicious websites and links to protect sensitive information

from unauthorised access and online threats like phishing and identity theft. Cisco (2024) defines cybersecurity practices as a healthy digital hygiene needed to help users prevent cyberattacks, such as using strong password and enabling multi-factor authentication (MFA). Cybersecurity practices refer to attitudes and behaviour maintained to protect personal information and prevent cybersecurity risks (Herath et al., 2022; Matlala, 2023). Cybersecurity practices are essential for an individual to protect their online transactions due to the rise in cybersecurity threats such as data breaches and financial fraud (Shah & Agarwal, 2020). Some scholars view cybersecurity practices as involving actions and behaviours individuals should adopt to protect their digital information from cyber criminals (Dodge et al., 2023; Herath et al., 2022; Jamil, 2023). Cybersecurity practices include unique password creation, enabling two-factor authentication, avoiding suspicious links, and other practices (Cain et al., 2018; Cisco, 2024; Herath et al., 2022). These practices can help prevent unauthorised access to sensitive information and reduce the risk of exposing financial and personal information during online activities (Cain et al., 2018; Cisco, 2024; Matlala, 2023).

2.5. User Experience

Several definitions of user experiences are extensive and focus mainly on subjective attributes such as user perception, satisfaction, feelings, and social aspect inclusion (Hassenzahl, 2018; Hinderks et al., 2022; Norman & Nielsen, 2016). According to Norman and Nielsen (2016), "user experience" refers to the broad interaction between the end-user and the company providing the products or services. In the same way, ISO 9241-210 defines user experience as “a person’s perceptions and reactions that result from the actual or anticipated use of a product or service” (Hinderks et al., 2022). Unger and Chandler (2012) define user experience as the aspects affecting perceptions and behaviour towards an organisation. According to Hotjar (2022), user experiences in e-commerce refer to the satisfaction users derive from interacting with an online shopping platform. Hence, it is the overall experiences, perceptions, reactions, and satisfaction that users have as they engage with online shopping platforms or websites (Hassenzahl, 2018; Hinderks et al., 2022).

2.6. E-commerce

Scholars have discussed the academic definition of e-commerce. According to Youssef and Hossam (2023), e-commerce uses electronic communications and technologies in business transactions to create and redefine relationships for value between organisations and individuals. Laudon and Traver (2020) define e-commerce as using the Internet, Web-based platforms, and mobile apps and browsers running on mobile devices to digitally transact business between organisations and individuals (Laudon & Traver, 2020). Similarly, Jain et al. (2021) explain e-commerce as “an internet vendor's website or online informal communities and platforms for directly trading goods or services to users”. It further refers to conducting online business via computing devices and online platforms (Wahab et al., 2023).

2.7. An Overview of Common Cybersecurity Threats in E-Commerce

This section outlines common cybersecurity threats that e-commerce platform users face when shopping online in e-commerce platforms and internet cafés.

2.7.1 Social Engineering

Social engineering is the most common scam technique cybercriminals use to influence people's behaviour and frequently take action unnecessarily in their best interest (Galov, 2023). It involves the psychological manipulation of users, compelling them to perform various tasks and activities that make them vulnerable to online attacks (Liu et al., 2022). Some attackers are anonymously targeting users in the internet café for social engineering attacks (Eze, 2019; Jimma, 2022). According to Resmo (2024), five million user accounts were compromised through social engineering attacks, while the "forget password" option is a common example of social engineering, allowing attackers to access user account systems or e-commerce ecosystems through malicious links (Aboelfotoh & Hikal, 2019). Similarly, a study by Fourie (2023) asserts that the recent security breach at Dis-Chem, which exposed the names and contact details of approximately 4 million South African individuals, was caused by social engineering attacks. The breach occurred due to weak passwords

and inadequate monitoring measures. Other examples of social engineering such as phishing, smishing and vishing are covered below.

2.7.1.1 Phishing Website

Phishing of websites is a severe form of online fraud that undermines users' experiences and confidence, negatively affecting both business reputation and online interactions (Badotra & Sundas, 2021; Dhobe et al., 2020; Prasad & Rohokale, 2020). Modern phishing websites often employ multiple-stage tactics to steal login credentials while appearing legitimate to e-commerce platform users, evading detection and security measures (Subramani et al., 2022). These attacks steal sensitive information, such as credentials or personal data, and exploit it (Desamsetti, 2021). Phishing websites are exacerbated by the increased use of electronic commerce and public internet cafés, where fake websites deceive users into revealing personal information (Dhobe et al., 2020; Hasan et al., 2023; Prasad & Rohokale, 2020). Attackers manipulate e-commerce platform users by gaining their trust on e-commerce platforms and exploiting their data for personal gain (Liu et al., 2022). For instance, phishing websites lead many South African users to fake websites and banking sites such as Standard Bank, ABSA, and others, prompting them to verify or update sensitive information such as login credentials and credit card details (Burwood, 2024). This is further supported by Wannenburg et al. (2023), who added that South Africans are particularly vulnerable to phishing attacks. Attackers often mimic trusted online shopping platforms such as Amazon, Takealot, or eBay for phishing emails using legitimate logos and images to trick victims into clicking malicious links to steal login credentials or capture credit card information from unsuspecting users (Avinir, 2022).

Phishing websites target vulnerable individuals and businesses, with 80% of attacks focused on financial services, webmail and payment services on e-commerce platforms and public locations (Dhobe et al., 2020; Madupati, 2022; Qabajeh et al., 2018; Sahoo & Gupta, 2019). According to a recent Cisco report, over 90% of data breaches stem from phishing attacks that require users' input on fraudulent websites (Subramani et al., 2022). This includes clicking on pop-ups, moving the mouse, and click-through actions (Zhang *et al.*, 2021). Subramani *et al.* (2022) used machine

learning to simulate and explore user experiences with phishing websites, analysing over 50,000 sites. They reveal that most phishing sites were online or cloud services, as well as financial, e-commerce, and payment services. Their findings showed that phishing primarily aims to steal login, personal, social, and financial information, which appeared to be a high level of phishing activity. The study further revealed that phishing information linked to email and passwords, with 28,736 and 35,762 pages, respectively (Subramani et al., 2022). Naive users are particularly susceptible to phishing scams due to their limited understanding of cybersecurity measures, resulting in increased susceptibility to scams and security breaches (Aboelfotoh & Hikal, 2019; Kshetri, 2021; Mosteanu & Galea, 2020). This highlights the need for continuous cybersecurity education and practices as protective measures to combat the growing phishing threat.

2.7.1.2 Smishing

Smishing is a form of SMS phishing which emerged as a significant cybersecurity threat in recent years, especially with the widespread use of smartphones to connect on a public network such as at an internet café (EC-Council, 2024; Liu et al., 2022), Smishing is a tactic attackers use to send phone messages to influence a victim's immediate behaviour to visit a malicious website or download anything maliciously (Liu et al., 2022). According to Liu et al. (2022), 328% of smishing frauds were recorded in 2020 alone. Bešić (2023) affirmed the use of smishing tactics by attackers to falsely claim to be a postal and package delivery service, requesting users to confirm their orders by providing confidential information. They also send an SMS posing as a bank, revealing account changes and requesting data, attempting to complete an action on their bank account (Bešić, 2023). With this, attackers target users on e-commerce websites and public networks to build relationships and collect data for personal use, targeting anyone regardless of their experience, education, or status (Desamsetti, 2021; Liu et al., 2022). For example, in South Africa, a survey by EC-Council (2024) revealed that 60% of South African users received spam messages weekly, with 28% experiencing it daily. The report highlighted smishing scams, where attackers impersonate bank officials to trick victims into sharing personal information or clicking malicious links promising rewards or discounts. Although awareness is rising, these

threats persist due to widespread reliance on SMS and mobile apps for online transactions in the public network (Peripherals, 2023).

2.7.1.3 Vishing

Literature shows that vishing or voice phishing is one of the social engineering attacks that exploits phone calls to deceive victims into disclosing sensitive information (Ali & Mohd Zaharon, 2024; Viji et al., 2022). The term "vishing" is derived from organisations that deal with users, such as banks and e-commerce businesses (Ali & Mohd Zaharon, 2024; Viji et al., 2022). Vishing or voice phishing scams can occur in two ways. Firstly, users receive an email indicating account issues, providing a customer service number to call, and being prompted to log in using account numbers and passwords. This scam is designed to trick e-commerce platform users into clicking on fraudulent links. Secondly, scams involve calling users directly and urging them to call fraudulent customer service numbers to protect their accounts. Vishing criminals may also create a false sense of security by confirming personal information, such as full name, address, or credit card number (Ali & Mohd Zaharon, 2024; Phomkamin et al., 2021). Once they do, they are prompted to enter their account details, such as their account number. Lastly, they also employ fake caller IDs to appear authentic and trustworthy (Viji et al., 2022). A study by Burwood (2024) reports a 36% year-on-year increase in online fraud in South Africa, with an average loss per incident increasing by 9%. The total loss from digital banking fraud reached R740,847,488 ($40.8 million), resulting in a 68% increase in financial impact, partly attributed to vishing attacks, where criminals obtain one-time passwords or random verification numbers from victims for fraudulent transactions (Burwood, 2024).

2.7.2 Malware

Malware, or malicious software, is the common cause of cyber-attacks, allowing cybercriminals to control a user's computer and content, often manifesting as viruses, Trojan horses, or worms. A study by Houmz et al. (2016) found that 60% of internet café computers were infected with malware capable of stealing user information as a sign of poor security levels. Malicious software usually threatens to release a victim's data, blocking access to it unless they pay a ransom. These threats harm targeted

services or public networks, prevent proper operation, install spyware, and control the situation (Banday & Qadri, 2011; Desamsetti, 2021; Kiselichki et al., 2022). Malware significantly threatens businesses, causing inconveniences for internet cafés and users (Aliyu, 2019; Andreianu, 2023). BigCommerce (2021) reports that 29% of e-commerce website traffic is malicious, used by attackers to target web-based applications, access sensitive data, or serve as a staging area for attacks. Many users have fallen victim to infected computers, which have led to security incidents, as attackers may compromise many computers in the internet café to launch a vast attack (Alawida et al., 2022; Aliyu, 2019; Ojo, 2021). Similarly, South Africa has the highest number of ransomware attacks, with over 1.5 million attacks targeting companies and internet cafés, costing R30 million a year for any successful attack. These attacks target e-commerce and users through emails, mobile banking and internet café environments (Houmz et al., 2016; Interpol, 2021; Nedbank, 2023).

2.7.3 E-skimming

Studies show that e-skimming has become a significant security concern in the e-commerce and public areas, such as internet cafés, due to its frequent use to steal users' payment details (Rus et al., 2024, 2023; Shah et al., 2024). E-skimming is a cybercrime where hackers steal sensitive payment information, such as credit card numbers, from e-commerce platform users by injecting malicious code into e-commerce websites or POS systems during purchase transactions (BigCommerce, 2021). For example, a study on the misuse of stolen payment data revealed that of 50 compromised sites, 15 cards were subjected to an attempt to misuse. The thieves tried to use the 15 cards at least 45 times (Rouge et al., 2020). According to the South African Banking Risk Information Centre in 2022, counterfeit credit card fraud victims lost R142 million, while losses from debit card fraud were R270 million. Attackers can use the stolen information to create fake credit cards, sell online, or make fraudulent purchases (Puchert, 2024).

2.7.4 Credit Card Fraud

Literature shows that the growing prevalence of credit card usage in online shopping platforms has led to increased fraud incidents, which have posed serious financial

risks to individuals in internet cafés and e-commerce platforms (Makki et al., 2019; Otokunefor & Kari, 2008; Singhal et al., 2023). Online shopping has made it easier for attackers to access credit card details, make unauthorised purchases, or hold data for ransom (Avinir, 2022). According to Goga et al. (2019), 70%-75% of South African users use credit and debit cards for e-commerce transactions, with Visa and Mastercard being the primary providers. As a result, credit card fraud has become a prevalent security issue, causing significant financial loss and loss of online users on e-commerce platforms (Goga et al., 2019; Jamra et al., 2020; Nasr et al., 2020). This makes users hesitant to share their credit card information online due to concerns about fraud. When attackers gain access to personal information, they can request new credit cards in the victim's name (Avinir, 2022).

2.7.5 Cyberattacks Targeting User Data on E-Commerce Platforms

Targeting personal data is one of the significant challenges in e-commerce. As the world becomes more digitised, the volume of personal data shared, stored, and saved online has surged (Oki et al., 2021; Zende, 2022), while access and use of public networks such as internet cafés increase cybercrime, potentially leading to the theft of e-commerce platform users' confidential information (Hussien et al., 2022). Globally, 30,000 online business transactions, including those conducted in South Africa, are hacked daily, resulting in significant financial losses (Palatty, 2023; Ramsern & Govender, 2023). Hackers often exploit vulnerabilities in merchant systems to access sensitive information, such as credit card details and personal data, during online purchases (Khan, 2019). Additionally, susceptible merchant back-end and database are exposed to external fulfilment centres (Khan, 2019). E-commerce platforms collect extensive data, including home addresses, phone numbers, bank card numbers, dates of birth, and others, with e-commerce platform users' purchasing history, making them prime targets for attacks (Liu et al., 2022; Vasupula et al., 2022). Therefore, e-commerce platform users must comprehend the risks associated with personal information and the potential cost of data breaches.

2.7.6 Payment Fraud

Several e-commerce platforms offer various payment options, including mobile payment, MasterCard, and cash on delivery, to enhance online shopping experiences. These options often link to third-party payment services like PayPal, which require customers' financial details and are frequently targeted by hackers, increasing their vulnerability to cyber-attacks (Hossain, 2019; Rosário, 2023; TransUnion, 2024). According to Kuruwitaarachchi et al. (2019), three key points of vulnerability in e-payment transactions are the customer end, server side, and communication channel, highlighting them as ongoing security concerns that restrict customers and vendors in e-commerce. In South Africa, for example, payment fraud increased from 414.4 million rands in 2022 to 452.3 million rands in 2023, affecting 63.1 per cent of e-commerce platform users in the unsecured public network, such as an internet café (Kitbuncha, 2017; Sabric, 2023; TransUnion, 2024). Payment fraud has become a significant challenge for both e-commerce and consumers, resulting in a loss of customer trust in online transactions. They emphasise the importance of protecting e-commerce transactions and customer personal data (Jamra et al., 2020; Mofokeng, 2021; Prasad & Rohokale, 2020). Nasr et al. (2020) found that payment fraud attempts increased by 7.1%, costing billions of dollars in losses for companies and their customers. Hamed and El-Deeb (2020) found that 125% of e-commerce platform users prefer cash payment due to perceived risk and privacy concerns, with 8 out of 10 opting for it due to the lack of trust in sharing credit card information online. Online payment systems are essential for customers to return broken or flawed merchandise, and credit card security is vital for online merchants (Aseri, 2021; Wahab et al., 2023).

2.7.7 SQL Injection and Cross-site Scripting (XSS)

Studies highlight SQL injection and cross-site scripting (XSS) as the most dangerous vulnerabilities in e-commerce (Agarwala, 2021; Dakov & Malinova, 2021). These attacks exploit input validation flaws to inject malicious code, potentially leading to unauthorised access to users' sensitive information, data theft and website defacement (Blancaflor et al., 2023). XSS affects the client-side by frequently using JavaScript to steal cookies or hijack sessions, which happens when users visit e-commerce sites that unknowingly execute the malicious code. At the same time, SQL

injection targets the database server by manipulating the web application; commonly, when user input is wrongly typed and thereby unexpectedly executed (Blancaflor et al., 2023; Lesko, 2020; Rahman et al., 2020).

2.7.8 Distributed Denial of Service (DDoS) and Botnet Attacks

DDoS and botnet attacks pose a significant threat to e-commerce, potentially causing substantial financial loss and disrupting services (Alawida et al., 2022; Varma et al., 2023). Botnets are compromised machine networks used as a tool to automate more extensive campaigns of DDoS attacks. A DDoS attack is an attack deployed by attackers to render online services to users by creating a large amount of traffic (Alawida et al., 2022; Interpol, 2021). Botnet threats in e-commerce applications require attention, as they can launch attacks, including DDoS. These attacks often affect the confidentiality, integrity and availability of e-commerce services. For example, literature shows reported cases of South African banks and businesses experiencing massive DDoS attacks (Interpol, 2021; Nyoni et al., 2024).

2.7.9 Main in-the-Middle Attacks

The growing occurrence of main in-the-middle (MITM) attacks poses a considerable security risk to users' sensitive information during online transmission over networks (Dakov & Malinova, 2021; Ilavendhan & Atchaya, 2024; Kimura et al., 2023). The connection to public Wi-Fi or the Internet accelerates MITM attacks. MITM attacks can monitor victims' browsing behaviour, eavesdrop on their communications, and tamper with their data. Literature reveals that many users ignorantly share or expose sensitive information through HTTP and unsecured public Internet as they shop on e-commerce sites with many third-party tracking domains (Bilal et al., 2023; Kimura et al., 2024, 2023). According to Yasar (2022), 35 per cent of websites are targeted for MITM attacks, especially when they do not apply HTTPS or SSL to transmit online information. Kimura et al. (2023) explain that many users become victims of e-commerce because attackers manipulate their URLs. All confidential information, including online banking details, was managed by the attackers, exposing the victims' sensitive information on the e-commerce sites.

2.7.10 Credential Stuffing

Credential stuffing is an attack that obtains stolen account credentials and attempts to "stuff" the compromised usernames and passwords from previous data breaches to gain access to other e-commerce platforms successfully (Barkworth et al., 2022; Rai et al., 2024). According to Lempereur (2022) and Petrosyan (2024), over 90% of global e-commerce login traffic originated from billions of credential-stuffing attacks. For example, in 2019, Dunkin' Doughnuts became a victim of this attack, resulting in 1,200 of their 10 million customers exposed, in which the attacker used the same stolen credentials to access other platforms (Cimpanu, 2019; Lempereur, 2022).

2.7.11 Supply Chain Attacks and Zero-Day Exploits

Studies emphasise the growing threat of online attacks on e-commerce supply chains. Supply chain attacks exploit vulnerabilities in the software development process, potentially compromising downstream customers (Faruk et al., 2022). These attacks can have significant economic impacts, with an average cost of $1.4M per enterprise in 2021 (Kshetri & Kshetri, 2022). Studies propose risk mitigation strategies, including zero-trust approaches, multi-factor authentication, and blockchain technology (Martinez & Javier, 2021; Zawaideh et al., 2023). Some researchers suggest government intervention through penalty schemes may benefit when consumer surplus is prioritised (Luo & Choi, 2022). However, detecting and preventing supply chain attacks remains challenging, with ongoing debates about vulnerability disclosure versus retention (Ablon & Bogart, 2017; Xinyuan, 2021). As e-commerce expands, addressing these cybersecurity concerns is crucial for maintaining supply chain resilience and consumer trust (Zawaideh et al., 2023).

2.7.12 E-Commerce Platform Users' Perceptions of Cybersecurity Threats

E-commerce platform users in South Africa face increasing concerns about cybersecurity threats, with the most common perceived risks including financial losses, identity theft, data exposure, online fraud, malware and phishing attacks (Dakov & Malinova, 2021; Malapane, 2019; Malapane & Ndlovu, 2024). Literature highlights the importance of addressing these perceived risks of e-commerce platform users to

enhance their shopping experiences (Butler & Butler, 2019; Pentz et al., 2020; Veiga et al., 2022). A study by Pentz et al. (2020) stated that inexperienced users are significantly affected by these risks, which impact their shopping experience or purchase intentions. Malapane (2019) highlights that users are distraught about exposure to these perceived risks, with financial risks being a primary concern. Makhitha and Ngobeni (2024) suggest that reducing cybersecurity risks can influence online shopping intentions. Meanwhile, Butler and Butler (2015) argue that despite growing concerns about perceived risks, many users, including those with prior negative experiences, continue to adopt poor password practices, leaving them vulnerable to cyberattacks. Beneke et al. (2010) assert that e-commerce platform users with previous experience and familiarity with the e-commerce platforms help to reduce these perceived risks of online shopping.

Similarly, Vanishree (2012) claims that perceived risks, such as online attacks and financial risks, do not affect experienced shoppers' intention to shop on e-commerce platforms. A study by Baloyi and Kotze (2017) highlighted that South African users are concerned about cybersecurity threats and the potential loss of personal information. Studies show that while users are concerned about their personal information, they often lack knowledge of effective cybersecurity practices to mitigate those risks (Dakov & Malinova, 2021; Kariuki et al., 2024; Shabe et al., 2017). User perception of cyber threats is shaped by a resigned attitude toward confidentiality, fear of missing out, and lack of understanding of the value of their personal information (Parker, 2020; Parker & Flowerday, 2021). While cybersecurity awareness campaigns are common, they often fail to change behaviour and do not effectively address users’ anxiety and fear of cyber-attacks while shopping on e-commerce platforms. The fear is further driven by insufficient cybersecurity knowledge, negatively affecting their adoption and compliance with recommended cybersecurity practices (Kariuki et al., 2024; Yang et al., 2020).

2.7.13 Online Shopping Behaviour and Cybersecurity Threats

The perception of cybersecurity threats influences online shopping behaviour in South Africa. Some studies indicate that perceived security and privacy risks are significant

factors that negatively affect e-commerce platform users in online shopping cart abandonment (Benson & Ndoro, 2022; Makhitha & Ngobeni, 2024, 2021). Financial and psychological risks also affect users' attitudes and shopping behaviour toward e-commerce. This negatively impacts their trust and perceptions of e-commerce platforms (Makhitha & Ngobeni, 2021; Pentz et al., 2020). Furthermore, Hariharan et al. (2023) conducted a study of 120 e-commerce platform users, revealing that cybersecurity risks negatively impact their perceptions and behaviour following cyber-attacks on e-commerce platforms. Similarly, personal experiences and various factors such as weak payment systems, perceived risks, and shoppers' mentality can influence shopping behaviour and the decisions made in the e-commerce platforms (Chowdhury & Chowdhury, 2017; Grobler et al., 2021).

Furthermore, user behaviour and security practices may influence their perceptions of e-commerce platforms and online shopping decisions (Osita et al., 2022; Saeed, 2023). On the other hand, Wahab et al. (2023) found that factors such as online vendor trust, cybercrime perception, and internet trust do not influence users' shopping behaviour or trust in e-commerce. They found no significant correlation between online safety and user behaviour (Wahab et al., 2023). Despite uncertainties, users continue to make online purchases, which does not affect their shopping behaviour (Netshirando et al., 2021). While many shoppers express concern about cybersecurity risks, the convenience of online shopping often leads them to overlook potential risks, revealing a complex link between cybersecurity practices and user behaviour (Brandreth & Ophoff, 2020). Consequently, understanding users' behaviour is vital for improving secure shopping experiences. Gaining more profound insight into user shopping behaviour can help to improve cybersecurity practices on e-commerce platforms (Saeed, 2023). Ultimately, this will reduce cyberattacks' impact and improve overall shopping experiences (Chowdhury et al., 2019; Saeed, 2023). These findings show evidence of cybersecurity risks affecting user behaviour and security practices in e-commerce platforms.

2.8. Causes of Attacks on Online Shoppers Using Public Internet Cafés

Literature reveals inadequate security measures, such as implementing multifactor authentication among websites, which diminishes user trust in the platforms and exposes e-commerce platform users to online attacks in the internet café settings (Brandreth & Ophoff, 2020; Houmz et al., 2016; Verkijika, 2019). For example, the risk in using unsecured connections and the lack of security measures were reported to be the cause of various attacks, such as compromised credentials and exposure of sensitive information among e-commerce platform users shopping online via public Wi-Fi or internet cafés (Aseri, 2021; Kaspersky, 2019). A study by Verkijika (2019) found that 92% of these websites exhibited poor password practices, with over 81% failing to provide guidance to users on creating secure passwords. Sunet and Zenzo (2022) also identified challenges in password security and a lack of multifactor authentication on these sites, particularly in e-commerce, including SMEs. Moreover, literature shows that multifactor authentication is underutilised and password-based security on e-commerce platforms requires improvement (Brandreth & Ophoff, 2020; Verkijika, 2019). This is in line with Sunet and Zenzo (2022), who claimed that implementing these measures remains inconsistent, as many e-commerce businesses prioritise profit over investing in cybersecurity training and awareness. Furthermore, users frequently lack awareness about e-commerce security measures, yet they continue to engage with online platforms (Yuniar & Fibrianto, 2021). However, many users perceive themselves as proficient in password security, but they often engage in unsafe password practices, partly due to insufficient guidance and support on improving cybersecurity practices among users (Butler & Butler, 2019, 2015). This highlights a significant gap between their perceived security abilities and cybersecurity practices (Butler & Butler, 2019, 2015). Brandreth and Ophoff (2020) and Verkijika (2019) emphasise that users' poor password practices result from their shortcomings, primarily from inadequate cybersecurity awareness and support in maintaining secure behaviours.

Studies show that users' behaviours can significantly improve with proper education on maintaining cybersecurity practices such as secure passwords and suspicious links (Brandreth & Ophoff, 2020; Sunet & Zenzo, 2022). Despite this, it remains unclear how effectively e-commerce platforms have implemented these security lessons (Sunet & Zenzo, 2022; Verkijika, 2019). Brandreth and Ophoff (2020) emphasise the

need for users' education about cybersecurity best practices, such as identifying phishing attempts, using multifactor authentication and securing passwords. Unfortunately, e-commerce platforms overlook these educational efforts, which can lead to user frustration and decreased confidence in online shopping (Brandreth & Ophoff, 2020). This is notably lacking among South African users; for example, a Cisco survey revealed gaps in cybersecurity knowledge, with 37% of users being unaware of multifactor authentication (MFA), and 19% have never changed their web-based passwords (Davison, 2023). Vega et al. (2022) emphasise that education-based approaches and awareness can be best practices to prevent phishing. Studies show that educational resources significantly reduce users' chances of entering their credentials into malicious websites by 40% (Resmo, 2024; Sahoo & Gupta, 2019). However, user behaviour often contributes to the inadequate application of security practices, such as reluctance to enable two-factor authentication; even though it enhances information security, some users choose not to perform it (Lim, 2021; Mashiane & Kritzinger, 2021; Van Der Schyff et al., 2023).

Cybersecurity practices are essential in e-commerce as they enhance user trust and confidence, protect sensitive data and mitigate potential threats in a public internet café (Aliyu, 2019; Brandreth & Ophoff, 2020; Omorog & Medina, 2020). E-commerce platforms can enhance user safety and security by implementing cybersecurity practices to protect personal and financial data and promote online shopping experiences (Bhatia et al., 2021). Adopting security measures such as multi-level security frameworks that include cryptography and steganography helps to protect personal and financial data, preventing unauthorised access (Bhatia et al., 2021; Haverkamp & Sarmah, 2024). For example, e-commerce companies such as Amazon and Alibaba use One-Time Passwords (OTP) for identity verification and Key Management Systems (KMS) to strengthen security during online transactions and manage encryption keys to protect user data; this remains secure, fostering trust to reduce risks and ensuring an effective online shopping experience (Bhatia et al., 2021).

E-commerce can enhance security by employing encryption algorithms like AES for e-commerce platform users' data and implementing multifactor authentication or two-factor authentication (2FA) to verify user identities (Atadoga et al., 2024; Osita et al., 2022; Saeed, 2023). These methods provide an additional layer of protection by

requiring extra steps apart from username and password, such as using a specific app or device to authenticate login attempts (Saeed, 2023; Shaikh et al., 2017; Zawaideh et al., 2023). Similarly, Laudon and Traver (2020) argue that effective authentication increases user security and sales by 10% to 20% as users become more comfortable with enhanced security due to high data breaches. By adapting security protocols to user preferences, e-commerce platforms can balance protection with ease of use, shopping frequency, and improve user satisfaction and loyalty (Davison, 2023; Nello-Deakin et al., 2024; Tutar et al., 2024).

Studies underline that transparent communication, such as secure SSL certificates for HTTPS hosting and secure payment systems, fosters trust and boosts users' confidence during the transition from HTTP to HTTPS, thereby enhancing their shopping experiences (Hossain et al., 2024; Shaikh et al., 2017; Zawaideh et al., 2023). Likewise, third-party endorsement through seals such as TRUSTe, VeriSign, MasterCard, Visa, and BBBOnline further boosts user trust and confidence by confirming that e-commerce platforms adhere to specific security standards and practices (Ribadu & Rahman, 2019). Trustmarks, such as logos, pictures, or symbols, help alleviate users’ concerns about security and privacy, which can lead to increased sales and surpassing objective source ratings (Cui et al., 2018; Lynn et al., 2016; Ribadu and Rahman, 2019). Also, Etzioni (2019) and Kuzma (2011) assert that these influence users' beliefs about privacy and security, affecting their cognitive and behavioural trust, ultimately influencing user willingness to provide personal information. Similarly, Vosta and Jalilvand (2023) note that a website seal of privacy protection significantly enhances trust perceptions compared to other websites. However, a study conducted by Kirlappos et al. (2012) on third-party trust seals such as VeriSign and Truste of 60 experienced e-commerce platform users found that 38% failed to notice trusted seals on websites. When they did see them, ratings were higher, but users had misconceptions about the presence of seals, which automatically legitimises any website. The study concluded that trust seals do not offer complete protection against scam websites, highlighting that other mechanisms, such as automatic verification of authenticity, are needed to support users' trust decisions (Kirlappos et al., 2012).

2.9. Show Recent Literature on Cybersecurity Practices in Various Contexts

Authors	Objectives	Findings	Recommended Cybersecurity Practices
Castaneda, (2025)	It determines the kinds of personal data users give to artificial intelligence services.	The study highlights that consumers showed a positive attitude towards the safety of artificial intelligence, feel comfortable using those services and tend to share sensitive information about themselves with AI services.	The study suggests that security habits are a vital part of information system protection. It recommends that users be mindful of the information they share online to reduce online risks and maintain good cybersecurity habits, such as using a password manager and unique passwords.
Ahmed (2024)	The study aims to understand the level of cybersecurity awareness and practices of application users and determine the impact on their consent to privacy policies through a case study in application downloading. It also aims to determine the impact of user cybersecurity practices, such as updating software and implementing security measures, on their decision to grant or deny permissions to applications.	The study reveals that many users did not understand cybersecurity measures when using the application, which contributed to users' vulnerability to cyber threats and their tendency to grant permission without fully understanding the implications. It stresses that many users exhibit poor cybersecurity practices such as failing to update applications regularly, using weak passwords and connecting to unsecure networks. These practices can expose users to various cybersecurity threats, including phishing attacks and data breaches.	The study recommends the following: Encouraging application developers to adopt user-friendly and transparent privacy policies that are concise and easily understandable; Developing and implementing full cybersecurity education programs to target different age groups and sectors; Collaborating with educational institutions to include cybersecurity and privacy awareness in their curricula; Using social media platforms and engaging with influencers to spread cybersecurity and privacy awareness messages; and Reviewing and strengthening existing regulatory frameworks related to cybersecurity and data protection.
Kakar et al. (2020)	The study aims to find out why some internet users are more prone to adopt prudent cybersecurity practices than others.	The study reveals that attitudes and behaviours of internet users vary based on regulatory focus. Users with a preventive focus are more likely to adopt and implement cybersecurity best practices than those with a promotion focus. Those with a preventive focus are less likely to experience cybersecurity attacks than users with a promotion focus.	Organisations need to tailor their cybersecurity awareness programs to be dependent on continuing regulatory focus for the users. Preventive focus should complement technical skills that security managers and analysts should advocate for, encouraging users to be more cautious and vigilant about cybersecurity risks.

Authors	Objectives	Findings	Recommended Cybersecurity Practices
Madupati (2022)	The study focuses on the technical perspective on day-to-day follow-ups that are helpful in cybersecurity for both individual and business purposes.	The study reveals multiple reports on common cybersecurity threats, such as phishing, and technical solutions to reduce the risks resulting from these attacks. It proposes multi-factor authentication, encryption protocols, permanent propagation patches and user education as basic elements of a proactive cybersecurity tactic.	The study recommends balancing security with user convenience by bolstering good security practices such as multi-factor authentication and regular updates, while recognising that these can also have an impact on user experiences. Education and the application of safety measures are vital to protect personal details and protective privacy in a world where people constantly access digital technology every day.
Kuraku et al. (2023)	The study examines the impact of computer users' behaviour on their cybersecurity awareness regarding phishing attacks, including the improper management of passwords, software updates, and neglect of regular security measures.	The study highlights major behavioural patterns, including improper password management, neglect of regular security updates, and clicking on suspicious attachments and links, which cause users to expose sensitive information on online platforms. While users show estimable cybersecurity practices, there is a need for ongoing education to empower users to further reduce the risk of falling victim to sophisticated cybersecurity threats.	The study recommends that understanding the connection between user behaviour and cybersecurity awareness will enable computer users to implement proactive measures, minimise the impact of frequent phishing attacks and enhance their cybersecurity resilience.
Al Shakosh (2024)	The study aims to explore and understand the awareness level among young adults regarding cybersecurity threats when utilising public Wi-Fi, and delve into the measures and practices employed by young adults to safeguard themselves from these identified threats.	The study reveals that young adults frequently use public Wi-Fi for various activities, including browsing social media platforms and accessing online resources. They found a discrepancy between awareness and practical security measures. Users exhibit varying levels of recognition of potential threats, with responses ranging from cautious to indifferent regarding the preservation of sensitive activities and the adoption of a careful approach to cybersecurity practices. Some young adults do not regularly adopt proactive cybersecurity measures, while others use cybersecurity practices and tools such as strong passwords, VPNs and antivirus software to safeguard their online activities, and others irregularly overlook such precautions.	The study suggests a need for targeted educational initiatives to enhance protective cybersecurity practices among users, which could inform future cybersecurity policies and educational programs. They should focus on increasing cybersecurity awareness to promote better security habits and reduce the associated risks with public Wi-Fi usage to protect the digital lives of young individuals in Sweden.

2.10. Cybersecurity Practices and User Experiences in Internet Cafés

Literature highlights the role of internet cafés in providing internet access to people in developing countries for essential services (Alontaga, 2018; Munyendo et al., 2023)**.** **I**nternet café serves as a viable environment for users to engage primarily in browsing and online activities (Labuschagne et al., 2011). However, there is a need for continuous awareness on how to improve cybersecurity practices among users (Munyendo et al., 2023; Szumski, 2018). Users are often confronted with online attacks due to a limited understanding of cybersecurity practices and computer literacy (Labuschagne et al., 2011; Munyendo et al., 2023). Aliyu (2019) reveals that many internet cafés and individual using their services had become victims of computer security incidents, which impacted them**.** Likewise, user attitudes and behaviour towards cybersecurity practices can impact their experiences and cybersecurity effectiveness in the internet café environment (Harshavardan and PadmaShani, 2023; Shava & Van Greunen, 2013). For example, the way users understand cybersecurity threats will determine their reactions to online risks. This could motivate or demotivate them to adopt cybersecurity practices (Aliyu, 2019).

Munyendo et al. (2023) emphasise that internet café managers often assist users in creating accounts and management, which at times employ insecure cybersecurity practices such as using a common password for their clients. This makes users vulnerable to account theft or hacking. Similarly, a study by Houmz et al. (2016) in Morocco found that 50% of internet cafés had inadequate cybersecurity practices, with disabled security tools, leading to negative user experiences. They stressed the importance of an awareness program to target the internet café managers and their users. Cybersecurity practices should be designed with user experiences in mind to encourage secure behaviour (Herath et al., 2022; Kleij, 2022). According to Alontaga (2018) and Angelova (2024), cybersecurity practices, including knowledge of digital skills and recognising cyber threats, are important for digital safety in internet cafés for users to enhance their experiences. The application of cybersecurity practices will safeguard users' digital presence and reduce the risks of falling victim to cyber threats. This will enable them to make informed decisions and take control of their online

experiences in the internet cafés environment (Maddel & Nandavadekar, 2014; Richard, 2023).

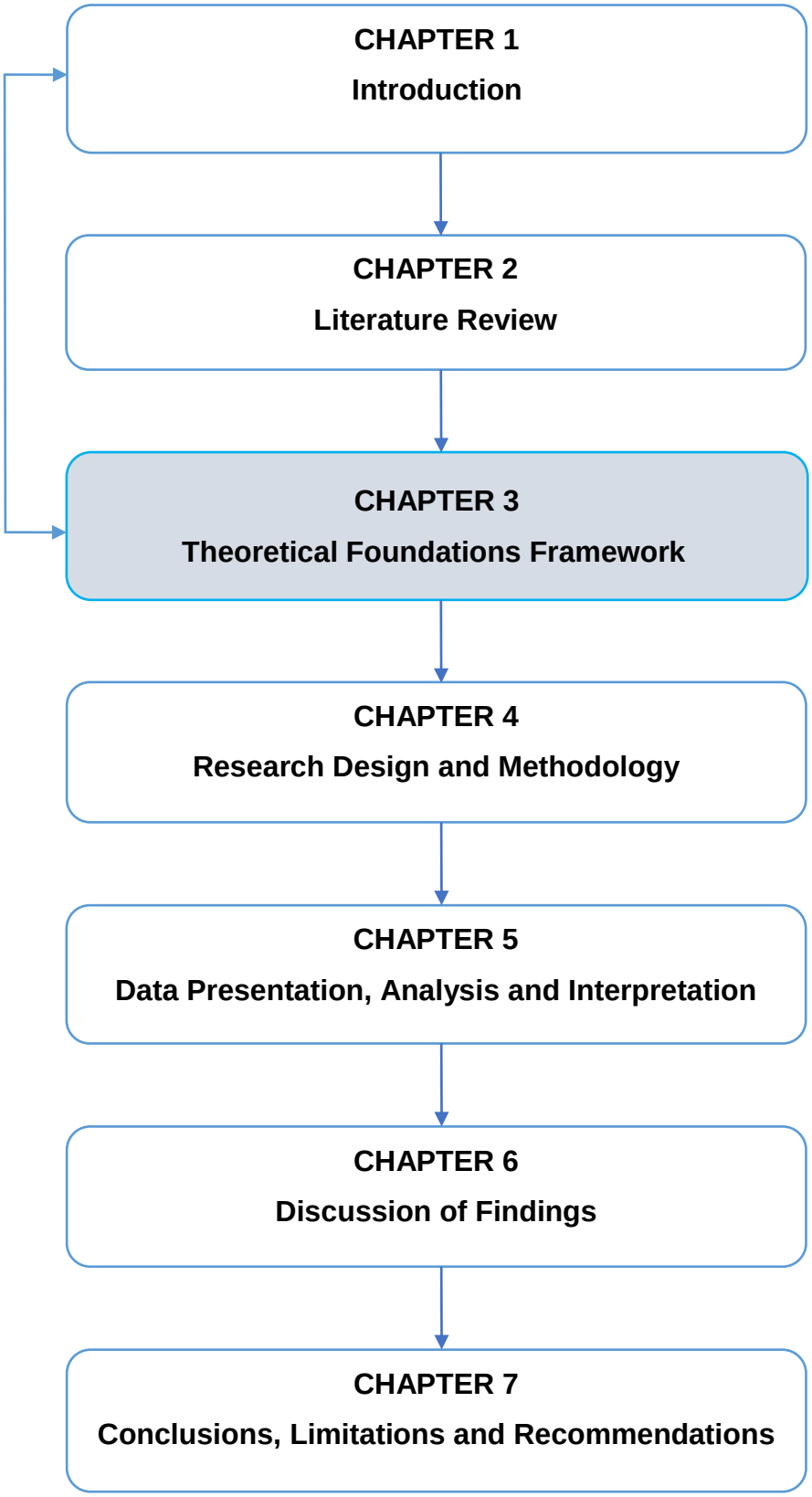
2.11. Conclusion

The chapter presented a literature review on cybersecurity threats, common cybersecurity threats and cybersecurity practices in e-commerce platforms. Factors affecting e-commerce platform users' experiences in e-commerce sectors were explained, and primary cybersecurity practices have been identified in the literature. Cybersecurity threats, including social engineering and phishing websites, were identified as major issues affecting e-commerce platform users who use unsecured connections for their online shopping activities. The literature indicates that cybersecurity threats pose significant challenges for e-commerce platform users shopping online, as they are increasingly targeted by online attacks aimed at stealing their personal and sensitive information.

There is evidence of financial losses, identity theft and online fraud resulting from the perceived risks among the e-commerce platform users. This perception affects users' shopping behaviour on the digital platforms. The literature identified the lack of cybersecurity practices, such as poor password usage and a lack of multifactor authentication, as unsecured behaviours or practices among e-commerce platform users who use internet café facilities for their shopping purposes. The literature highlights the need for education on cybersecurity practices to guide e-commerce platform users, particularly those with a limited understanding of cybersecurity, who are vulnerable to unprotected public networks like internet cafés.

The next chapter will examine the application of Protection Motivation Theory to recent studies in cybersecurity, cybersecurity practices and e-commerce platform users' experiences in e-commerce.

CHAPTER 3: THEORETICAL FOUNDATIONS FRAMEWORK



3.1. Introduction

The previous chapter presented literature review on common cybersecurity threats and cybersecurity practices on e-commerce platform users' experiences, perceptions and shopping behaviour within the context of e-commerce and internet cafés. Chapter 3 will give an account of the theoretical framework, i.e. Protection Motivation Theory (PMT), adopted in this study. This chapter also identifies and addresses gaps in the literature regarding the use of the Protection Motivation Theory (PMT) to assess the impact of cybersecurity practices on e-commerce platform users' experiences, providing a comprehensive analysis of relevant research to bridge these gaps.

3.2. Protection Motivation Theory (PMT)

The Protection Motivation Theory (PMT) is a widely recognised theoretical framework originally in health and then adopted in information systems to understand and predict information security behaviours of individuals (Haag et al., 2021; Marikyan & Papagiannidis, 2023; Rogers, 1983). The PMT has been used primarily in two ways: 1) as a framework for designing persuasive communications and 2) as a social cognition model for predicting security behaviour. According to PMT, the social cognitive model and persuasive communications can influence user attitude to change through cognitive appraisals (Floyd et al., 2000; Haag et al., 2021). Persuasive messages and the social cognitive model impact user intentions on perceived threats to change their attitude towards protection behaviours (Babaei & Vassileva, 2024; Ganesh et al., 2022), providing new insights into the behavioural problems of e-commerce platform users (Frauenstein et al., 2023). The PMT posits that the motivation to protect oneself from threats is essential for determining protective behaviour and understanding how individuals respond to threats (Haag et al., 2021; Marikyan & Papagiannidis, 2023; Shiri et al., 2024). The PMT applies to any situation involving threats and is widely used as an information system theory to understand and predict individual security behaviour, relevant to e-commerce platform users (Alsmadi et al., 2024; Raj Sreenath et al., 2024). It explains individuals' cognitive processes when faced with threats and how these processes influence their motivation

to engage in protective behaviours (Haag et al., 2021; Marikyan & Papagiannidis, 2023).

Rogers (1983) outlines key factors that elicit motivation and subsequent protective behaviour. The individual must believe that 1) the threat is severe, 2) one is vulnerable to the threat, 3) the recommended protective behaviour is effective in preventing the threat, 4) one can perform the recommended protective behaviour, 5) rewards from the current or potentially risky behaviours are rewarded by a factor that reduces the probability of engaging in the current or potential risky behaviour, and 6) costs of the recommended protective behaviours are rewarded by factors that increase the probability to engage in the recommended protective behaviour (Marikyan & Papagiannidis, 2023; Rogers, 1983). Specifically, the PMT suggests individuals must see their vulnerability to severe threats (threat appraisal) and weigh the cost of implementing protective actions to adhere to the recommended behaviour (Coping appraisal) (Haag et al., 2021; Rogers, 1983, 1975). According to the PMT, at the core are two cognitive processes, namely threat appraisal and coping appraisal, that mediate the effects of threatening information on various coping modes, which arouses the motivation to protect oneself as recommended, i.e., protection motivation (Haag et al., 2021; Shiri et al., 2024). These processes are central to forming the protection motivation. PMT suggests that individuals engage in a cognitive process of assessing threats and their abilities to cope with them. Similar threats could likewise invoke motivation to initiate coping appraisal processes (Haag et al., 2021; Marikyan & Papagiannidis, 2023).

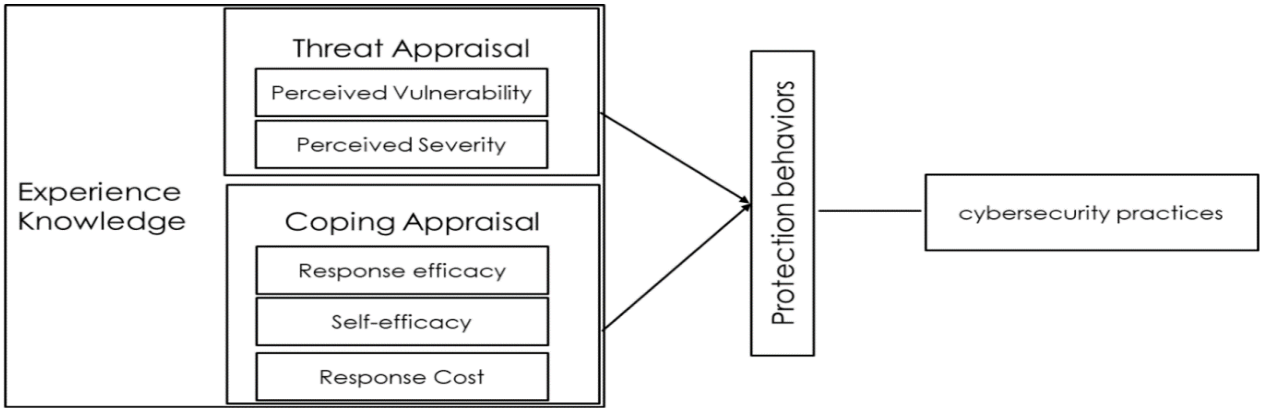


Figure 3.1: Conceptual model created from PMT Theory by Rogers (1983, 1975)

Figure 3.1 represents each component of PMT discussed in the next section.

As explained above, key components of PMT, such as threat and coping appraisals, will be used to assess the impact of cybersecurity practices on users' experiences in the e-commerce platforms in this study, as depicted in Figure 3.1. The diagram illustrates how threat appraisals (perceived susceptibility and severity) and coping appraisals (response efficacy, self-efficacy, and response cost) are applied to cybersecurity practices, explaining their potential impact on users' experiences on e-commerce platforms (see Figure 3.1). Other PMT components that were unrelated to this study were therefore excluded.

3.2.1 Threat Appraisal

The threat appraisal component of the PMT is essential in understanding user behaviour and experience in the context of e-commerce websites. This process evaluates the threat, which involves two components: perceived severity, which assesses the severity of the threat's consequences, and perceived vulnerability, which determines the likelihood of experiencing these threats (Rogers, 1983; Ruan et al., 2020; Wang et al., 2022). If either severity or vulnerability is perceived as low, it can reduce motivation to act, affecting overall threat perception and users' experiences (Haag et al., 2021; Marikyan & Papagiannidis, 2023; Rogers, 1983). E-commerce platform users who access platforms via public networks or unprotected devices without employing secure practices are vulnerable to cybersecurity risks, which can lead to negative experiences (Prasetyo & Wahab, 2022; Tsai et al., 2016).

3.2.1.1 Perceived Vulnerability

Perceived vulnerability refers to users' subjective assessment of the likelihood of falling victim to potential cybersecurity threats, which can influence their shopping experiences (Ghazali et al., 2023; Rahman, Prasetyo & Wahab, 2022; Shiri et al., 2024). This risk of cybersecurity threats can increase users' weakness, limiting control over their personal data in digital platforms (Aseri, 2021; Maphosa, 2023; Prasad & Rohokale, 2020), with anxieties on perceived threats such as data breaches, identity thefts and financial losses noticed during online transactions (Prasad and Rohokale, 2020). Factors such as transaction frequency and personal information exposure affect users' likelihood to face unfavourable online security hazards and perceived

vulnerability (Torten et al., 2018). However, users often underrate risks and prioritise their convenience and price over security, disregarding security warnings and viewing cybersecurity as an obstacle to their shopping experiences (Grobler et al., 2021; Kirlappos et al., 2012; Wahab et al., 2023). This perception reduces the effectiveness of protective measures and negatively exacerbates susceptibility (Chowdhury et al., 2019).

3.2.1.2 Perceived Severity

Perceived severity is an individual's assessment of the negative consequences of an event based on their belief in the seriousness of the damage (Kariuki et al., 2024; Shiri et al., 2024). According to PMT, the perception of the threat's severity is essential for motivating protective behaviour; a lack of this perception can reduce motivation even if the threat is severe (Boerman et al., 2021). Technical knowledge and awareness have been shown to correlate with perceived severity (Ham, 2017; Shah and Agarwal, 2020; Strycharz et al., 2019). Online threat perceptions of dangers or severity are influenced by personal experiences, others' experiences, and news media (Tsai et al., 2016). Users' understanding of the potential problems posed by data breaches and security threats affects their perception of severity. When they perceive severe consequences for their privacy and security, they are more likely to adjust their security behaviour to prevent future incidents (Giwah et al., 2019; Prasetyo & Wahab, 2022).

Liu et al. (2018) highlight that user behaviours and experiences play a critical role in the effectiveness of security mechanisms; if users feel unmotivated or misunderstand these mechanisms, their success can be compromised on e-commerce platforms. Insufficient ability to perceive cyber-attack risks and identify effective preventive measures can negatively impact protective behaviour (Ghazali et al., 2023; Mamat et al., 2023; Wu et al., 2024). Also, users' perceptions of the severity and likelihood of threats can significantly influence their intention to purchase online. Those who perceive severe threats may be more motivated to take protective actions, such as avoiding e-commerce sites or adopting additional security practices (Chennamaneni & Gupta, 2023; Omar et al., 2021; Phamthi et al., 2024). Conversely, the perceived benefits of risky behaviour, such as the convenience of online shopping, can affect the

threat appraisal process (Mamat et al., 2023). If users believe the benefits of using e-commerce sites outweigh the risks, they may be less motivated to adopt protective actions (Grobler et al., 2021; Kirlappos et al., 2012). Thus, the threat appraisal component of the PMT offers a valuable framework for understanding how users' perceptions of privacy and security risks can influence their behavioural intention in e-commerce sites (Omar et al., 2021; Saeed, 2023; Sajikumar et al., 2024).

3.2.2 Coping Appraisal

The coping appraisal component of PMT is essential for determining users' intentions to adopt protective measures. It includes three key factors: self-efficacy, response efficacy, and response costs (Haag et al., 2021; Shiri et al., 2024). Coping appraisal plays a vital role in shaping individuals' decisions to adopt cybersecurity measures (Haque et al., 2020; Schneider & Rahman, 2021).

Response efficacy is the belief that the recommended protection action will effectively mitigate or eliminate the threat. For instance, implementing cybersecurity measures can reduce the likelihood of falling victim to cyber threats (Ghazali et al., 2023; Haag et al., 2021; Marikyan and Papagiannidis, 2023).

Self-efficacy is the belief in one's ability to execute the recommended protection actions and manage online activities successfully. High self-efficacy is essential for effective decision-making regarding online security and privacy during online transactions to protect sensitive information (Haag et al., 2021; Rahman Prasetyo & Wahab, 2022; Tsai et al., 2016).

Response Cost: it encompasses the perceived costs associated with taking protective actions, such as time, money, effort, and inconvenience, which is the cost of using security protection (Haag et al., 2021; Marikyan & Papagiannidis, 2023).

Understanding these components will help to evaluate the effectiveness and feasibility of e-commerce platform users' protective behaviours, such as strong passwords, enabling two-factor authentication, and financial transaction monitoring (Mashiane & Kritzinger, 2021). Coping appraisals are also linked to the intention to use anti-virus software for identity theft protection (Tsai et al., 2016) and adopt blockchain for data privacy and security (Marikyan et al., 2022). Individuals with high self-efficacy are

better at managing privacy and security risks (Boerman et al., 2021) by engaging in protective behaviour (Giwah et al., 2019; Mou et al., 2022) and responding to training and cybersecurity measures (Schneider & Rahman, 2021). In addition, those with higher internet skills (De Kimpe et al., 2021; Tsai et al., 2016) and knowledge about security measures are more likely to protect their online activities (Lee and Seomun, 2021). The threat messages continued with information on response efficacy and self-efficacy (Jansen & Van Schaik, 2019), which influenced user intentions to adopt smartphone security measures (Schneider & Rahman, 2021) on e-commerce platforms (Pobee, 2021), to protect themselves against a specific threat (Boerman et al., 2021). Understanding these cognitive processes guides the development of user-centred security measures, enabling proactive protection of online activities (Avalos et al., 2022; Humaidi & Alghazo, 2022).

3.3. Protection Motivation Theory in Cybersecurity

The PMT has been extensively applied in the field of formation systems to understand and predict cybersecurity behaviour. Studies highlight PMT's effectiveness in analysing how users respond to cyber threats and engage in protective behaviours (Almansoori et al., 2023; Alsmadi et al., 2024; Avalos et al., 2022). For example, according to Sommestad et al. (2015), PMT constructs positively impact security behaviour, particularly when coping methods are concrete and voluntary. PMT constructs significantly influence information security behaviour of nurses, affecting their cybersecurity measures (Lee & Seomun, 2021). A study conducted by Giwah et al. (2019) demonstrated that mobile security self-efficacy influences users' motivation and suggested security training programs as a data breach prevention for mobile device security measures. Cybersecurity vulnerabilities stem from limited knowledge and skills among educators, compromised threat appraisal and misguided cybersecurity self-efficacy (Magunje & Chigona, 2024). Educators should focus on self-efficacy, cybersecurity training design and programs and enhance individuals' response efficacy and protection motivation (Khan et al., 2024, 2023). According to Tawalbeh and Muheidat (2023), threat and coping factors significantly influence employees' motivation towards cybersecurity behaviour. Highly motivated employees

with high threat appraisal, response efficacy, and self-efficacy engage in cybersecurity exercise, awareness and organisational effort, positively influencing PTM constructs (Kuppusamy et al., 2022; Sulaiman et al., 2022).

PMT components such as perceived threats and self-efficacy significantly influence protection motivation in response to cyberattacks. Interventions should focus on individual vulnerability and improve the effectiveness of self-protective measures while highlighting organisational consequences (Vrhovec & Mihelič, 2021). Self-efficacy, a key predictor of security intentions readability, may be less effective when fear of cyberattacks is high and more effective when fear is low (Vrhovec & Mihelič, 2021). According to Ding et al. (2014), the application of PMT to improve security motivation through training found that PMT enhance threat perception and coping responses. In a study by Schneider and Rahman (2021), PMT factors affecting smartphone security measures adoption among undergraduates are recommended to improve hardware and software security solutions. Self-efficacy increases users' protective behaviour and safeguards them through education. They identified that security coping factors predict protective behaviour intention and suggest increasing awareness, motivation to protect against cyber threats, and well-designed cybersecurity measures. Coping messages are more effective in taking action against cybersecurity threats than threat appeals in enhancing online security behaviour, with effectiveness influenced by risk attitudes, age, and country (Van Bavel et al., 2019). Similarly, a study by Humaidi and Alghazo (2022) confirmed that threat and coping appraisal positively impact cybersecurity protective behaviour, although self-efficacy is less influential. It was noted that overconfidence in cybersecurity knowledge and internet trust could undermine motivation for protective measures, particularly highlighting the role of self-efficacy in coping mechanisms (De Kimpe et al., 2021).

PMT constructs supported response cost and effectiveness, affecting motivation for security, while vulnerability and severity were less impactful in a study by Vestad (2022). According to Kariuki et al. (2024), small-scale traders in Southern Africa lacked cybersecurity knowledge, making them more susceptible to cyber threats, and recommended enhanced technical information and safer digital practices. Similarly, Hassan et al. (2024) explored the impact of e-service users' intention to protect

themselves against cyber fraud. They found that cybersecurity efficacy and response efficacy positively influence protection behaviour, while perceived vulnerability does not. In a meta-analysis conducted by Mou et al. (2022), they highlighted that response efficacy and self-efficacy are strong predictors impacting security behaviour, with PMT theoretical relationships being stronger in personal contexts than in the workplace, while intention-behaviour relationships are stronger in the workplace and compliance settings. A PMT study on university students' compliance with cybersecurity measures shows that they are influenced by their perception of threat severity, likelihood, and their belief in the effectiveness of the recommended solutions, suggesting the need for targeted awareness initiatives (Mtambeka et al., 2023). Additionally, perceived costs, response efficacy, self-efficacy, perceived severity, and perceived vulnerability significantly impact cybersecurity awareness (Almansoori et al., 2023; Tran et al., 2024). Moreover, Jansen and Van Schaik (2019) used PMT to investigate how fear of manipulative messages impacts user cognitions, attitudes, and precautionary behaviour against phishing attacks. They found that strong fear appeal significantly influences attitudes and intentions, while perceived vulnerability is low and recommend qualitative studies to understand user perceptions and reactions.

3.4. Protection Motivation Theory in Privacy

Some studies applied PMT to examine its application to privacy concerns and protection. Sajikumar et al. (2024) explored how privacy concerns and mobile cybersecurity awareness interact with PMT constructs. They found that increasing awareness about mobile cybersecurity threats can improve user protection, reduce privacy concerns, and improve security during mobile transactions. A study conducted by Mousavi et al. (2020) used PMT constructs to examine how coping and threat appraisals impact user protective behaviour on social networking sites. They revealed that these appraisals significantly affect privacy behaviours and engagement in risky actions. Ioannou et al. (2021) applied PMT to study how dispositional mindfulness affects privacy concerns of threat appraisal. They found that mindful buyers perceive privacy threats as less severe and are more willing to share personal information online. Similarly, Terlizzi et al. (2019) demonstrated that PMT constructs highlight the importance of cybersecurity and data privacy in mobile banking, activating fears of

data loss and reducing trust in the platform. Additionally, PMT constructs, and high social norms do not necessarily increase privacy protection motivation on Facebook. Users' self-withdrawal intentions are influenced by their perception of privacy threats and protection effectiveness in a study by Meier et al. (2020). Likewise, Boerman et al. (2021) employed PMT constructs to examine the motivation for online privacy protection, finding that perceived severity and response efficacy significantly influence privacy-protection behaviour.

Moreover, Read and Van Der Schyff (2020) studied the use of Facebook privacy settings through the theory of planned behaviour (TPB) and PMT. They discovered that ineffective use of privacy settings could be attributed to subjective norms and user ignorance about privacy threats. Users on Facebook are at risk of privacy threats due to incomplete, inaccurate, or missing information in threat appraisal processes (Hinds et al., 2020). Chennamaneni and Gupta (2023) explored factors influencing the privacy concerns of mobile app users. They found that threat appraisal significantly impacts privacy concerns, with neuroticism affecting perceived vulnerability and severity. Users' coping appraisals also influence their privacy. Visinescu et al. (2016) found that privacy risk perception, the need for privacy, self-efficacy and the effectiveness of preventive measures significantly impact individuals' decisions to develop protective strategies in a cloud computing environment. MMHS fear may stem from privacy concerns triggered by personal information threats, leading to attempts to reduce emotional instability and find adaptive coping responses in a study by Zhang et al. (2021). According to Shiri et al. (2024), PMT components enhance user motivation by providing effective mechanisms to combat threats, emphasising the need to understand privacy-related risks to improve self-efficacy and reduce vulnerability.

3.5. Application of Protection Motivation Theory in E-commerce Contexts

Protection motivation theory has been applied across various e-commerce studies to analyse how perceptions of threats and coping mechanisms shape users' and businesses' protective behaviour (Gumasing et al., 2023; Pobee, 2021; Prasetyo & Wahab, 2022). For example, higher perceived severity and lower response costs encourage users to engage with information on manipulative design in e-commerce,

suggesting platforms can improve user protection by enhancing transparency and accountability, according to a study by Babaei and Vassileva (2024). Furthermore, according to Roberts and Rahman (2021), an understanding of self-efficacy and response efficacy aids in developing training programs for end-user behaviours against cyber threats. PTM can be utilised to develop tools that counter cyber fraud affecting e-commerce platform users, indicating that users' online habits can either aid or compromise them (Ghazali et al., 2023). Furthermore, enhanced protection measures can be implemented to prevent users from falling victim to cyber fraud (Saeed, 2023). PTM constructs revealed that tourists are highly vulnerable to various cyber-attacks such as insecure transactions, personal data breaches and phishing, underscoring the need for effective responses to these threats (Ghaderi et al., 2024). According to Gumasing et al.'s (2023) study on PMT, which used a machine learning ensemble to evaluate factors affecting online grocery app usage in the Philippines, found that perceived benefits, vulnerability and behavioural intention were significant factors, with perceived severity influencing intention and usage and response efficacy impacting behaviour towards online groceries. Perceived severity, self-efficacy, and safety habit behaviour influence user loyalty in e-commerce platforms, particularly in response to data breaches, with safety habits significantly affecting trustworthiness (Prasetyo & Wahab, 2022). Additionally, hardiness and habit significantly impact SME's employee security behaviour intention, while the threat appraisal process did not significantly influence this intention (Aigbefo et al., 2022).

Furthermore, studies such as Teofilus et al. (2020) showed that Indonesian millennials' low-risk perception and privacy concerns reduced their online shopping intention, emphasising the importance of transparency in e-commerce platforms. E-commerce businesses, particularly Tokopedia, should be more attentive to terms and conditions regarding privacy. They highlight the need to explore perspectives on privacy fear in PMT. Self-efficacy and response efficacy influenced user attitudes towards online purchases during COVID-19, highlighting the role of protective motivations in shaping shopping behaviour (Mat Dawi et al., 2024). PMT constructs impact perceived vulnerability, response cost, response efficacy, and security habits in end-user security behaviour during COVID-19. However, policy compliance attitude, self-efficacy, and

perceived severity do not significantly impact behaviour intention (Kautondokwa et al., 2021). Perceived severity, response efficacy, and self-efficacy had a positive impact on users' continuous adoption of m-payments through effective awareness campaigns for the platforms (Hamzah, 2024). In the same way, Misra et al. (2022) highlighted that perceived vulnerability drives SMEs to adopt the Electronic Marketplace despite low self-efficacy. Older groups are more vulnerable to business closure if they do not join the Electronic Marketplace, which leads to a positive attitude towards online selling. Self-efficacy, response-efficacy and attitude significantly influence their behavioural intention to adopt e-commerce in a study by Pobee (2021). However, perceived vulnerability, severity, and response costs have insignificant effects, recommending that e-vendors should create user-friendly websites to reduce user stress and anxiety. Similarly, Bekkers et al. (2023) found that entrepreneurs are more likely to take preventive measures against ransomware when they perceive the risk as severe, their company as vulnerable, and are concerned about potential threats. However, those with high self-efficacy and confidence in their existing preventive measures (response efficacy) are less likely to take preventive measures. Additionally, Idayani et al. (2024) applied PMT, revealing that individuals are motivated to take preventive actions against cyber threats by assessing their protective behaviour and acceptance of security measures by Fintech platforms.

3.6. Protection Motivation Theory and User Experiences

Studies have demonstrated the varied impact of PMT constructs on user experiences across different domains. For instance, Zhao et al. (2018) emphasised that perceived vulnerability and severity significantly influence middle-aged and other users' engagement with mobile services. Shakela and Jazri (2019) assessed user experience and the ability to detect spear phishing attacks using PMT, focusing on vulnerability and user awareness. Likewise, Mat Dawi et al. (2024) confirmed that enhancing the user experience in online shopping platforms boosts perceived behavioural control. A seamless and satisfying experience can reinforce them and increase online purchase behaviour. Also, according to a study by Yang et al. (2020), organisational users, unlike home users, are more motivated to engage in protective behaviour to install password management due to a higher sense of accountability

and influence from IT officers, reflecting differences in response efficacy. Similarly, Tsai et al. (2016) reveal that internet users' security habits and response efficacy are influenced by perceived severity rather than susceptibility, which plays a vital role in their experience of online threats. Awareness alone was insufficient for protective behaviour, as those with more knowledge often feel overly confident, leading to lower intentions in their online safety measures in the future (Tsai et al., 2016).

According to Marikyan et al.'s (2022) study on PMT and blockchain adoption, user experiences and perceptions, perceived threat vulnerability, response cost, and self-efficacy positively influence users' intentions to adopt the technology, while perceived severity had no significant effect. The study suggests that future research should focus on qualitative studies to examine users' experiences and perceptions of blockchain utilisation. Oh et al. (2023) supported these findings, showing that invulnerability and self-efficacy contribute to blockchain acceptance, promoting transparency and adoption. Wang (2023) applies PMT to problematic streaming services use, demonstrating that perceived threats, such as serious negative consequences from overuse, can trigger users to experience fear and drive them to reduce their usage. This reduction is more likely when user believe their actions will effectively mitigate the threat (response efficacy) and have confidence in their ability to execute these actions (self-efficacy). However, the response cost of reducing usage does not significantly impact their motivation to change their behaviour. PMT suggests that knowledge influences decision-making, with perceived vulnerability being more influenced by one's perceived experience than actual knowledge or competence (Debb & McClellan, 2021).

3.7. Application of Protection Motivation Theory in Cybersecurity Practices

The application of PMT in cybersecurity practices emphasises its relevance in various recent studies (Dodge et al., 2023; Jamil, 2023; Skjelvik & Vestad, 2023). PMT constructs provide a deeper understanding of the factors influencing users' cybersecurity behaviours and willingness to adopt cybersecurity practices. However, specific factors that lead to improved cybersecurity practices remain unresolved, potentially leading to ambiguity. Ganesh et al. (2022) utilised PMT to develop a 2D persuasive game that educates users on smartphone privacy and security practices.

Also, Jamil et al. (2024) found that all PMT constructs, except threat susceptibility, are successful predictors of safe cyber practices, with increased cybersecurity costs negatively impacting these practices. Similarly, Shah and Agarwal (2020) found that smartphone users in India exhibited varying cybersecurity behaviours and practices. While some utilised common features such as screen locks, overall cybersecurity practices were inadequate, with many users either not adopting or unaware of technical measures such as encryption and remote wipe functions. Yeng et al. (2023) explored PMT constructs to enhance phishing prevention, emphasising the importance of ethical measures to combat deceptive practices.

Furthermore, according to Kalhoro et al. (2021), cybersecurity awareness and training help employees prepare for social engineering attacks, with self-efficacy being strongly linked to confidence in performing security behaviour and cyber hygiene practices. Ophoff and Lakay (2019) investigated computer users' motivation to adopt security measures against ransomware using PMT, finding that perceived threat severity and vulnerability do not directly influence protection motivation. Still, fear and self-efficacy significantly influence coping appraisal. Similarly, Kim et al. (2024) argued that AI self-efficacy can enhance organisational cybersecurity practices by reducing workload-related effects on behaviour. They recommend an interdisciplinary approach to AI self-efficacy training as part of cybersecurity strategies. Roberts and Rahman (2021) examined how digital native status influences security decision-making. They found that self-efficacy and response efficacy significantly impact antivirus software usage intentions, and they recommend effective training programs to improve them. PMT factors affect employees' anti-malware behaviour intentions, with coping appraisal being more predictive than threat appraisal. Response costs may be a barrier, while response efficacy is the key facilitator (Blythe & Coventry, 2018).

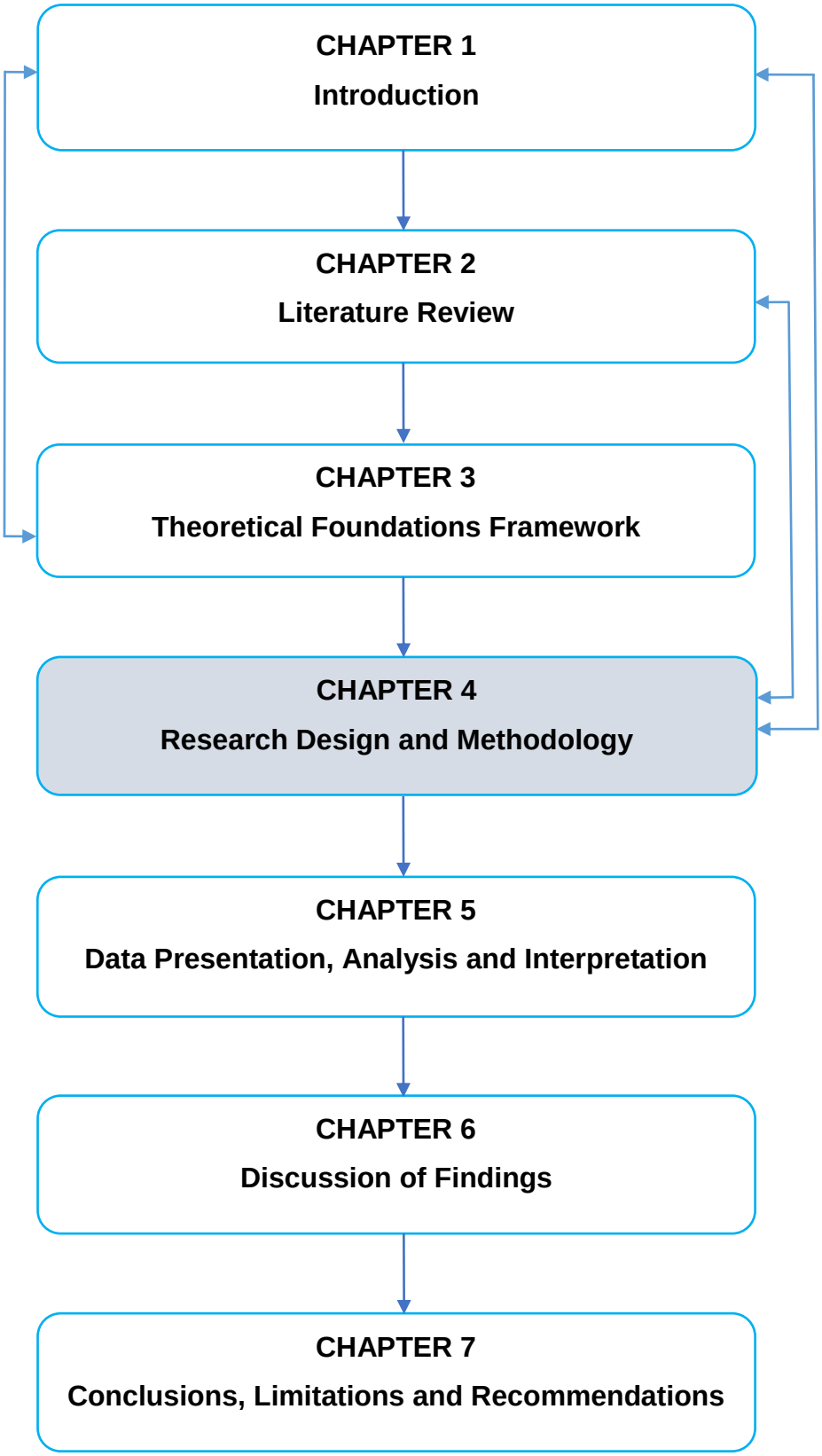
In a study in Malaysia, Humaidi and Alghazo (2022) applied PMT constructs, finding that security awareness influences employees' psychological factors, leading to better cybersecurity practices. Jamil (2023) explored cybersecurity practices in Australian microbusinesses, revealing that PMT significantly predicts user intention to avoid cyber incidents, with prior knowledge and experience playing critical roles in adopting cybersecurity practices such as installing Password Manager Software in their businesses. Tian (2024) focused on password manager adoption, highlighting that web self-efficacy and perceived risk directly impact trust in these tools. According to

Skjelvik and Vestad (2023), in a qualitative study on cybersecurity practices in Norwegian municipalities, they found low self-efficacy and response efficacy among employees, with recommendations to increase knowledge and improve cybersecurity practices through better education and shared understanding of risks. Likewise, Dodge et al. (2023) investigated user motivations for adopting cybersecurity practices; greater perceived severity and vulnerability positively affect these intentions, and users with low self-efficacy feel helpless and avoid cybersecurity practices, while those with high self-efficacy may be overconfident and ignore IT recommendations. They emphasise the importance of effective communication strategies, gamified simulation and personalised approaches to improving self-efficacy and reducing threat fatigue. This study further advocates for a user-centred approach, seeing users as contributors to organisational security, and recommends educating users about risks by sharing victim-impact stories to enhance user engagement (Dodge et al., 2023).

3.8. Conclusion

This chapter explained the Protection Motivation Theory (PMT) and its valuable insights into factors influencing e-commerce platform users, such as perceived vulnerability, threat severity, self-efficacy, and response efficacy, to improve cybersecurity practices for practical users' experiences in e-commerce. It advocates for multi-layered approaches to strengthen cybersecurity practices and behaviours. Also, PMT is essential to understanding the protective behaviours of e-commerce businesses and users. Research can focus on using PMT and fear appeal in the context of actual victims to gain insights into user acceptance of protective measures, especially those involving blockchain or Fintech technologies. While most studies on PMT constructs employed quantitative methods, there is a need for mixed methods research to understand better participants' perceptions and experiences of these constructs, particularly in the context of e-commerce. Similarly, there is a lack of recent studies that specifically assess the impact of cybersecurity practices on the experiences of e-commerce platform users using Protective Motivation Theory. The next chapter presents in detail the research design and methodology used for this study.

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY



4.1. Introduction

This study intended to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha. Chapter 3 discussed protection motivation theory as a theoretical foundation framework and its application to cybersecurity, privacy, cybersecurity practice, user experiences and e-commerce for this study. In this chapter, the research methodology that guides this research's aim will be presented. It elucidates various sections of research methodology using the Research Onion Model by Saunders et al. (2023).

4.2. Research Methodology

Research methodology is a systematic approach and research process applied in addressing research problems by collecting, analysing and interpreting data for scientific investigations (Creswell & Creswell, 2023; Saunders et al., 2023). It specifies the research design, which serves as an outline for conducting the research, including sampling, data collection tools and analysis techniques (Creswell, 2021; Roestenburg et al., 2021). The choice of research methodology employed in this research dependent on the research inquiries, required data for the research study and specific research problem intended to be addressed (Abdelhakim & Badr, 2021; Creswell, 2021). The researcher needs to consider the nature of data needed to decide whether to employ qualitative, quantitative or mixed methods, which can be informed by existing literature and the research problem (Creswell, 2014; Greenfield & Greener, 2016). The research objective and questions for this study requires the researcher to collect quantitative and qualitative data from e-commerce platform users in the public internet café in Gqeberha. Therefore, this study utilises an explanatory sequential mixed methods design based on its scientific inquiry. Further, this study research methodology is derived from the Research Onion Model (ROM) developed by Saunders et al. (2023). The Research Onion Model has been successfully employed by many researchers in information systems studies as a research process and framework to guide their research investigation (e.g. Alturki, 2021; Deshpande & Magerko, 2024; Mardiana, 2020). For that reason, the ROM is the research process that was employed to guide the explanatory sequential mixed methods research

design for this study, which represents a systematic and simple framework, step-by-step applied in solving the research problem. The researcher thoroughly explains the components of each research procedure in this chapter.

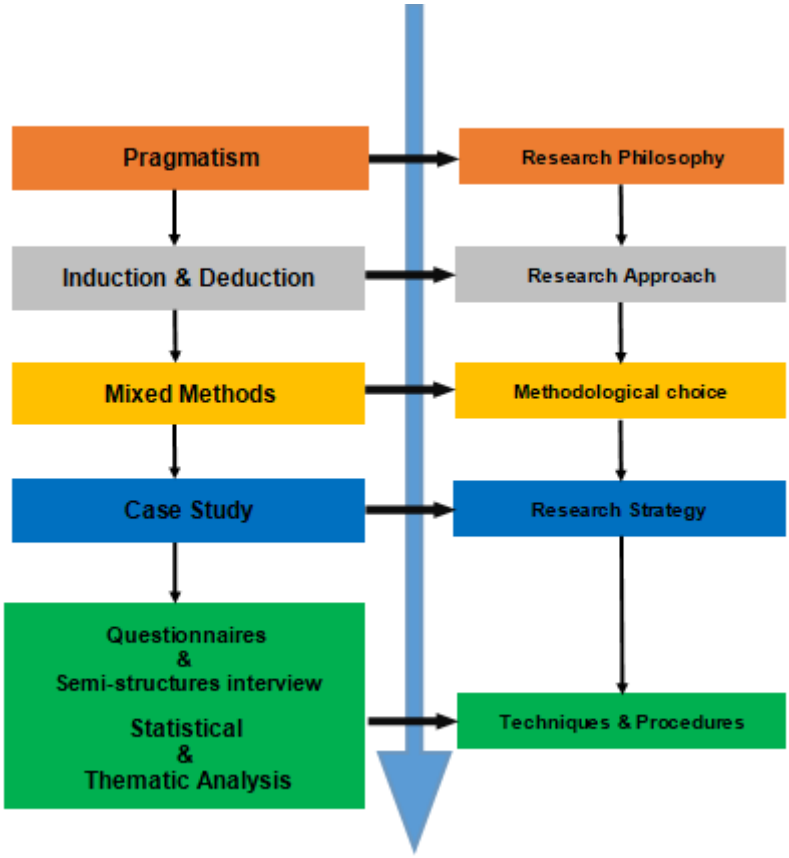


Figure 4.1: A mind map diagram for the research methodology chain derives from the ROM

4.3. Choice of Research Philosophy

Research philosophy is vital for academic inquiry as a foundational aspect that shapes the approach and methodological choice in a research study (Creswell, 2014; Mouton, 1996). The choice of research philosophy is based on the set of beliefs guiding the development of knowledge, which significantly has implications in the selection of methodology, which should be aligned with the research problems (Creswell, 2021; Roestenburg et al., 2021; Saunders et al., 2023). Some researchers reveal that knowledge development and worldview are shaped through the research philosophy lens. This philosophy informs their methodological choices and techniques, which can be either objective facts or subjective interpretation in the exploration of their research questions (Al-Ababneh, 2020; Creswell & Creswell, 2018). Common philosophical

types include Interpretivism, Critical Realism, Positivism and Pragmatism (Roestenburg et al., 2021; Saunders et al., 2023) (see Figure 4.1). However, research philosophies utilised in the majority of studies in information systems are Interpretivism, Positivism and Pragmatism (Alturki, 2021; Kankam, 2019).

4.3.1 Positivism

Positivism is a research philosophy that posits that reality is objective, which emphasises the use of scientific methods such as hypothesis testing or questions grounded in quantitative methods to generalise the study's findings in society (Alharahsheh & Pius, 2020; Junjie & Yingxin, 2022). Positivist science is philosophical stance often used in the social sciences, but it faces criticism for its reliance on scientific methods and social inquiry. Positivism is used by a researcher to quantify data, relying on statistical analysis to uncover patterns that govern social inquiry (Alharahsheh & Pius, 2020; Junjie & Yingxin, 2022). Some scholars argue that positivism is mismatched with social sciences, which have been superseded by other research philosophies like pragmatism and believe its impact has been overstated in methodological consideration (Corry et al., 2019; Roestenburg et al., 2021). In this study, evaluating cybersecurity practices and experiences of e-commerce platform users requires consideration of several issues which could not be fully captured with a postivist philosophy alone. It requires integrating qualitative insights with the positivist structure to fully comprehend users' perceptions and behaviours in public internet cafés, thereby enriching the study findings.

4.3.2 Interpretivism

Interpretivism is a research philosophy which focuses on understanding human behaviour and beliefs through the interpretation of meanings. Even though it is commonly used in the information systems field, interpretivism has its philosophical origins in other disciplines such as anthropology and philosophy (Corry et al., 2019; Junjie & Yingxin, 2022). The interpretivist philosophy highlights that human experiences and social contexts require interpretation that cannot be duly captured by using a positivist approach, challenging the use of positivism (Pulla & Carter, 2018;

Walsham, 1995). Interpretivist researchers claim that knowledge of reality and worldview can be socially constructed by individuals, which also influences how truth is interpreted (Al-Ababneh, 2020; Junjie & Yingxin, 2022). Interpretivism emphasises the significance of interpretation in understanding social phenomena and the subjective nature of knowledge, observing knowledge as relative and diverse, which is entangled with the researcher's view, while rejecting positivist notions of objective truth (Goertz & Mahoney, 2012; Hiller, 2016). The investigation of cybersecurity practices and experiences of online shoppers within the context of e-commerce and internet cafés is far from what users' abilities can handle due to the various cybersecurity risks they face daily. This approach enables the researcher to fully grasp how cybersecurity practices influenced e-commerce platform users' behaviours, perceptions and experiences in public internet cafés, which may be overlooked by the lens of positivism, to understand them deeply. However, the use of interpretivism also comes with its limitations, as it cannot be applied to generalise the research findings, which prompts the researchers to consider the use of pragmatism philosophy for this research inquiry (Hiller, 2016).

4.3.3 Pragmatism

Pragmatism posits that the use of a philosophical and methodological approach is appropriate in solving specific research problems (Allemang et al., 2022; Shook, 2023). Its philosophical foundation makes remarkable contributions by embracing a variety of methods in social sciences (Allemang et al., 2022; Morgan, 2014). Pragmatist philosophy posits that human actions are inseparable from their prior experiences, and those experiences originate in their beliefs. It also dissolves the idea of using older philosophical knowledge and suggesting that new direction is possible as human thoughts and beliefs are rooted in their consequences and actions (Goldkuhl, 2012; Kaushik and Walsh, 2019; Morgan, 2014). Pragmatism asserts that a researcher cannot determine reality for all at once in social science about the natural environment and rejects the idea that knowledge can be entirely abstract, dependent on habits, beliefs and experiences (Kamau, 2022; Morgan, 2014; Shook, 2023). Moreover, pragmatist epistemology posits that knowledge is rooted in human

experience, and the world perception of an individual is basically influenced by their common experience that exists to govern their actions (Goldkuhl, 2012; Kaushik & Walsh, 2019). Pragmatist epistemology does not perceive knowledge as reality but considers it a constructive purpose to cope with human existence as they participate in the world (Goldkuhl, 2012; Legg & Hookway, 2008). Pragmatist axiology emphasises the role of value-laden and moral considerations in research studies, influencing how research is conducted to benefit people and the knowledge being gained in the anticipation of the research inquiry, which influences the researchers' values and politics (Allemang et al., 2022; Kaushik & Walsh, 2019).

Pragmatism justifies the use of mixed methods as an acceptable methodological combination, emphasising that the appropriate method is one that effectively produces the consequences of the desired research inquiry and gives answers to the research problem (Allemang et al., 2022; Creswell, 2013; Kaushik & Walsh, 2019). As a result, studies have considered the flexibility of pragmatist philosophy in employing both qualitative and quantitative data in addressing research questions. For example, pragmatism allows researchers to utilise interviews and questionnaires or vice versa as their preferred methodological tools to address their research questions (Legg & Hookway, 2008; Morgan, 2014; Shook, 2023). Therefore, a pragmatist approach can be directly linked to mixed methods, which promotes its need in social sciences, allowing researchers to expand their view beyond interpretivist and positivist approaches. Pragmatism emphasises the practical implications of ideas and actions, enabling the researcher to vigorously engage with their world to change it rather than just observing it (Sharma et al., 2023).

This research utilised the PMT to assess the impact of cybersecurity practices on the experiences that online shoppers are confronted with, in the natural setting of a public internet café in Geqberha. The PMT was employed to guide the use of explanatory sequential mixed methods in this study. The use of pragmatism enables researchers to adopt explanatory sequential mixed methods, allowing for the collection of quantitative data in the first phase on e-commerce platform users' experiences and cybersecurity practices to capture the complexity of their challenges fully. During the second phase of qualitative research, the researcher will be able to gain an in-depth

insight into how these challenges affect individuals' behaviours, motivations and experiences in the adoption of cybersecurity practices in the e-commerce environment. A pragmatist approach enables the researcher to grasp these multifaceted issues and provide a recommendation on cybersecurity practices that can improve e-commerce platform user experiences in Gqeberha as they shop online in the public internet café setting.

4.4. Research Approach

A research approach refers to the method of conducting a research study, which contains the unequivocal stages for a research study and its purpose, the underlying role of a researcher and the method of data analysis (Creswell, 2014; Roestenburg et al., 2021). Studies highlight the uniqueness of each approach and its contributions in addressing the anticipated research problems to attain the research aims through their specific purposes (Creswell & Poth, 2016). The ROM recognises deduction, abduction and induction as the three research approaches as shown in Figure 4.1. These approaches will be explored in this section (Saunders et al., 2023).

4.4.1 Deduction

The deductive approach in research is a theory-testing process that begins by using existing theories, hypotheses or questions to confirm whether the theory applies to them in a specific instance. This approach applies a coherent flow from broad ideas to specific deductions by generalising its rules in specific cases (Bhattacherjee, 2012; Creswell, 2013; Saunders et al., 2023). The deductive approach uses theoretical propositions as the foundational facts for data collection and analysis. This approach is valuable for research results in order to generalise the reliability of the data. Furthermore, it effectively allows researchers to analyse the collected data through a predetermined framework (Clift et al., 2019; Habibi, 2021; Young et al., 2020). The deductive approach enables the researchers to employ appropriate instruments in the research study to address the research questions through the validation of existing theories (Clift et al., 2019; Habibi, 2021; Young et al., 2020).

4.4.2 Induction

In contrast, the inductive approach begins with the observations and seeks to establish the generalisation of the theory instead of commencing from a foundational theory (Bhattacherjee, 2012; Creswell and Poth, 2016; Habibi, 2021). This approach derives insights using raw data without pre-existing theoretical frameworks, aiming to summarise collected data to formulate meaning, patterns and themes in connection to the research aims and develop broad theories for the research findings (Creswell & Poth, 2016; Roestenburg et al., 2021). The inductive approach is particularly valuable for a qualitative researcher due to its flexibility and straightforward approach in the analysis of data that allows for providing an in-depth reliability and validity of research findings (Creswell, 2021; Creswell & Poth, 2016).

4.4.3 Abduction

The abductive approach complements both the inductive and deductive approaches in research inquiry, which involves an innovative inference to generate new hypotheses and theories grounded on recapitulating between deduction, induction and abduction to put together surprising evidence (Hobbs et al., 1993; Kennedy and Thornberg, 2018)**.** This approach proffers theory construction and promises knowledge creation in social science. The abductive approach is an alternative pragmatism that can be used for deductive or inductive reasoning when addressing a complex phenomenon (Hobbs et al., 1993; Paavola, 2015). One of the benefits of the abductive approach comes with its capability to handle uncertainty, which provides a balance between inductive and deductive methods for the development of theory and testing in qualitative and quantitative research, making it a multipurpose tool for researchers (Awuzie & McDermott, 2017; Brandt & Timmermans, 2021).

An abductive approach is used to complement both the inductive and deductive approaches in this study. The deductive approach is employed, guided by the PMT to focus on specific factors affecting cybersecurity practices and user experiences within e-commerce platforms in the natural setting of a public environment, such as an internet café. This helps to use PMT components to test the validity of the theory through the collection of empirical data from e-commerce platform users. Moreover,

the use of an inductive approach provided deeper, more insightful data to create themes and patterns on how e-commerce platform users' perceptions and experiences of cybersecurity risks and how these impact their cybersecurity practices in an internet café. Both approaches contributes systematically to the findings of this study.

4.5. Methodological Choice

As shown in Figure 4.1, this section delves into various research methodologies explained in ROM by Saunders et al. (2023). Methodological choices and research designs are vital aspects of social science research. However, literature presents multiple methods for research designs (Creswell & Creswell, 2023; Saunders et al., 2023). Methodological choice or research designs involves the consideration of quantitative, qualitative or mixed methods approaches, which are frequently established on the research background and discipline (Creswell, 2013; Leavy, 2017; Vogt et al., 2012). The methodological choice and research designs are vital when conducting a research project to have an effective outcome (Creswell, 2021; Leavy, 2017; Vogt et al., 2012). The selection of an appropriate research design by researchers should be carefully based on the research processes, including the problem statement, relevant literature, and research questions, which shape the analysis and data collection needed to provide a relevant outcome for the research investigation (Asenahabi, 2019; Greener, 2018; Hedrick et al., 1993).

4.5.1 Quantitative Design

According to Mohajan (2020), the quantitative research method uses numerical data and statistical analysis to investigate research phenomena. The research design in quantitative studies is primarily based on experimental and non-experimental designs, including observational studies, quasi-experimental designs, and experimental designs, each serving distinct purposes (Bloomfield & Fisher, 2019; Creswell, 2021; Stapor, 2020). The validity of the quantitative researches are linked to the main components such as experiments and questionnaires which characteristically include employing deductive reasoning for the formulation of hypotheses and identification of

variables to determine the size of data to be collected and analysed for a research outcome (Bloomfield & Fisher, 2019; Creswell, 2013; Price & Lovell, 2018).

4.5.2 Qualitative Design

The qualitative research method is central to understanding individual experiences, perceptions and social interactions through various data collection tools such as focus groups, interviews and observations by focusing on the exploration of quality rather than quantity of research phenomena (Creswell, 2021; Maxwell & Chmiel, 2015; Roller, 2020). Qualitative researchers make use of inductive and interpretative approaches to generate themes or meaning as it emerges through the data collection and analysis (Babchuk, 2019; Creswell, 2014; Nouri et al., 2018). The use of qualitative design enables researchers to capture people's feelings and thoughts to generate meaning that cannot be accomplished with the quantitative research method. The qualitative research method, however, has limitations in generalising the research findings due to the researcher's bias, subjectivity and smaller sample sizes (Bekele & Ago, 2022; Marshall et al., 2013; Mthuli et al., 2022). As emphasised by Kaushik and Walsh (2019), the appropriate research method is the one that addresses the research questions and problems. Therefore, this study opts for mixed methods design as its methodological choice.

4.5.3 Mixed Methods Design

In information system studies, mixed methods design is utilised by combining quantitative and qualitative approaches into a single study to provide a broader understanding to address the complex phenomena and make available relevant answers to the research problems or questions (Creswell and Creswell, 2023; Kaushik and Walsh, 2019; Kimmons, 2022; Wasti et al., 2022). It offers many benefits, including development, initiation, complementarity, triangulation and expansion of the research results, enriching the quantitative aspect with qualitative data (Creswell, 2021; Creswell and Creswell, 2018; Wasti et al., 2022). Sharma et al. (2023) emphasise that mixed methods design allows the examination of relationships amongst diverse variables, which cannot be possible with just a single research

design. Mixed methods design can improve research validity and reliability, providing a comprehensive view of scientific problems in social science (Creswell, 2021; Creswell & Poth, 2016). Creswell and Creswell (2023) highlight their core designs in social science, including explanatory sequential, exploratory sequential and convergent parallel designs (see Figure 4.2). Figure 4.2 demonstrates the three key types of mixed methods designs, which are determined by the study aim and time involved in employing two different data collection approaches.

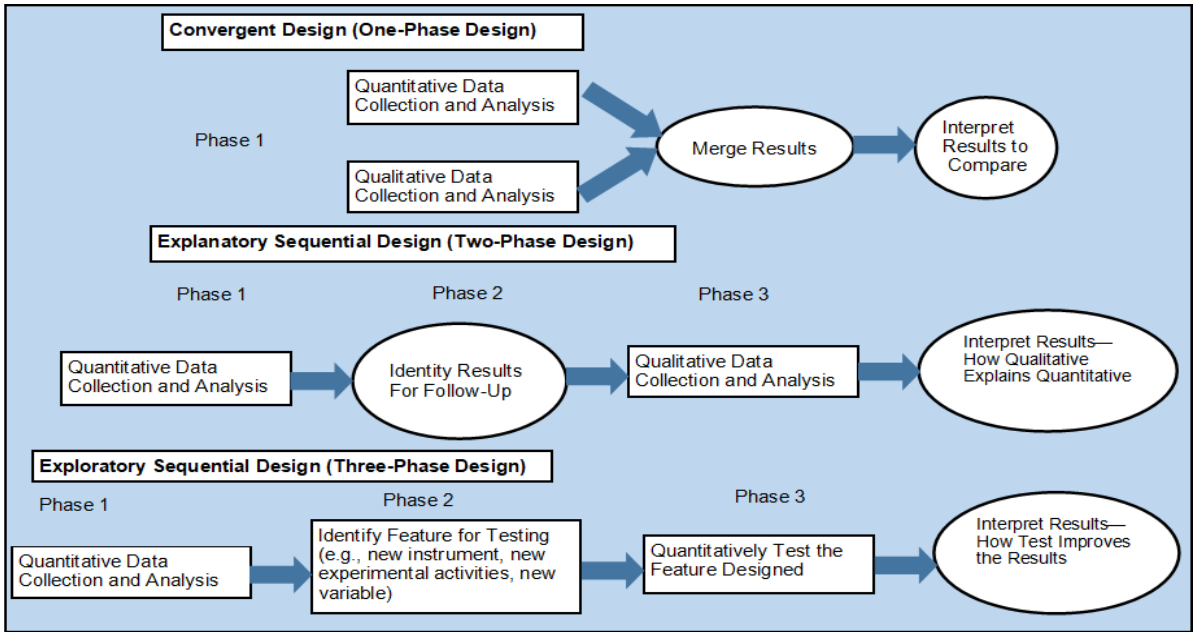


Figure 4.2: Core three mixed methods design adopted from Creswell and Creswell (2023)

Mixed methods design allows researchers to use both quantitative and qualitative approaches to answer the same research question with greater certainty, which broadens the inferences of the research conclusions. It justifies the combination of both closed-ended quantitative data and open-ended qualitative data, which can be of help in comprehending the research problem (Creswell & Creswell, 2023; Sharma et al., 2023). Mixed methods design enables the researcher to draw conclusions from the integration analysis for insight and interpretation, which frames their worldview and explanation drawn from the existing literature (Creswell, 2021; Creswell & Creswell, 2018). Creswell and Creswell (2023) emphasise that choosing the correct type of mixed methods is based on the primary research objective and problem that the researcher intends to solve, which informs the kind of data to be collected. This study intents to *use the PMT to assess the impact of cybersecurity practices on the*

experiences of online shoppers with e-commerce platforms in Gqeberha. Therefore, this study's aim and research questions informed the selection of proper mixed methods design to enable the researchers to acquire required data to attain the research study as illustrated in Figure 4.2 which was recommended by Creswell and Creswell (2023). As a result, the appropriate mixed methods design for this study was applied based on the research questions as shown in Table 4.1.

Table 4.1: Selection of appropriate design focused on the study research inquiries

Research questions	Required Data
1. What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?	Quantitative data (Questionnaire) Qualitative data (Interview)
2. How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?	Quantitative data (Questionnaire) Qualitative data (Interview)
3. How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?	Quantitative data (Questionnaire) Qualitative data (Interview)
4. What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping?	Quantitative data (Questionnaire) Qualitative data (Interview)

For this study to achieve the intended outcome of answering the research questions, it is important for the researcher to employ a explanatory sequential mixed methods design that enables the collection of quantitative and qualitative data from the e-commerce platform users in an internet café setting (Creswell, 2021; Toyon, 2021). Quantitative data on the impact of cybersecurity practices and the experiences of online shoppers' experiences in an internet café was collected and analysed first. After that, qualitative data was collected as a follow-up to the quantitative findings to gain further in-depth insight into the users' perceptions, motivations and experiences (Creswell, 2014; Creswell & Creswell, 2023). Thus, the selection of explanatory sequential mixed methods is suitable for this study (see Figure 4.3 and Table 4.1). Creswell and Creswell (2023) stressed that an explanatory sequential mixed methods design involves a two-phase data collection in which the researcher can collect quantitative data in the first phase, analysing results, while using the outcomes to build on for the next qualitative phase (see Figure 4.3). Figure 4.3 illustrates the explanatory sequential mixed methods design for this study.

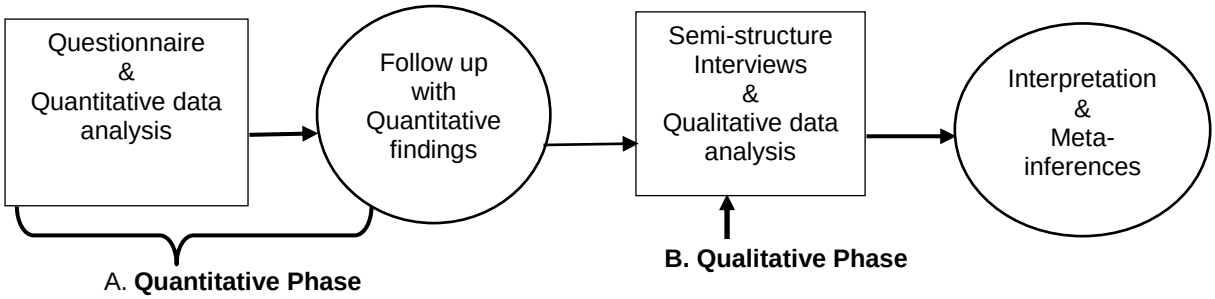


Figure 4.3: Explanatory sequential mixed methods design (Creswell and Creswell, 2023)

Moreover, an explanatory sequential mixed methods design is intended to elucidate initial quantitative results with qualitative data by joining two databases together (Creswell & Creswell, 2018; Kimmons, 2022). For example, the quantitative data may show unpredictable results that necessitate further exploration of qualitative data to discover the complexities that cannot be captured through the lens of numerical data alone. Creswell and Creswell (2018) emphasise that with explanatory sequential mixed methods, researchers can employ questionnaires in the initial phases, analyse the results, and then follow up with qualitative interviews to provide the best justification for unusual questionnaire responses. Thus, the combination of quantitative and qualitative data enriches the data analysis by linking statistical scores with individual experiences to develop a recommended solution that can enhance cybersecurity practices for e-commerce platform users in the public internet cafés environment in Gqeberha.

4.6. Research Strategy

The Research Onion Model clarifies the choice of research strategy that should govern a research methodology (Saunders et al., 2023). Research strategy refers to the plan of action to reach the research aim, which shows how the researcher will conduct the research questions to answer them (Saunders et al., 2023). It serves as a bridge between the researcher's philosophy and methodological choice for data collection and analysis (Roestenburg et al., 2021). The researcher's choice of research strategy is informed by the research aim and questions, which are coherently connected to the research approach, philosophy and purpose. It is guided by the required amount of time, scope of existing knowledge and availability of other resources such as data and potential participants (Alturki, 2021; Islam & Aldaihani, 2022).

Saunders et al. (2023) stress different strategies that could be employed within mixed methods design, such as case study, grounded theory, ethnography and action research. However, this study used an explanatory sequential mixed methods design to investigate e-commerce platform users' experiences and cybersecurity practices in Gqeberha, making it suitable for a case study. A case study offers an opportunity to investigate real-life situations to provide rich interpretation and analysis when limited knowledge of the setting of the phenomenon studied is available (Yin, 2018, 2014). Case studies are widely employed in social sciences to provide an in-depth understanding of a case's process and interactional dynamics within a unit of study, which is restricted to a certain study population. One of the advantages of a case study is that it permits researchers to use various data collection techniques and data sources to support the reliability of the research data (Harrison et al., 2017; Remenyi, 2022; Yin, 2018). This study employed an explanatory sequential mixed methods design to assess the impact of cybersecurity practices on the experiences of online shoppers in the e-commerce platforms guided by the PMT. This design is methodically chosen to address the research questions and offer an actionable solution for cybersecurity practices that can improve online shopping experiences in e-commerce. Therefore, the following sections will delve deeply into the population and sampling techniques for this study in Gqeberha.

4.6.1 Study Population, Sample Sizes and Sampling Techniques

4.6.2 Population

Population is defined as the entire group of subjects or objects for the research inquiry as the central focus of the study investigation (Asiamah et al., 2017; Hossan et al., 2023; Willie, 2024). The concept of population is vital for differentiating between the general, accessible and target population to ensure a smooth sampling and generalisability of study findings (Hossan et al., 2023; Willie, 2024). Moreover, the target population is described as a group of individuals or participants to which the study will be generalised by the researchers (Rahman et al., 2022). This research target population includes e-commerce platform users who are relying on the internet cafés for their online transactions from the selected three internet cafés in Gqeberha,

Eastern Cape, namely: Internet café A (North End), Internet café B (Central), and Internet café C (North End) (SA Experience, 2024). It comprises individuals aged 18 years and above with diverse educational backgrounds, who meet the study's criteria of concern to the researcher, enabling the generalisation of the study investigation.

According to Asiamah et al. (2017), population specification is essential for quantitative and qualitative studies; however, each study require samples of varying sizes. Moreover, quantitative research requires a large number of respondents to ensure the generalisability of the research outcomes, whereas qualitative research typically involves a few participants to provide in-depth insights and perceptions regarding the research inquiry (Creswell & Creswell, 2023, 2018; Willie, 2024). The same target population of e-commerce platform users who frequently use public internet cafés in Geqberha applied for this research project with different samples, sampling techniques and data collection and analysis (Creswell, 2021; Flick, 2018; Hossan et al., 2023). Table 4.2 outlines the target population, sampling techniques, sample size, data collection and analysis for quantitative and qualitative phases for this study, which will be covered in detail in the next section. Thus, this study applies the term *respondents* for the quantitative phase and *participants* used for the qualitative phase (Mason et al., 2021; Toyon, 2021).

4.6.3 Sampling Technique and Dimensions

As suggested by Andrade (2020) and Lakens (2022), the sampling technique for a research investigation should be determined by the sample population, data type and sampling size required for the research objective.

Sampling involves selecting a representative sample from an entire population to gain insights into a broader phenomenon. The unit of study is a sample subset chosen from a sample size of the population for investigation (Rahman et al., 2022; Saunders et al., 2023). Sampling is vital in research due to the difficulty of collecting data from an entire population. The sample size is based on the ideal number of valid inferences (Sharma, 2017; Taherdoost, 2016). Andrade (2020) and Lakens (2022) emphasise that proper sampling methods and adequate sample size ensure representative, enabling generalisation of the conclusions to the entire population. This study aims to

assess the impact of cybersecurity practices on the experiences of online shoppers in e-commerce in Gqeberha and recommend cybersecurity practices perceived by e-commerce platform users. To attain this, Table 4.2 shows the sample size for the quantitative and qualitative phases of this research study.

Table 4.2: Quantitative and Qualitative Phases for this Research Study

Item description	Quantitative phase	Qualitative phase
Population	Online shoppers in internet cafes	Online shoppers in internet cafes, same as in the quantitative phase
Sampling of Sites	Random	Random
Sample size of sites	N= 3	N= 3, same as in the quantitative phase
Sample size	88 to 100 respondents	4 to 10 participants
Sampling technique	Probability sampling	Purposive Sampling
Data collection instrument	Questionnaire	Semi-structured Interview guide
Data analysis	Descriptive and inferential statistics with SPSS	Thematic analysis with Atlas.ti
Rigour	Validity and reliability	Trustworthiness

4.6.3.1 Population and Sampling Method for the Internet Cafés

In this study, the City of Gqeberha has more than six internet cafés. Purposive sampling was used to select three internet cafés that are strategically positioned in busy areas for the data collection. Purposive or judgmental sampling is a non-probability sampling method used in both quantitative and qualitative research. It involves the intentional selection of participants based on the researcher's knowledge or judgement (Hossan et al., 2023; Sharma, 2017). These internet cafés cater to a diverse range of clients, who patronise them for their daily activities. Internet café A (North End) serves lower-income households, job seekers and students who rely on its services. Internet café C (North End) is the busiest café located at the commercial sites, attracting mixed demographics such as students, working professionals and others. Moreover, Internet café B (Central) is located at the centre of town, serving students, small businesses, job seekers and other clients. These internet cafés receive 60 to 80 clients per month, who always visit them for their day-to-day activities. The selection of these cafes enable the researcher to capture a broad range of individuals using their services for online transactions; to gain insight into their experiences, cybersecurity practices and cybersecurity threats encountered in the public internet café environment in Gqeberha. Therefore, the sampling method for quantitative and

qualitative research will be discussed next in this section, which shows how it is utilised in those three selected internet cafés introduced above.

4.6.3.2 Sampling Method for the Quantitative Phase

Probability sampling techniques are used where the population size and location are known, with an accurate chance of selecting the sample at least once (Sharma, 2017; Taherdoost, 2016b). According to Bhattacherjee (2012), probability samplings have two attributes. Firstly, every entity in the population has a non-zero chance of being chosen. Secondly, it involves a random selection. Each entity in the population has an equal opportunity to be selected (Rahman et al., 2022; Sharma, 2017). In the quantitative phase, random sampling was used to target the population, which includes individuals visiting the three Internet cafés monthly in Gqeberha: Internet café A (North End), Internet café B (Central), and Internet café C (North End). As explained in section 4.6.3.1, the internet managers/owners provided list of clients received on a monthly basis, which was used to calculate number of clients using sample size formular (See Table 4.3). So, the study used a sample size of 88-100 respondents, calculated using the sample frame table to ensure an appropriate number of internet café users. (see Table 4:3). Quantitative data were collected from respondents using a self-administered questionnaire with closed-ended Likert Scale questions.

Table 4.3: The sample frame

Name of Internet Cafés	No of clients	No of respondents	Percentage
A	60	51	30.0
B	60	51	30.0
C	80	68	40.0
Total	**200**	**170**	**100**

The sample size was calculated using the formula below, where:
n = sample size of adjusted population
N = population size
e = accepted level of error set at 0.05

$$n = \frac{N}{1+N\,(e)^2}$$

$$n = \frac{165}{1+165\,x\,(0.05)^2}$$

$$n = 170 \,/\, (1 + 170x(0.05)^2$$

= 170 / (1+1.13)
170/2.13

Sample size (n) = 80

The sample size should be, however, increased to 10% to leave room for non-response (n= 80+8 = 88)

4.6.3.3 Sampling Method for the Qualitative Phase

The purposive sampling technique was utilised to select between four and ten participants in the qualitative phase, and data saturation was used to determine the sample size (Braun & Clarke, 2021a; Stake, 2013). Purposive sampling relies on the researchers' judgment to purposefully select the participants based on the study criteria (Saunders et al., 2023; Sharma, 2017). Using purposive sampling techniques, participants from the initial sample was chosen from the quantitative phase for in-depth interviews to gain insight into their perceptions and behaviours with cybersecurity practices on e-commerce platforms in Internet cafés (Creswell and Creswell, 2023, 2018). Participants were informed during the questionnaire phase that they were contacted for a follow-up interview, and this contact occurred separately via email and over the phone. One-on-one interviews were conducted face-to-face using phone device. Moreover, qualitative studies stress the importance of the researcher finding the individuals who can enrich and provide valuable insights into the study phenomenon (Bhattacherjee, 2012; Creswell, 2013). This method allows the researcher to understand the phenomenon by interpreting participants' meanings using various data collection techniques to develop words that make a theoretical contribution (Creswell, 2013; Creswell and Poth, 2016).

4.7. Data Collection Techniques and Procedures

According to the ROM by Saunders et al. (2023), techniques and procedures constitute the final layer of the research process, which explains the data collection as illustrated. Data collection is the process of gathering participant information systematically when conducting a scientific inquiry. Studies explain many types of data collection procedures, namely observation, interviews, focus groups, and questionnaires that a researcher can utilise to gather and collect data in a research investigation (Creswell & Creswell, 2018; Roestenburg et al., 2021; Saunders et al., 2023). This study employed an explanatory sequential mixed methods design to examine the research objective. This study used a questionnaire for quantitative data and semi-structured interviews for qualitative methods as its data collection instruments (Creswell & Creswell, 2018; Roestenburg et al., 2021). The next sections

on data collection phases for explanatory sequential mixed methods design cover the data collection techniques for this study in greater detail.

4.7.1 Data Collection Phase for Explanatory Sequential Mixed Methods

The data collection techniques start with designing instruments to gather raw data or selecting appropriate databases aligned to the research objectives. This study utilised questionnaires and semi-structured interviews, which will impact the process of creating the data collection instruments (Ponto, 2015; Toyon, 2021). The development phase of questionnaires is essential in data collection techniques. At the same time, an interview involves a sequence of prepared questions derived from questionnaire instruments, which are designed to stimulate answers and information from the individuals. Interviews allow the researchers to pose key questions, which can either occur face-to-face or over the phone (Ponto, 2015). Also, scholars stress the significance of structural consistency in sequence, structure, techniques and content throughout the data collection in answering research questions. Therefore, questionnaires are compared to the standardised interview in which the quality of its standard is vital for the reliability of the research inquiry, which can include structured and open-ended questions to extensively address the study objectives (Creswell & Clark, 2017; Creswell, 2021; Ponto, 2015). As depicted in Figure 4.4, the workflow of the explanatory sequential mixed methods design, adapted from Toyon (2021), is employed in this study. This approach shows the structures of data collection and analysis, integrating and reporting to ensure a seamless conversion from the quantitative phase to the qualitative phase. This design workflow ensures a clear transition for this study to facilitate the integration of the research outcomes to provide an in-depth assessment of the PMT and how it influences cybersecurity practices and e-commerce platform users' experiences within e-commerce on public internet café settings.

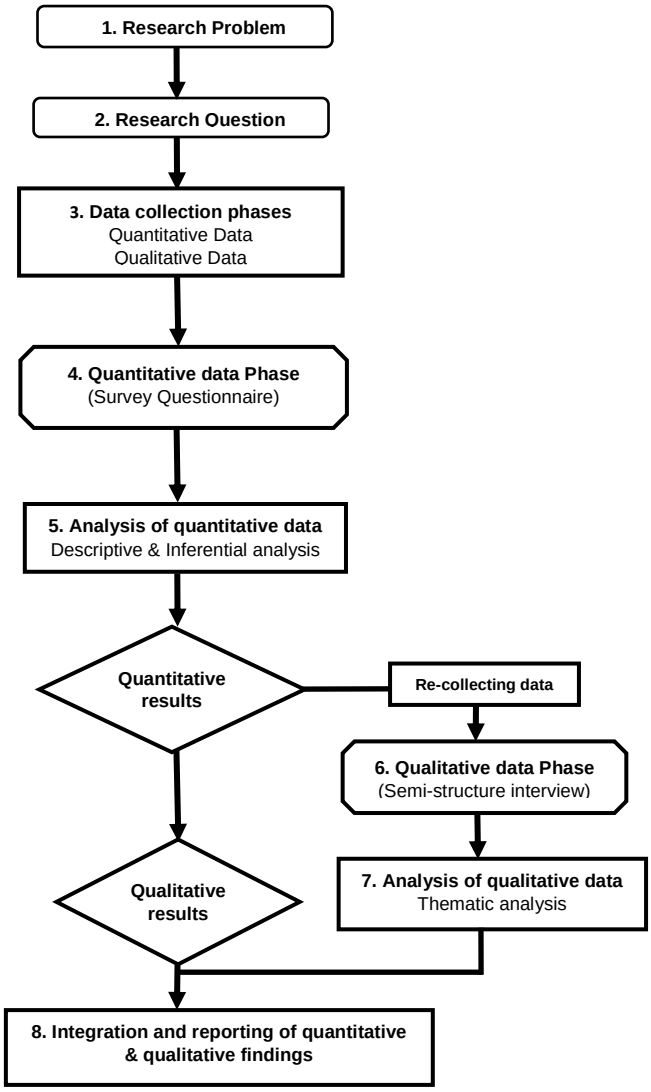


Figure 4.4: Workflow of explanatory sequential mixed methods design adapted for this study from Toyon (2021)

4.7.2 Questionnaire Data Collection Techniques

Questionnaire methods are frequently utilised by researchers in social science to reach and collect quantitative data from their target respondents (Roopa & Rani, 2012; Toyon, 2021). According to Taherdoost (2022), a questionnaire is an essential tool based on a set of questions that enables researchers to gather data on beliefs, attitudes and preferences from larger populations. An appropriate design of a questionnaire aims at obtaining statistically useful information and precisely reflecting the respondents' opinions (Taherdoost, 2022b; Timmins, 2015). The main steps for designing an effective questionnaire include defining the research objectives, selecting the right questions, types, and using the correct wording (Taherdoost, 2022b;

Thwaites Bee & Murdoch-Eaton, 2016). The length, structure, and presentation of the questionnaire may have a substantial effect on the response rate and data quality. The questionnaire design, such as format and layout, requires careful consideration, which needs expertise for pre-testing and piloting to avoid common pitfalls, potential issues, and ensure reliable results (Taherdoost, 2022b; Thwaites Bee and Murdoch-Eaton, 2016). The core advantages and disadvantages of a questionnaire are discussed in the following section.

4.7.2.1 Advantages and Disadvantages of the Questionnaire Method

The advantages and disadvantages of the questionnaire method are covered below in Table 4.4.

Table 4.4: Advantages and disadvantages of the questionnaire method

Advantages	Disadvantages
• One advantage of questionnaires is the response efficiency and cost-effectiveness for collecting a large amount of information (Meirte et al., 2020). • Questionnaires offer the benefits of accessing a wide geographic coverage, groups and individuals who share specific interests, attitudes and values regarding research issues, problems and activities (Mazikana, 2023; Taherdoost, 2022b). • Questionnaires can yield the right response that can be easily tabulated or scored, resulting in data analysis when containing items with choices to be checked (Patten, 2016; Wright, 2005). • Questionnaires are also useful for the collection of information that involves sensitive matters. It can be anonymously administered to encourage respondents to be sincere in their response (Fife-Schaw, 2020; Price & Lovell, 2018).	• Studies have asserted that questionnaires may be swayed by social-desirable responses from the respondents (Meirte et al., 2020; Patten, 2016; Rice et al., 2017). • The respondents may give responses which they think are socially desirable but may not be fully true (Patten, 2016; Rice et al., 2017). However, making the response anonymous can reduce the effect of social desirability (Patten, 2016). • Another disadvantage of questionnaires stems from the short-answer and multiple-choice items, with restricted responses that do not give enough room to obtain in-depth information from the respondents (Meirte et al., 2020; Wright, 2005). • The response rate to questionnaires is often low, especially if they are mailed to potential respondents who do not know the researcher. However, researchers can expect a higher response rate when contacting potential respondents by telephone or in-person distribution (Mazikana, 2023; Patten, 2016; Taherdoost, 2022b).

4.7.2.2 Step-by-Step Process for the Questionnaire Design and Pilot-Testing

Scholars suggest steps that the researcher can follow to develop a standardised questionnaire for a research study (e.g. Roopa & Rani, 2012; Taherdoost, 2022).

Figure 4.5 depicts the sequence of steps that the researcher follows for the development and validation of the questionnaire for this research.

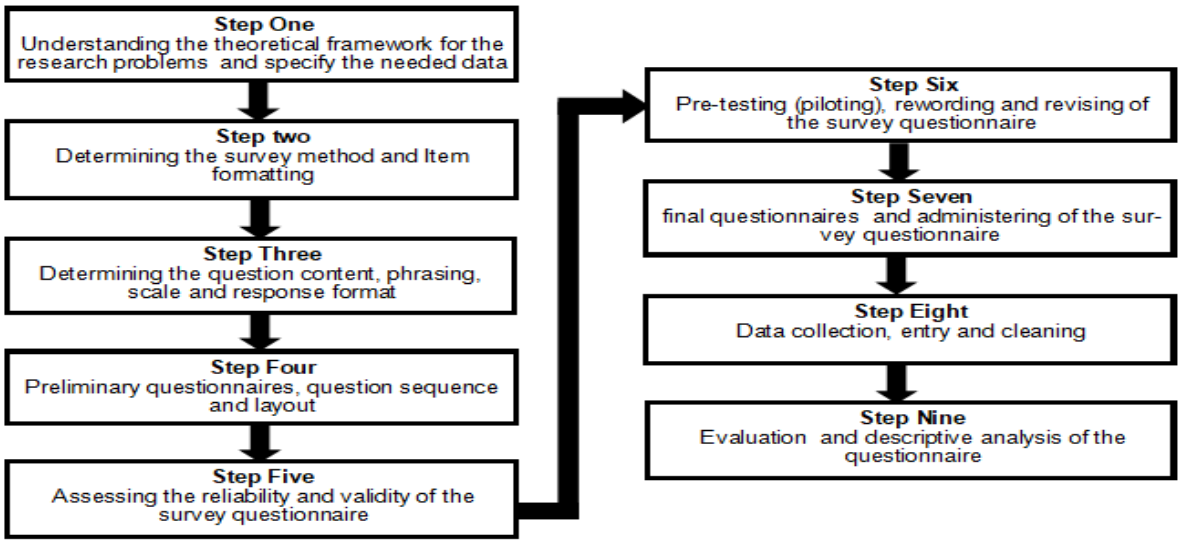


Figure 4.5: Step-by-step development of questionnaire for this study, adapted from Kishore et al. (2021) and Roopa and Rani (2012)

The use of a questionnaire in this study enables the researcher to reach a large audience on cybersecurity practices and experiences within e-commerce platforms in an internet café setting. The developmental process of the questionnaire is guided by this study's objective and research questions, as cited in Chapter One. The questionnaire consists of four sections, as shown below in Table 4.5.

Table 4.5: Structure of the Questionnaire

SECTION A **Demographic information**	**Purpose:** This section is intended to obtain information pertaining to e-commerce platform users' background, shopping platforms and experiences **Research Questions:** This section will answer part of the research questions for this study
SECTION B **Perception of cybersecurity threats and risks when shopping online in an internet café**	**Purpose:** This section is intended to use PMT to assess perceived cybersecurity threats among e-commerce platform users and how they influence their online shopping behaviour in an internet café setting **Research question**: This section will answer research question 1
SECTION C **Awareness of basic cybersecurity practices and measures when shopping online in an internet café**	**Purpose:** This section is intended to use PMT to assess the basic cybersecurity measures/practices among e-commerce platform users, and how it affects their satisfaction and shopping experience in an internet café **Research Question:** This section will answer research question 2
SECTION D **Perceived effectiveness of cybersecurity practices**	**Purpose:** This section is intended to PMT assess the perceptions of cybersecurity threats and effectiveness of cybersecurity practices among e-commerce platform users in an internet café environment and provide recommendations on cybersecurity practices **Research Question:** This section will address research questions 3 and 4

The researcher follows steps one to four to guide the development of the questionnaire for this study (See Figure 4.5). The questionnaire were sent for face validity to ensure the logical flow of the questionnaire layout and items. In addition, it was assessed for construct validity to ensure the items are currently grouped under intended constructs for this research study. Content validity was conducted on the questionnaires to ensure all key concepts are covered. Furthermore, a statistician was asked to assess the items and measurements in the questionnaires. The questionnaires was piloted (or pretested) to minimise any shortcomings of ambiguous items and the instruments. Feedback was used to revise, rephrase and improve redundant items on the questionnaire.

4.7.3 Data Collection for the Quantitative Phase

The researcher distributed a self-administered questionnaire with closed-ended Likert scale questions for 100 e-commerce platform users in three Internet cafés: Internet café A (North End), Internet Café B (Central), and Internet café C (North End) in Gqeberha (Tsoai and Chipunza, 2022). The questionnaire is adapted from the Security Behaviour Intention Scale (SBIS) by Egelman and Peer (2015). The adapted questionnaire contains key PMT constructs such as threat appraisal, response efficacy, response cost and self-efficacy to assess the participants' cybersecurity practices and experiences. The SBIS was successfully used by Van Bavel et al. (2019) to evaluate online security behaviours like choosing strong passwords, security awareness, and protection against attacks. The SBIS has basic security questions on protection techniques. The questionnaire was distributed in-person/face-to-face to the respondents to answer the questions. Section 5.2.2 and Table 5.1 provides detail of the distribution method for this study (Ponto, 2015; Toyon, 2021). The questionnaire was anonymous designed to encourage honest responses. Respondents received brief guidance on how to access the questionnaires to ensure private, independent responses and enhance data reliability.

4.7.4 Quantitative Data Analysis

In the quantitative phase of data analysis, statistical methods were utilised to process the collected data, which help to organise and provide quantitative results. This study

utilises Statistical Package for the Social Sciences (SPSS) version 29 to analyse the quantitative data. The result were presented in descriptive and inferential statistics such as frequencies and charts (MacRae, 2019; Toyon, 2021). Descriptive statistics are mathematical techniques utilised to summarise and describe datasets through numerical facts, tables or graphics to provide guidance for advancement in science and addressing societal problems (Lee, 2020; Sharma et al., 2018). Inferential statistics are vital for making inferences and generalising findings from samples to populations (Stapor, 2020). The use of descriptive and inferential statistics enabled the researcher to summarise and analyse questionnaire responses on cybersecurity perceptions, practices and experiences among e-commerce platform users in an internet café (Dong, 2023; Lee, 2020).

4.7.5 Validity and Reliability of the Questionnaire

Scholars specifically highlight the significance of addressing data validity and reliability issues in explanatory sequential mixed methods, emphasising strategies to enhance research quality through the use of multiple data sources and collection methods (Creswell & Creswell, 2018; Noble & Smith, 2014). Explanatory sequential mixed methods utilise quantitative and qualitative data collection techniques, allowing triangulation to enrich data validity and reliability in a research study (Creswell and Creswell, 2023; Ganji et al., 2017). Meanwhile, Toyon (2021) emphasises that the main approach to achieve validity and reliability in a quantitative study is to utilise an appropriate questionnaire design which can accurately measure, recognise and investigate the research inquiry. Researchers can address the issue of validity by ensuring a sample's representativeness (Toyon, 2021). Quantitative researchers explain the different types of validity tests, namely: internal validity, face validity, construct validity and external validity, which can be used to enhance quantitative data and questionnaire design (Saunders et al., 2023, 2019; Toyon, 2021). Internal validity is linked to a positivist study that validates the degree of change in the dependent variable that is ascribed to the independent variable. This tests the causal relationship of how these variables can have a statistical significance on the research output in quantitative studies (Cahit, 2015; Cook & Rumrill, 2005). Face validity is utilised in quantitative studies to evaluate the logical flow of the questionnaire accurately and

scales that the researchers intended to achieve the research investigation (Allen et al., 2023; Downing, 2006).

Moreover, construct validity is used in a questionnaire design to test the extent of psychological measurement, by setting a set of questions to measure the presence of the intended construct accurately. It entails the theoretical connections between the constructs and their measures (Piedmont, 2023; Stone, 2019; Trafimow, 2022). External validity explains how the generalisability of research findings can be applied to wider populations and other contexts (Saunders et al., 2023). Reliability tests are an essential aspect that ensures the stability of the measurement of research outcomes, and can reproduce the same results when put under constant conditions (Heale and Twycross, 2015; Sadık, 2019). Moreover, some social science researchers argue that common method variance (CMV) is a significant threat to research validity (Craighead et al., 2011; Tehseen et al., 2017). Rodríguez-Ardura & Meseguer-Artola, (2020) stressed that potential issues of CMV in the questionnaire's design are recognised when the assessable link between one construct or another has been overstated and put differently. To address this, studies encouraged the use of a mixed methodological strategy for CMV, recommending that researchers should apply preventative remedies (ex-ante) in the early stage of questionnaire design, in combination with the use of post-hoc techniques (ex-post statistical techniques) (Rodríguez-Ardura and Meseguer-Artola, 2020; Wall et al., 2022).

4.7.6 Feedback from an Expert and Pilot Questionnaires

The researcher incorporates ex-ante techniques in the early stage of the questionnaire design, which was also designed in line with the study objective and research questions. The questionnaire was assessed with the assistance of an expert for validity; some questions and items were restructured based on the expert feedback to enhance the clarity and logical flow of the questionnaire and minimise response biases (Baumgartner & Weijters, 2021; Malhotra et al., 2017). Furthermore, the questionnaire was administered to a small group of six e-commerce platform users with extensive shopping experience (four users have 6 to 10 years of experience across multiple platforms, and two users have less than 1 year of experience on a single platform). All

participants expressed satisfaction. However, some changes were made based on their recommendations. The final questionnaire was reworded based on the feedback to ensure the respondents clearly understand the instructions and can correctly answer the questions under the specified conditions. In addition, the design of questionnaire was anonymous to enable respondents provided honest answers, feel safe, and minimise common method variance (CMV).

4.7.7 Qualitative Phase of Semi-Structured Interviews

This phase, as suggested by Toyon (2021), is the next phase determined by quantitative results. It involves recollecting and compiling qualitative data through interview methods to gain further insight and comprehend the influence of cybersecurity practices on e-commerce platform users' experiences, perceptions, and beliefs about the study inquiry. The advantage of the interview method is that it allows researchers to acquire in-depth insights from participants through personal interaction, which can further produce meticulous information and analysis for the study outcomes (Creswell & Clark, 2017; Toyon, 2021; Yin, 2018). The participants were invited from the initial quantitative samples for an in-depth interview to comprehend their behaviours and perceptions on cybersecurity threats and cybersecurity practices within the e-commerce platforms in the internet cafés setting. The quantitative results were used to guide the development of an interview guide by adopting a funnel approach, starting from broad to specific questions to further examine the emerging scores in greater depth for this research investigation (Roller, 2020).

Participants were notified about the potential follow-up interviews in the initial questionnaire phase. Subsequent contact were made over the phone. Interviews were conducted in person and over the phone, with participants' responses securely recorded using a recording app. Before each interview session, participants were briefed on the purpose of the study and provided with the informed consent form. A sample of 7 participants were interviewed, with the final number determined by data saturation (Braun & Clarke, 2021a; Stake, 2013). Data saturation is the point at which no new codes or themes emerge from the data collection and analysis (Braun & Clarke, 2021a). However, there is no minimum threshold required for data saturation,

as scholars argue about the number of participants to achieve it. For example, Corbin and Strauss (2008) stress 5 participants while Stake emphasises the use of 4-10 participants (Stake, 2006, cited in Mthuli et al., 2022). In fact, Braun and Clarke (2021) accentuate that data saturation can only be achieved through data quality, depth and engagement with the collected data. Hence, this study follows Braun and Clarke, who say that meaning or theme is not innate or self-evident during data collection; instead, they result from deliberately conducting analysis aimed at developing an interpretation (Braun & Clarke, 2021a; Rahimi & Khatooni, 2024).

4.7.8 Qualitative Data Analysis

Qualitative analysis is the process used to classify and extract meaningful data from the textual information to identify patterns and themes (Brooks et al., 2018; Graue, 2015; Tenny et al., 2017). Graue (2015) and Noble and Smith (2014) reveal that qualitative researchers typically work with textual, audio-visual and documentary data, transcribed to identify patterns and themes related to the identified code. Moreover, Braun and Clarke (2021b, 2021c) posit that themes are recognised across the collected data set concerning research questions. Theme development is closely tied to the coding process, with themes emerging from it. The coding procedure is unstructured and organic, allowing code to evolve as the researcher gains a deeper understanding of the data (Braun & Clarke, 2021b, 2021c). This study utilised ATLAS.ti 25 for the analysis of qualitative data, as shown in Table 4.6. Following Braun and Clarke's reflexive thematic analysis were employed to analyse the recorded interview (Braun & Clarke, 2021c, 2019). The interview were transcribed word for word and analysed by using Braun and Clarke's six-phase analytical process for data management, coding and theme development (Braun & Clarke, 2021c, 2019; Finlay, 2021). Reflexive thematic analysis (RTA) is a theoretically accessible and adaptable method for identifying and analysing patterns or themes in qualitative data (Braun & Clarke, 2021c, 2019). Some studies emphasise that RTA prompts researchers to consider their subjectivity and positionality, examining how they arrived at their analysis and interpretation (Braun et al., 2022; Braun & Clarke, 2024; Hughes et al., 2024). RTA can be beneficial for reflecting on how researchers' prior knowledge and experiences may influence data collection and analysis, as well as how the data

collection and analysis process can alter the researcher's views (Braun et al., 2022; Rowland & Conolly, 2024).

Table 4.6: Reflexive Thematic Analysis phases

Analytic Phase	Description	Actions
Data familiarisation	The researcher starts to familiarise themselves with the depth and breadth of the data intimately. Immersion stage for searching pattern.	• Read and re-read the data/transcripts • Writing rough notes
Generating Initial codes	The researcher begins to organise the data items in a meaningful and orderly way.	• Succinct labels/items are arranged into meaningful group • Following the coding of each data items • Collation/matching of codes and themes
Searching for themes	The researcher starts to sort the codes and data together to identify meaning and patterns in the datasets.	• Linking of data to each relevant theme after the collation • Grouping of selective categories of meaning and themes together
Review of themes	The researcher verifies that the theme is consistent with the entire dataset and other themes. The researcher begins to assess whether it addresses the research questions.	• Improvement and development of codes/themes • Collapsing themes together • Splitting and refining the codes/themes
Define and name themes	The researcher writes a detailed analysis of each theme. The researcher looks for a story to tell about the theme and the overall data.	• Identified themes in order to organise to tell a story • Ideally succinct and thought-provoking title for each theme
Report production	The researcher presents the themes in a wider report, which includes an interesting account of the story and discussion as told in the entire data.	• Merging the analytic description into a convincing story • Using an instructive data extract as evidence • Writing beyond the simple report of the themes

Source: adopted from Braun et al. (2019) and Braun and Clarke (2021c, 2019)

Braun and Clarke (2022) state that the RTA six-phase analytical process is not linear; it requires an iterative approach, in which the researcher needs to work backwards

and forward constantly throughout the data analysis process. The six-phase analytical process is followed to analyse data, as explained in detail in this section.

Phase One: Dataset Familiarisation

The researcher listened to each audio recording multiple times to get familiarised with the qualitative datasets, while taking notes to identify key statements from the interview data (Braun & Clarke, 2022, 2021c; Konstantinos, 2024). In this process, the researchers continuously listen to the audio recording to visually engage with each participant's words and feelings. This helps the researcher become deeply engaged with the breadth and depth of data to understand participants' views, perceptions and beliefs. After that, each participant's recording was transcribed word-for-word into a separate Word document. The researcher then read and reread all participants' transcripts individually, before importing them to Atlas.ti 25 for the next phase.

Phase Two: Generating Initial Codes

Following the active familiarisation process, in this second phase, the initial code begins to organise or arrange into a meaningful and orderly way. Campbell et al. (2021) asserted that generating codes (a word or label) characterises the important organisation of the data, which are narrower than the themes to be identified in the next phase. Braun and Clarke (2022) vitally emphasise that coding and meaning should be drawn from the dataset inductively or deductively. This means that the researcher must allow the data to speak for itself using deductive means by applying the existing theory as the lens to guide the data analysis (Braun & Clarke, 2022, 2021c). Studies within the RTA codes can be both inductive and deductive, originating and developed from the collected data (Braun & Clarke, 2022; Rowland & Conolly, 2024). This necessitates several iterative rounds of re-examining the transcripts to refine the codes, to produce a workable and differentiated dataset (Hughes et al., 2024). During this phase, the researchers revisited the research questions periodically. This was done in response to what the dataset was saying, to expand the points of analysis beyond those reflexively predicted by the researchers (Braun et al., 2022; Hughes et al., 2024). Additionally, these codes were inductively grouped into

broad patterns of meaning, before the sorted codes were deductively combined to align with the PMT constructs, cybersecurity threat, cybersecurity practices and user experience (Campbell et al., 2021; Hughes et al., 2024). The diagram below in Figure 4.6 illustrates a sample of the numerical count of multiple codes that were organised and collated into coherent groups from the interview data.

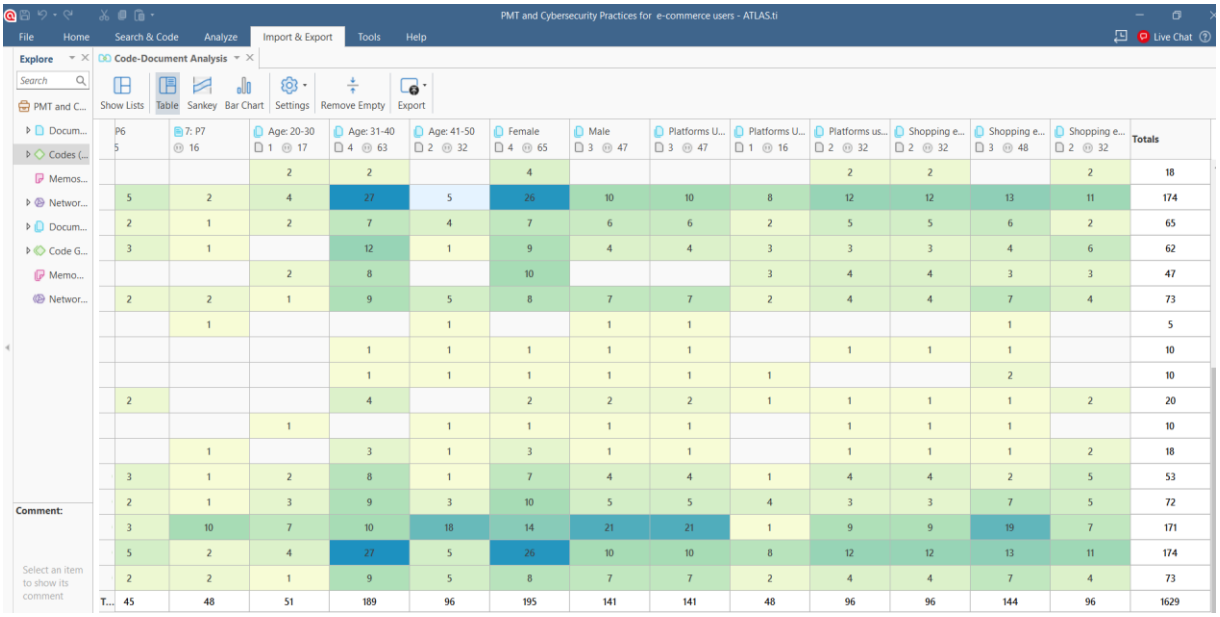


Figure 4.6: Sample of the coding process on e-commerce platform users for this study

Phase Three: Initial Themes Generation

Following the second phase, the researcher focused on sorting the codes into initial themes. This phase was previously known as *searching for themes,* before Braun and Clark renamed it *generating initial themes* in their recent works (Braun & Clarke, 2022, 2019; Campbell et al., 2021). As emphasised by Braun and Clarke (2022), themes are actively created by the researchers and not passively waiting in the data to be found. The researcher began to selectively group codes according to the identity theme and sub-themes. This process was executed manually and in Atlas.ti, sorting similar codes to form potential themes into the coding groups. Moreover, theme construction was influenced by the researcher's years of experience in cybersecurity (Campbell et al., 2021; Rowland & Conolly, 2024). Additionally, the themes contributed to the overall story on e-commerce platform users' experiences: cybersecurity threats, basic

security measures and cybersecurity practices. An example of the themes generated and grouped is presented in Figure 4.7**.**

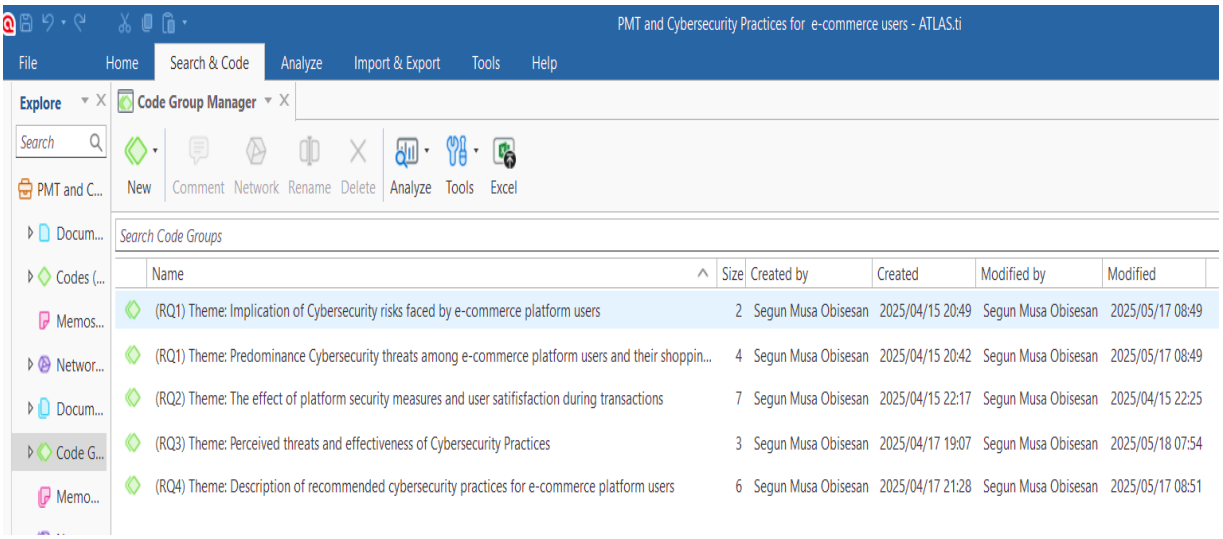


Figure 4.7: Sample of the initial grouped themes for this study

Phases Four and Five: Reviewing and Defining Themes

This phase involves the dual process, checking that all constructed themes are aligned with the study objective and research questions. At this stage, all the organised themes and possible sub-themes were subjected to further scrutiny to ensure they were tied into the similar themes that they belong to (Braun & Clarke, 2022; Rowland & Conolly, 2024). The themes were modified and refined to be catchy and to tell a compelling story about the data overall. Furthermore, according to Rowland and Conolly (2024), when a researcher is pleased with the themes and sub-themes, internally in relation to a correct supportive dataset, they can be established through definition, after completing the evaluation of the overarching themes from the dataset. Theme titles were further revised after grouping to eliminate duplication, and identified themes were valid to provide data that captured as most suitable to fulfil this study's research questions. Examples of themes and sub-themes reviewed and extracted from the data for this study are illustrated in Table 5.6 of Chapter 5.

Phase Six: Writing up

This is the final phase of RTA, which involves writing the findings as a report or dissertation (Braun & Clarke, 2022). According to Rowland and Conolly (2024), the

reports produced should involve a concise and interesting account representing the themes and the research questions. In this study, the researcher concluded that the analytical process resulted in creating themes and sub-themes based on the context, within which these data extract was embedded and associated with the research questions for this project. These extracted data were purposefully incorporated as evidence to provide more context to the themes. Additionally, the themes and sub-themes were adjusted to address the PMT, cybersecurity practices and e-commerce platform users in the internet cafés. The findings for all the themes and sub-themes were presented and discussed in Chapter 5.

4.7.9 Rigour/Trustworthiness (Credibility, dependability, transferability, conformability)

The concepts of validity and reliability are observed by qualitative researchers (Nha, 2021; Noble & Smith, 2015; Sadık, 2019). In qualitative studies, terms such as credibility, trust value, rigour, confirmability, applicability and trustworthiness are used to describe validity (Nha, 2021; Noble & Smith, 2015; Sadık, 2019). The use of credibility to denote internal validity in qualitative research suggests that member-checks and triangulation methods rely on interpretation from multiple sources (Sadık, 2019; Yin, 2018). Transferability, which represents external validity, depends on researchers providing a comprehensive description of the research context, allowing readers to apply the knowledge to their own settings (Sadık, 2019). Dependability is recommended as a measure of reliability in qualitative research (Sadık, 2019). In addition, conformability is vital to ensuring the rigour and trustworthiness. Qualitative researchers stressed the connection of conformability to other criteria such as transferability and credibility for rigour and trustworthiness (Kakar et al., 2023; Shenton, 2004; Singh et al., 2021). According to Kakar et al. (2023), conformability demonstrates the magnitude of research findings' objectivity that emerged from the data instead of researcher bias. Trust values are attained through reflexivity, reflection on personal perspectives, and aligning research findings with the phenomenon under investigation (Noble & Smith, 2015). Triangulating data from various sources strengthens the credibility of the study, which is contingent upon the suitability of the

data collection method in capturing the study's purpose (Ahmed, 2024; Healy & Perry, 2000; Sadık, 2019). Moreover, explanatory sequential mixed methods enables triangulation, which addresses rigour, trustworthiness, credibility, dependability, transferability, conformability and trustworthiness in the qualitative phase of this research study. The researcher employs a variety of instruments, such as questionnaires and interviews, to improve the credibility, dependability, transferability, conformability, rigour and trustworthiness of the research study.

4.7.10 Data Analysis for Explanatory Sequential Mixed Methods

Studies stressed that researchers could anticipate the quantitative scores based on existing literature and the theory while extending the findings to a larger population in comparison with the qualitative themes (Babaei & Vassileva, 2024; Creswell & Creswell, 2023; Schwendtner et al., 2024). Moreover, Figure 4.8 depicts a joint display template for an explanatory sequential mixed methods design, showing how a researcher can integrate quantitative scores in the first phase and then qualitative themes as a follow-up to build on the quantitative results (Creswell & Creswell, 2023). The joint display template, which combines explanatory sequential mixed methods, will be utilised later in the discussion of findings sections for this study (Figure 4.8).

Quantitative Scores	Quantitative Follow-Up Themes	Metainferences
High Scores	Theme 1 Theme 2 Theme 3	How Themes Explain the Scores
Medium Scores	Theme 4 Theme 5 Theme 6	How Themes Explain the Scores
Low Scores	Theme 7 Theme 8 Theme 9	How Themes Explain the Scores

Figure 4.8: Joint display template for explanatory sequential design adopted from Creswell and Creswell (2023)

Furthermore, Figure 4.8 guides the study to describe how the qualitative themes helped to provide insight into the different quantitative scores of individuals in the research study. Recent studies such as Schwendtner et al. (2024) employed explanatory sequential mixed methods design with PMT components to assess

perceived threat on behavioural changes and the moderating effect of age. They utilised quantitative methods for Austrian consumers in the beginning phase and subsequently followed with qualitative interviews. Also, Babaei and Vassileva (2024) studied the evaluation of users' intention to learn about manipulative design and factors influencing those intentions. Table 4.7 below represents the adapted joint display of explanatory sequential mixed methods outlined by Creswell and Creswell (2023), which is the methodological choice that this research study will follow.

Table 4.7: A joint display template for explanatory sequential mixed methods for e-commerce platform users

Internet cafés	Quantitative Scores	Qualitative follow-up themes	Meta-inferences
Perceived cybersecurity threats	85 – 80 = High	Cybersecurity fallout Phishing and smishing scams	How themes explain the scores
	78 – 70 = Medium	Fake retail platforms Mistrust OTP messages	
	58 – 50 = Low	Risk of disclosing personal data User behaviour in e-commerce	
Basic cybersecurity practices	86 – 80 = High	Knowledge of security measures and experiences Password management in shared environment	How Themes Explain the Scores
	78 = Medium	Anticipated security measures in building user confidence Adoption of advanced payment methods	
Application of cybersecurity measures	67 – 41 = High	Verification practices and purchasing decisions	How Themes Explain the Scores
	25 – 15 = Medium	Preference for recognised sites	
	12 – 1 = Low	Low legitimacy awareness of safety features	
Impact of cybersecurity practices on users' perceived cyber risks	92 – 84 = High	Confidence in security routines	How Themes Explain the Scores
	76 – 65 = Medium	Risk perception and feelings of online safety in digital platforms	
	52 = Low	Frustration and missing instructions in e-commerce security design	

Adapted from Creswell and Creswell (2023)

4.8. Ethical Considerations

According to (2021), ethical considerations are vital in research methodology and design, and the researcher should address ethical issues during the course of the research project. The key principles and ethical concerns, such as informed consent,

risk of harm and confidentiality, are part of the specific requirements that the researcher must address about the target population for the data collection (Chang, 2021; Hasan et al., 2021). Rhodes University Human Research Ethics Committee SOP 4.1 highlights the following ethical areas that this study address for the involvement of human participants (Rhodes University, 2024). The researcher obtained ethical clearance from the University's Ethical Committee before commencing data collection.

The principles of informed consent

The participants in this study were over 18 years old. The purpose of this research was explained to ensure their voluntary participation, and they have the right to withdraw without coercion.

Information to participants

The researcher briefly explained the aims of the research study, which includes research details. Additionally, the purpose and confidentiality of data collection was explained to all participants.

Informed consent of participants

A clear explanation of the study's objectives was provided to participants along with the informed consent form, and they signed before data collection begins. Participants were assured of their rights to withdraw from the study without coercion.

Anonymity of participants and confidentiality of data

The researcher informs all participants about the data collection procedure, and they remain anonymous in the study. All participants' data are kept confidential; only the researcher and supervisor will have access to the collected data.

Collection and storage of research data

All participant recordings, transcripts and data are securely stored with restricted access. Additionally, the researcher will ensure the privacy and confidentiality of all collected data during the research project.

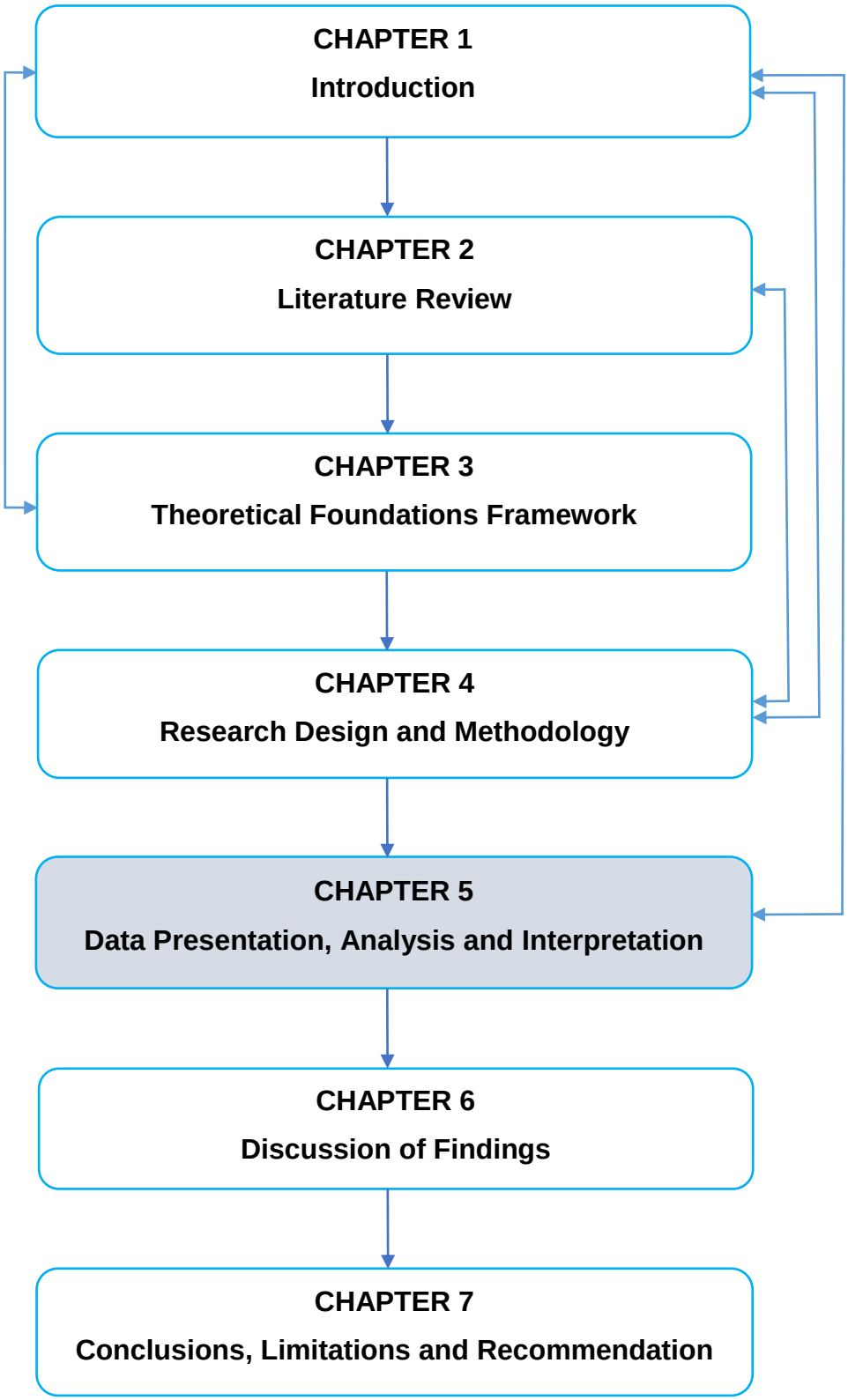
Risks and benefits

This research includes the risks and benefits in the consent letter provided to the participants.

4.9. Conclusion

This chapter outlined the research methodology employed for this research. The Research Onion Model guides this study provided a detailed description of the research process and its systematic steps to achieve the study objectives. The chapter employed an explanatory sequential mixed methods design; quantitative data were utilised in the first phase, from which the quantitative scores inform the subsequent qualitative phase to explore and deepen understanding of the results emerging from the quantitative findings. Integrating results from both phases will enable a comprehensive analysis of the relationship between cybersecurity practices and e-commerce platform users' experiences within e-commerce platforms in the public internet café settings. The next chapter presents and interprets the results of this research study. Data analysis and interpretation will be presented in the next chapter.

CHAPTER 5: DATA PRESENTATION, ANALYSIS AND INTERPRETATION



5.1. Introduction

The study adopted the *PMT to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha.* Chapter 4 presented the research methodology, research philosophy, methodological choice and data collection procedures, and the adapted research methodology from the Research Onion Model framework. The study uses an explanatory sequential mixed methods design to achieve the study objectives.

This chapter presents an analysis and interpretation of the results from both quantitative and qualitative phases of the empirical component of the study. The rest of the chapter is organised as follows: Quantitative data analysis, instrument reliability, and quantitative data presented as frequency tables, graphs, Spearman correlation, and chi-square test using descriptive and inferential statistics for the quantitative phase. In the qualitative phase, qualitative data analysis involved presenting and analysing themes and sub-themes using reflexive thematic analytical processes.

5.2. Quantitative Data Analysis

The data presentation, analysis and interpretation are systematically structured around the research questions of the study.

1. What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?
2. How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?
3. How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?
4. What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping?

5.2.1 Instrument Reliability

The questionnaire items were determined using the Cronbach's alpha test and were found to have a value of 0.854, which was highly acceptable. This implied that all items in the questionnaire consistently measured the same construct and positively contributed to the overall reliability of this project (Gizaw et al., 2022).

5.2.2 Response Rate for the Self-Administered Questionnaire Used in the Quantitative Phase

One hundred questionnaires were distributed to respondents in the three internet cafés in Internet café A, B and C. Out of these questionnaires, Ninety (90) questionnaires were correctly completed, and ten (10) were rejected because the respondents partially completed 1 to 3 questions of Section A of the questionnaires, and indicating that they were not shopping online (See Table 5.1). The overall response rate was 90% and the results are illustrated in Figure 5.1.

Table 5.1: Distribution of questionnaires per internet café

Internet Café	Distributed questionnaires	Accepted	Rejected	Reason for rejection	Response rate
A	26	23	3	Incomplete questionnaires/ Not online shoppers	23%
B	26	23	3	Incomplete questionnaires/ Not online shoppers	23%
C	48	44	4	Incomplete questionnaires/ Not online shoppers	44%
Total	**100**	**90**	**10**		**90%**

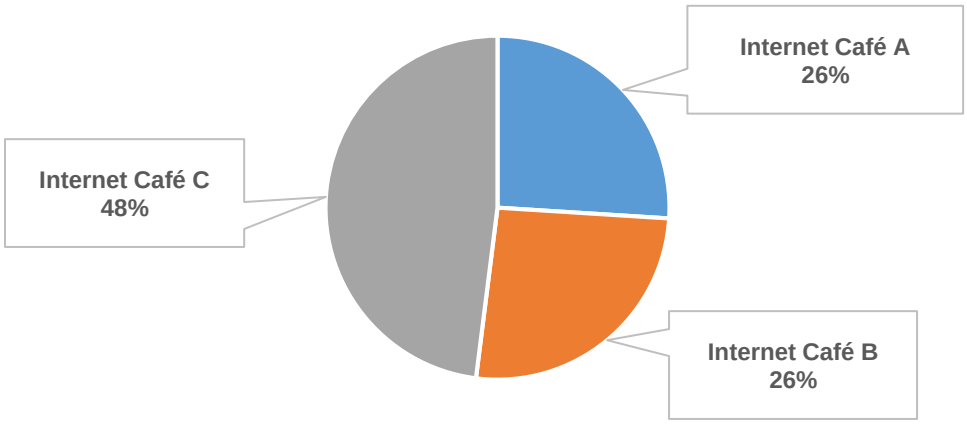


Figure 5.1: Distribution of questionnaires for the internet cafés

The results show the distribution of the accepted questionnaires by internet cafés. Internet café C accounts for 48% of the respondents, while Internet Café A and B account for 26% each. Therefore, the results reported in this study were based on the 90 respondents' data on the impact of cybersecurity practices and user experiences within e-commerce platforms in the Internet cafés in Gqeberha.

Table 5.2 represents the reliability test for the questionnaire items used for this quantitative phase.

Table 5.2: Reliability test for the Questionnaire items

	n=90	
Items	**No of Items**	**Cronbach's Alpha**
Section A: Demographic Information for e-commerce users	10	0.634
Section B: Perceptions of Cybersecurity Threats and Risks when shopping online in an internet café	10	0.897
Section C: Awareness of Basic Cybersecurity Practices and Measures when shopping online in an internet café	11	0.756
Section D: Perceived Cybersecurity Practices Effectiveness	9	0.670
Overall questionnaire's reliability	40	0.854

5.2.3 Demographic information about respondents

The results in Table 5.3 depict demographic information of the respondents from whom the data used in the quantitative phase were collected. Demographic data were based on the characteristics of e-commerce platform users needed to assess the impact of cybersecurity practices on their experiences with e-commerce platforms in Internet cafés in Gqberha, Eastern Cape.

Table 5.3: Demographic information for e-commerce platform users

Respondents (n = 90)		f	%
Gender	Female	41	45.6
	Male	49	54.4
Age	18-19	2	2.2
	20-30	40	44.4
	31-40	30	33.3
	41-50	12	13.3
	50+	6	6.7
Education	Matric	40	44.4
	Diploma	19	21.1
	Bachelor	25	27.8
	Honours	2	2.2
	Master's	4	4.4
	Doctorate	0	0.0
Online Shopping Experience	Less than 1 year	15	16.7
	1-3 years	48	53.3
	4-6 years	20	22.2
	7-10 years	5	5.6
	More than 10 years	2	2.2
Shopping Frequency	Rarely	43	47.8
	Occasionally	16	17.8
	Frequently	16	17.8
	Very Frequently	15	16.7
Number of Platforms Used	1 Platform	17	18.9
	2-3 Platforms	49	54.4
	4-5 Platform	16	17.8
	More than 5 platforms	8	8.9

The results show that more male respondents (49, 54.4%) than female respondents (41, 45.6%) shopped online at internet cafés. Collectively, the results further indicated that the predominant e-commerce platform users were of the age groups between 20 and 40, who accounted for up to 77.7%, 20 to 30 (44.4%), and 31 to 40 (33.3%). The least number of e-commerce platform users using internet cafes were those aged above 41 years (41-50, 13.3% and 50+, 6.7%). These results suggest that internet users over 41 years old are less likely to shop online. Regarding educational qualifications, the results indicate that a higher percentage of e-commerce platform

users hold Matric (44.4%), Bachelor's degrees (27.8%) and Diploma (21.1%) degrees, followed by those with higher qualifications, such as Master's (4.4%) and Honours degrees (2.2%). This implies that most respondents shopping on e-commerce platforms were mostly those with matric as the highest level of education.

Moreover, these results indicate that most respondents have had several years of online shopping experience, 1-3 years (53.3%), 4-6 years (22.2%) and less than 1 year (16.7%). Only a few respondents have 7-10 years (5.6%) and more than 10 years (2.2%) of online shopping experience. These results demonstrate that many respondents had less than 4 years of online shopping experience in internet cafés. In addition, most respondents, 47.8%, shop less than once a month (rarely), while 17.8% shop occasionally in the internet café. E-commerce platform users who frequently or very frequently shop online in an internet café was 17.8% and 16.7% respectively. The results further indicate that the majority of respondents use multiple platforms for online shopping, with 2-3 platforms (54.4%), and one platform (18.9%), while only a few e-commerce platform users shop on 4-5 platforms (17.8%) and more than five platforms (8.9%). The results confirm an increasing use of multiple platforms among respondents, driven by the convenience and accessibility of online shopping platforms, which may expose them to cybersecurity risks.

5.2.4 General Knowledge and Understanding of Cybersecurity Risks

In Figure 5.2, the respondents were asked to rate their knowledge and understanding of cybersecurity risks when shopping online on e-commerce platforms on a 4-point Likert Scale (4=Excellent, 3=Good, 2=Average and 1=Poor).

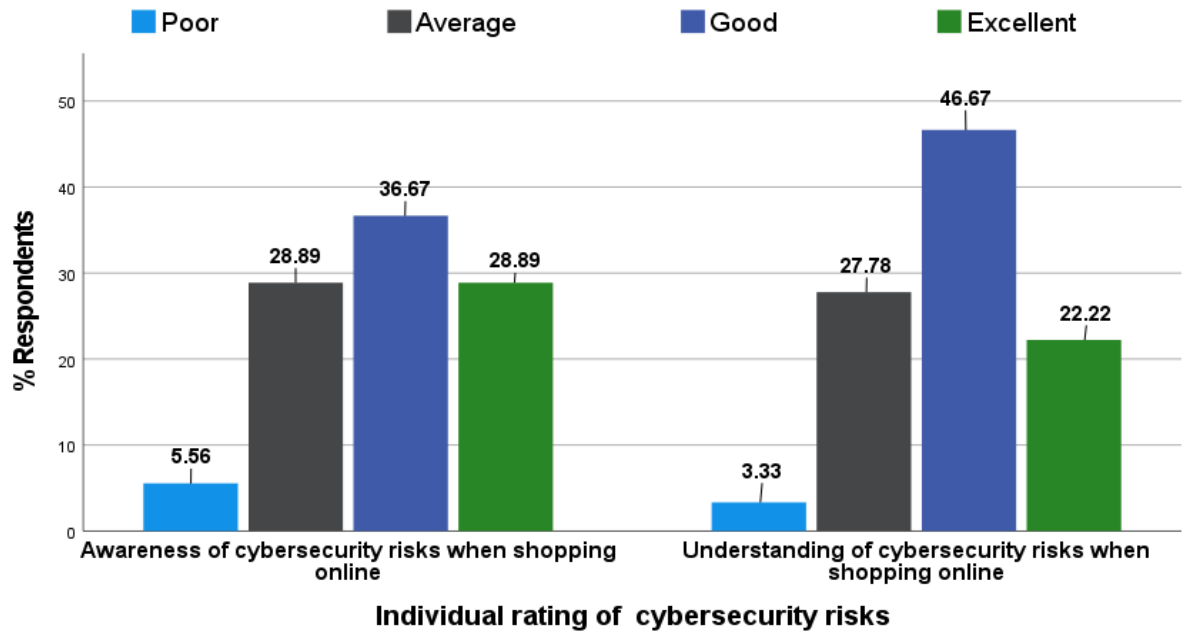


Figure 5.2: E-commerce platform users' overall knowledge of cybersecurity risks

The findings reveal that the respondents rated their knowledge of cybersecurity risks as excellent (28.89%) and good (36.67%). 28.89% of the respondents, rated their knowledge as average, and only 5.56% considered to have poor knowledge of cybersecurity risks. Furthermore, the majority of respondents (69%) rated their understanding of cybersecurity risks as excellent (22.22%), followed by good (46.67%). 27.78% respondents were rated as average. Only 3.33% of respondents had a poor understanding of cybersecurity risks. This implies that the level of knowledge and understanding of cybersecurity risks among the respondents used in this study was good.

5.2.5 General Knowledge and Understanding of Best Security Practices

The respondents were asked to show on a 4-point Likert Scale (4=Excellent, 3=Good, 2=Average and 1=Poor) in Figure 5.3, their general knowledge and understanding of best security practices when shopping on e-commerce platforms.

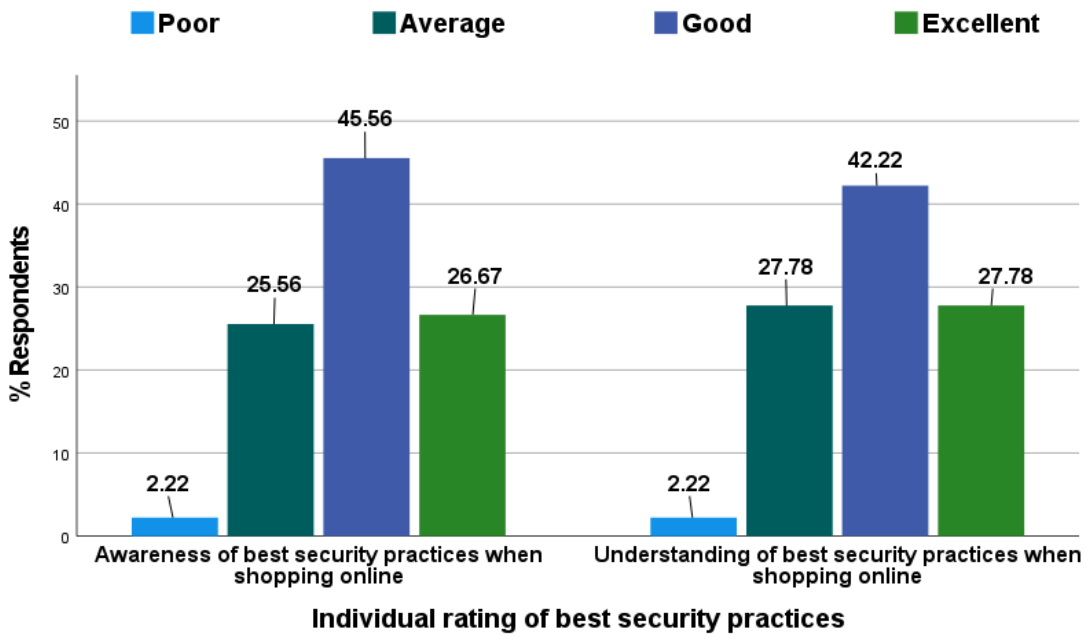


Figure 5.3: E-commerce platform users' general knowledge of best security practices

The results indicate that the respondents rated having knowledge of best security practices as excellent (25.56%) and good (45.56%). 26.67% of the respondents rated their knowledge of best security practices as average, while 2.22% rated it as poor. In addition, the majority of respondents (69%) rated their understanding of best security practices as excellent (27.78%), while 42.2% considered themselves good. However, 27.78% of the respondents rated their understanding of best security practices as average, and 2.22% considered it poor. This implies that many respondents considered themselves to have a better understanding of best security practices, while a few users considered themselves to lack the best security practices. Therefore, the level of knowledge and understanding of best security practices among respondents was relatively good for this study.

5.2.6 Perceived cybersecurity risks to be affecting e-commerce platform users in a public internet cafés

The respondents showed their ratings on perceived cybersecurity threats in the quantitative phase on a 5-point Likert scale (5=strongly agree, 4=agree, 3=not sure, 2=disagree and 1=disagree). Table 5.4 depicts the e-commerce platform users' perception of cybersecurity risks and how they impacted their online shopping activities.

Table 5.4: E-commerce platform users perceived cybersecurity risks and threats

Ratings (n= 90)							
Item	**Strongly Agree f (%)**	**Agree f (%)**	**Not Sure f (%)**	**Disagree f (%)**	**Strongly Disagree f(%)**	**Mean**	**Std. Dev**
I am concerned about my personal and financial information being stolen while shopping online	49(54.4%)	25 (27.8%)	6 (6.7%)	7(7.8%)	3(3.3%)	4.22	1.089
I believe cybercriminals frequently target online shopping platforms to steal customer data.	43 (47.8%)	30 (33.3%)	9 (10.0%)	5 (5.6%)	3 (3.3%)	4.17	1.041
I worry about falling victim to phishing scams or fake shopping websites when using internet cafe facilities.	34 (37.8%)	29 (32.2%)	13 (14.4%)	13 (14.4%)	1(1.1%)	3.91	1.098
I feel that online shopping platforms do not provide sufficient protection against cybersecurity threats	24 (26.7%)	27 (30.0%)	18 (20.0%)	17 (18.9%)	4 (4.4%)	3.56	1.200
I am concerned that malware or spyware could compromise my accounts on the e-commerce platforms I use for online shopping	19 (21.1%)	33 (36.7%)	22 (24.4%)	14 (15.6%)	2 (2.2%)	3.59	1.059
I believe shopping on e-commerce platforms in an internet café significantly increases cybersecurity risks	27 (30.0%)	26 (28.9%)	26 (28.9%)	9 (10.0%)	2 (2.2%)	3.74	1.066
I believe phishing attempts (e.g., fake emails or websites asking for personal information) are a significant risk when shopping online	44 (48.9%)	33 (36.7%)	4 (4.4%)	8 (8.9%)	1 (1.1%)	4.23	.972
I am concerned about being redirected to fraudulent or suspicious websites while making a purchase	40 (44.4%)	31 (34.4%)	7 (7.8%)	11 (12.2%)	1 (1.1%)	4.09	1.056
I believe e-commerce platform users are at risk of unauthorised transactions or suspicious activities on their bank or payment accounts	35 (38.9%)	33 (36.7%)	11 (12.2%)	9 (10.0%)	2 (2.2%)	4.00	1.060
I am worried about receiving fake order confirmation emails or scam messages after shopping online	34 (37.8%)	38 (42.2%)	4 (4.4%)	13 (14.4%)	1 (1.1%)	4.01	1.055

The results in Table 5.4 show respondents' ratings on how perceived cybersecurity risks impacted e-commerce platform users when shopping online in an internet café. Most respondents, 82.22% (mean score 4.22), affirmed that they were concerned about their personal and financial information being stolen. The majority of respondents (81.11%, mean score 4.17) believe that cybercriminals target online shopping to steal their data. The respondents, 70% (mean score 3.91), were worried about falling victim to phishing scams or fake shopping websites when using internet café facilities. This was consistent with 56.67% (mean scores 3.56) of respondents believing that e-commerce platforms do not provide enough protection against cybersecurity threats, and 57.78% (mean scores 3.59) were concerned that malware or spyware could compromise their account when using e-commerce platforms.

Moreover, the factor highly rated among the respondents on perceived cybersecurity risks was 58.89% (mean score 3.74), indicating that shopping on e-commerce platforms in an internet café increases their cybersecurity risks. 85.56% (mean score 4.23) showed that phishing attempts, such as fake emails or websites asking for personal data, were major risks for their online shopping. This corresponded with 78.88% (mean score 4.09) of respondents who were concerned about being redirected to fraudulent or suspicious websites, especially while making payments. This result was consistent with 75.56% (mean score 4.00) who believe that they were at risk of unauthorised transactions or suspicious activities on their bank or payment accounts. 80% (mean score 4.01) of the respondents were worried about receiving fake order confirmations, emails, or scam messages after shopping online on e-commerce platforms. These results confirmed that many e-commerce platform users had a serious perception of cybersecurity risks, especially regarding personal and financial information, targeted cyberattacks, phishing, identity theft, smishing, platform security vulnerabilities, and fraudulent websites in the internet café setting. This implies that the respondents in this study were highly concerned about cybersecurity risks, as reflected in a high mean score (mostly above 4.0).

5.2.7 E-commerce platform users' awareness of basic cybersecurity practices in the shared internet cafés environment

Figure 5.4 shows the results of respondents' ratings on basic awareness of cybersecurity practices implemented for their safety when using e-commerce

platforms on a 5-point Likert scale (5=strongly agree, 4=agree, 3=neutral, 2=disagree, and 1=strongly disagree).

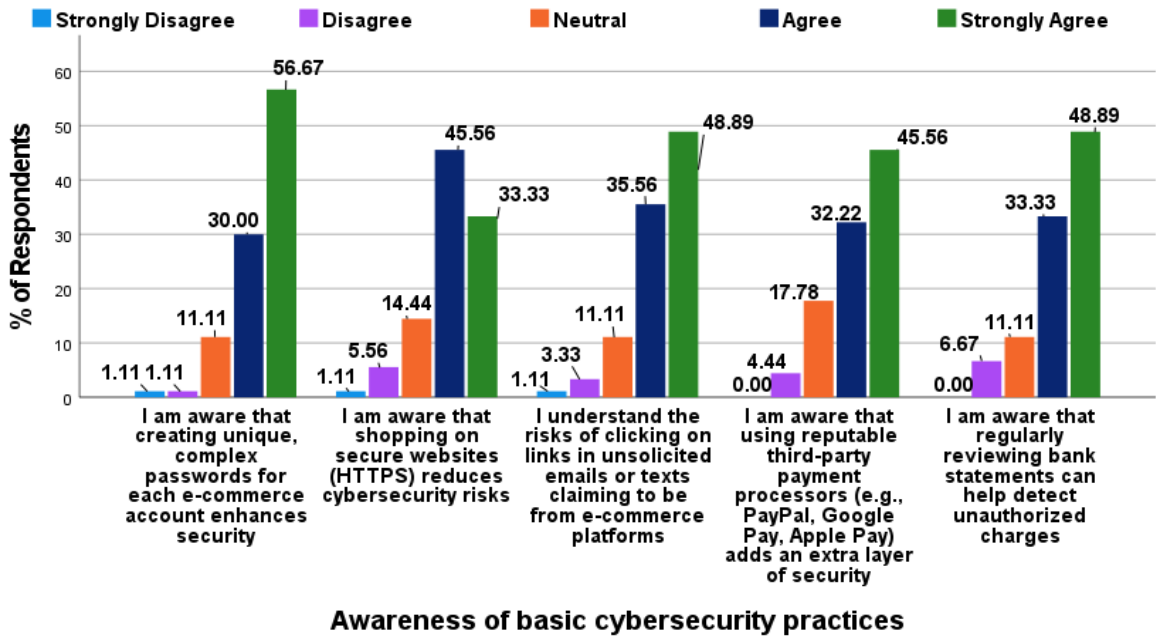


Figure 5.4: Basic cybersecurity practices for e-commerce platform users

The results indicate that a significant majority of respondents, 86.67%, were aware of the importance of creating unique passwords for their accounts. 78.89% of respondents were aware that secure websites (HTTPS) reduce cyber threats. This was followed by 84.45% who understood the risks of clicking on links in unsolicited emails or texts that appear to be from e-commerce platforms. 77.88% of respondents were aware of the importance of using reputable third-party payment processors. Moreover, 82.22% of the respondents were aware of the need to review bank statements for unauthorised charges regularly. These findings show that the majority of respondents have fundamental awareness of cybersecurity practices such as password creation, understand unsolicited emails or texts, and review bank statements. However, there was a moderate awareness of secure websites (HTTPS) and third-party payment processors among them. This implies that the awareness of basic cybersecurity practices among the respondents was moderate for this study.

5.2.8 E-commerce platform users' adoption of cybersecurity measures

The respondents were asked to rate their active use of cybersecurity measures and how these measures impact their satisfaction and shopping experiences on a 5-point Likert Scale (Always = 5, Often = 4, Sometimes = 3, Rarely =, and Never = 1).

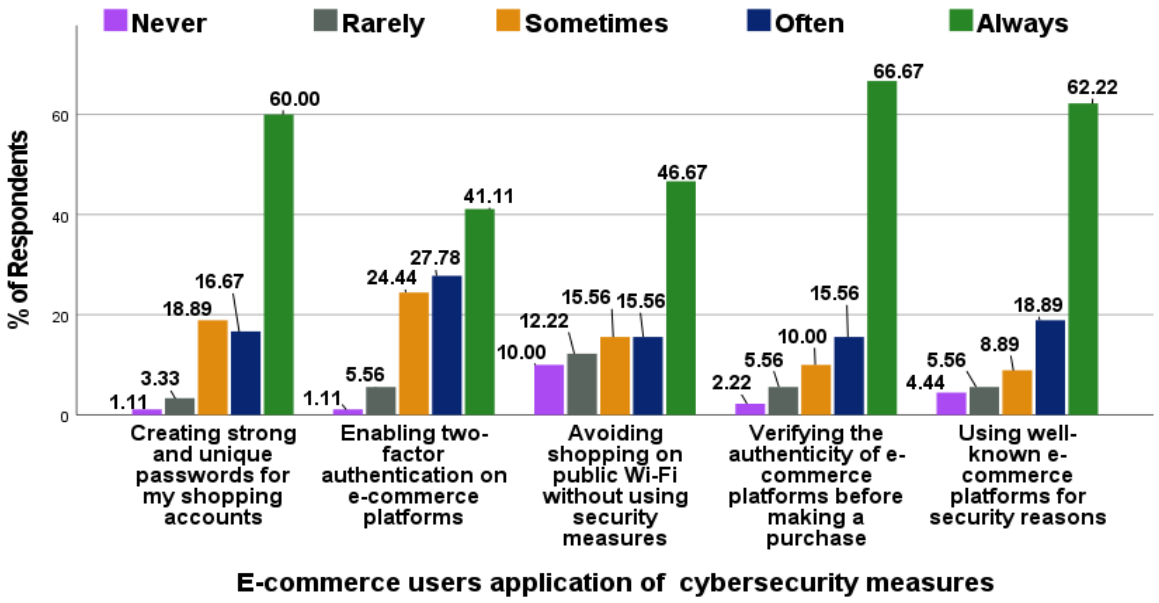


Figure 5.5: Adoption of cybersecurity measures among e-commerce platform users

Figure 5.5 indicates that most of the respondents (60%) always adopted cybersecurity measures by creating passwords for their accounts, 41.11% enabled two-factor authentication, 46.67% avoided shopping on public Wi-Fi without using security measures, 66.67% verified the authenticity of platforms before making a purchase, and 62.2% used well-known e-commerce platforms for security reasons. Similarly, respondents who often used cybersecurity measures were 16.67% more likely to create strong passwords, 27.78% more likely to enable two-factor authentication, 15.56% more likely to avoid shopping on public Wi-Fi without using security measures, 15.56% more likely to verify e-commerce platforms before making an online purchase, and 18.89% more likely to only use well-known e-commerce platforms due to security concerns. Furthermore, the results indicate that respondents adopt cybersecurity measures to varying degrees, with 8.89% adopting them sometimes and 3.33% to 12.22% rarely. However, 1.11% to 10% of the respondents never adopt cybersecurity measures when shopping on the e-commerce platforms in an internet café environment. These findings show the respondents' cybersecurity habits when

shopping online in the internet cafés. The majority of the respondents consistently adopt safe habits of following cybersecurity measures. However, a certain portion still occasionally engages in unsafe habits, sometimes or rarely, and never follows these practices, particularly among e-commerce platform users in an internet café.

5.2.9 Impact of the effectiveness of cybersecurity practices on e-commerce platform users' perceived cybersecurity threats

In Table 5.5, the resepondents showed their ratings on influence of the effective of cybersecurity practices in relation to the cyber threats faced during online transactions based on the 5- point Likert Scale (5=strongly agree, 4=agree, 3=neutral, 2=disagree, 1=strongly disagree). The relationship between the effectiveness of cybersecurity practices and the perceived cyber risks and experiences of e-commerce platform users was illustrated in Table 5.4. The results reveal the respondents' ratings (52.3% to 92.2%), with a mean score of 3.47 to 4.10 indicating the efficiency of cybersecurity practices in responding to the extent of their perceived cybersecurity threats being confronted when shopping online in the internet cafés. The factors highly rated among the respondents, influencing their confidence in cybersecurity practices were: strong password and Two-factor authentication reduce cyber threats 92.2% (mean score 4.47); checking for security indicator (padlock, SSL) before making purchase 67.8% (mean score 4.06); regularly update passwords and enabling two-authentication for online shopping accounts to enhance security 65.5% (mean score 3.89); and fear of cybersecurity risks influenced their decisions to take extra security measures when shopping or making online payments 73.4% (mean score 4.04).

Table 5.5: Ratings of e-commerce platform users' perceived cyber threats and various cybersecurity practices

Ratings on (=90)							
Items	**Strongly Agree f (%)**	**Agree f (%)**	**Neutral f (%)**	**Disagree f (%)**	**Strongly Disagree f (%)**	**Means**	**Std. Dev**
I believe that cybersecurity practices such as strong passwords, two-factor authentication effectively reduce my risk of cybersecurity risks while shopping online	54 (60.0%)	29 (32.2%)	4 (4.4%)	1 (1.1%)	2 (2.2%)	4.47	.824
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	36 (40.0%)	25 (27.8%)	27 (30.0%)	2 (2.2%)	0 (0.0%)	4.06	.891
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	30 (33.3%)	29 (32.2%)	24 (26.7%)	5 (5.6%)	2 (2.2%)	3.89	1.011
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments	33 (36.7%)	33 (36.7%)	19 (21.1%)	5 (5.6%)	0 (0.0%)	4.04	.898
I regularly check for cybersecurity updates or tips to improve my online shopping security	35 (38.9%)	24 (26.7%)	25 (27.8%)	5 (5.6%)	1 (1.1%)	3.97	.999
I avoid shopping on websites that seem untrustworthy	55 (61.1%)	21(23.3%)	11 (12.2%)	2 (2.2%)	1 (1.1%)	4.41	.873
I find it difficult to apply security measures on e-commerce platforms	24 (26.7%)	23 (25.6%)	22 (24.4%)	13 (14.4%)	8 (8.9%)	3.47	1.274
I limit my online shopping activities due to concerns about cybersecurity threats in an unsecured website when using internet café	40 (44.4%)	29 (32.2%)	12 (13.3%)	8 (8.9%)	1 (1.1%)	4.10	1.017
Even when I know a website is secure, my concerns about cyber threats make me reconsider purchasing from an e-commerce platform when shopping online	38 (42.2%)	31(34.4%)	10 (11.1%)	9 (10.0%)	2 (2.2%)	4.04	1.070

Furthermore, the respondents rated 65.6% (mean scores 3.97), for regularly checking for cybersecurity updates or tips to improve online shopping security. The majority of respondents 84.4% (mean scores 4.41), rated avoiding untrustworthy websites and 52.3% (mean scores 3.47) find it difficulty in applying security measures. 76.6% (means scores 4.10) of the respondents, limit their online shopping activities due to cybersecurity concerns in unsecured websites and 76.6% (mean 4.04) rated that even with secure websites, concern about the security risks make them to reconsider completing their online transactions on e-commerce platforms. These findings show e-commerce platform users in Gqeberha were generally cybersecurity conscious but still many of respondents were confronting with challenges on how to properly implement cybersecurity practices when shopping on e-commerce platforms. This suggests that respondents were generally have strong confidence in the efficacy of cybersecurity practices, with high agreement on security practices such as two-factor authentication, checking for SSL certificates. However, this study further shows that cybersecurity fears continue to influence respondents shopping behaviour even when platforms are secure. This indicates that perceived threats were shaping the respondent's decision-making and caution in e-commerce platforms for this study.

5.2.10 Inferential Statistics for E-Commerce Platform Users

The inferential statistics for e-commerce platform users conducted for the quantitative phase are presented in detail in this section.

5.2.10.1 Awareness and understanding of cybersecurity risks and best security practices

The study used Chi-square tests to examine the association between the demographic variables, online shopping experience and shopping frequency of the e-commerce platform user's awareness or understanding of cybersecurity risks and best security practices. The results in Table AP1 in Appendix 10 show that most of the p-values ($p>0.05$), indicating no significant association between demographic variables and cybersecurity awareness or understanding cybersecurity risks and best security practices. Moreover, it shows that there was a statistically significant result between

shopping frequency and awareness of cybersecurity risks (X^2 = 18.15, df = 9, p < 0.033). This result suggests that the frequency of online shopping by e-commerce platform users may influence their awareness of cybersecurity risks, and factors such as age, gender, and education level do not show a substantial impact in this study.

Table AP2 in Appendix 10 shows the significance of e-commerce platform users' awareness and understanding of best security practices based on the Spearman correlations. The correlation result shows that e-commerce platform users' awareness and understanding of best security practices were strongly associated with cybersecurity practices (r=0.770; n=90; p <.001), indicating that users who were aware also tend to understand the application of those practices. However, Spearman correlations between awareness of best security practices (e.g., creating strong passwords, checking for padlocks and updating passwords) were statistically significant but weak at p-values between 0.227 and 0.305. Moreover, the understanding of best security practices and cybersecurity practices, such as fake order confirmation worries, checking for padlocks, or avoiding shopping on untrusted platforms, is statistically significant, but weak at a p-value between 0.240 and 0.209. This implies that awareness or understanding of best security practices alone does not strongly improve cybersecurity practices, but it contributes modestly to e-commerce platform users.

Furthermore, the awareness and understanding of cybersecurity risks among e-commerce platform users were rated as revealed in Table AP3 in Appendix 10. The Spearman correlation shows a strong correlation between awareness and understanding of cyber risks (r=0.712; n=90; p < .001), emphasising the idea that cognitive knowledge and cybersecurity risks are closely linked. The correlations between awareness or understanding of cyber risks and cybersecurity practices (e.g. enabling 2FA, checking SSL or padlock, updating password or recognising secure websites) were all statistically significant but weak at p-values between 0.209 and 0.256. This suggests that while e-commerce platform users were aware of and understood cybersecurity risks, they were less likely to apply their knowledge of cybersecurity practices consistently when shopping online in the internet café.

5.2.10.2 Age and gender on shopping frequency for e-commerce platform users

The study used Chi-square tests to examine the association between the demographic variables (age and gender) and shopping frequency among e-commerce platform users. The results in Table AP4 in Appendix 10 indicate that there was no strong statistically significant association between age and shopping frequency among the users (X^2 = 6.259, df = 12, p = 0.902). This implies that age did not have a strong influence on how often e-commerce platform users engaged in online shopping activities in the internet café environment in this study.

Furthermore, the Chi-square results on gender and shopping frequency in Table AP5 in Appendix 10 show that there was a statistically significant association between gender and shopping frequency (X^2 = 8.885, df = 3, p = 0.031). This result suggests that gender may significantly influence the frequency of e-commerce platform users' engagement in online shopping within the internet café environment.

5.2.10.3 Overall impact of the effectiveness of cybersecurity practices on perceived cybersecurity threats among e-commerce platform users

The overall score for the impact and effectiveness of cybersecurity practices was evaluated based on perceived cybersecurity threats among e-commerce platform users, using Spearman correlation. All the correlations reported in Table AP6 in Appendix 10 were statistically significant at a p-value ($p<0.05$), indicating a moderate to weak association between perceived risks and the impact of cybersecurity practices on e-commerce platform users. It shows a strong and statistically significant association between checking for security indicators, regularly updating passwords and enabling two-factor authentication (r = 0.471; n = 90; p = 0.000). This implies that users who are very cautious when evaluating the credibility of the platforms tend also to adopt cybersecurity practices. Moreover, the degree of relevance varied with those cybersecurity practices, with regularly updating passwords and checking for security updates being even stronger (r = 0.379; n = 90; p = 0.000). This implies that there was a constant positive influence of cybersecurity practices among users. E-commerce platform users who perceive threats play a vital role in the effectiveness of cybersecurity practices. For example, the fear of perceived threats was significantly

correlated with cybersecurity practices among e-commerce platform users such as avoiding untrustworthy e-commerce websites (r = 0.379; n = 90; p = 0.000), reconsidering purchases even on secure e-commerce platform (r = 0.435; n = 90; p = 0.000), and checking for cybersecurity updates (r = 0.452; n = 90; p = 0.000). This was evident of the role that concerns over cybersecurity threats played as driving forces towards the effectiveness of cybersecurity practices among the e-commerce platform users.

5.3. Qualitative Data Analysis

The findings for qualitative phase interpretation and analysis were provided based on the research questions for this research project. The themes and sub-themes analysed were presented in Table 5.7, and the analytical processes followed for this study were covered in detail in this section.

5.3.1 Semi-structured interview for the qualitative phase

The demographic information of the participant groups, such as their age, gender, years of experience, and platform, is tabulated in Table 5.6. It reflects the participants' experiences and how they contributed to their online transactions. Their perception of cybersecurity challenges and cybersecurity practices that they encountered during their years of online shopping in public internet cafés in Gqeberha.

Table 5.6: Demographics of participants for qualitative phases (e-commerce platform users)

Participant's ID	Age	Gender	Years of Experience	Platforms Used
P1	20-30	Female	More than 10	More than 5
P2	31-40	Female	5	3
P3	31-40	Female	10	More than 5
P4	41-50	Male	2	5
P5	31-40	Female	2	2
P6	31-40	Male	5	4
P7	41-50	Male	2.6	5

5.3.2 Findings for the qualitative phases

This section presents the key themes and sub-themes for the findings from the qualitative data, which will be elaborated in this section as shown in Table 5.7. The results are presented with quotes from the participants that show how it complements the findings within this section.

Table 5.7: Themes and sub-themes on the impact of cybersecurity practices on e-commerce platform users

SQR	Themes	Sub-themes
Research Question 1	1. Predominance of cybersecurity threats among e-commerce platform users and their shopping behaviour	1.1. Risk of disclosing personal data 1.2. Phishing and Smishing scams 1.3. Fake retail platforms targeting e-commerce platform users 1.4. Mistrust triggered by phishing attacks mimicking OTP requests
	2. Implications of cybersecurity risks faced by e-commerce platform users	2.1. Cybercrime Fallout: from account theft to financial loss 2.2. User behaviour in digital platforms
Research Question 2	3. The effect of platform security measures and user satisfaction during transactions	3.1. Verification practices and purchasing decisions 3.2. Anticipated security measures and their role in building confidence 3.3. Adoption of advanced payment methods and fraud preventive behaviour 3.4. Preferences for recognised websites 3.5. Password management in shared environment 3.6. Low legitimacy awareness of safety features 3.7. Knowledge of security measures and experiences
Research Question 3	4. Perceived threats and effectiveness of cybersecurity practices	4.1. User risk perception and feelings of online safety in digital platforms 4.2. Confidence in security routines 4.3. Frustration and missing instructions in e-commerce security design
Research Question 4	5. Description of suggested cybersecurity practices for e-commerce platform users	5.1. Building trust through perceived data protection and risk disclosure 5.2. Integrating biometric verification to strengthen e-commerce platform security 5.3. Website verification cues processes 5.4. Use of secure and flexible payment options in e-commerce 5.5. Adoption of password managers 5.6. Improving cybersecurity habits through platform-supported user education

5.3.2.1 Theme 1: Predominance of cybersecurity threats among e-commerce platform users and their shopping behaviour

This first theme explored the prevalence of cybersecurity risks that e-commerce platform users encountered on these platforms. It revealed frequent challenges of e-commerce platform users' exposure to various cybersecurity risks (see Figure 5.6). The theme revealed the threat appraisals of PMT, showing the perceived vulnerability and severity of e-commerce platform users, because of shopping on e-commerce platforms in the internet café.

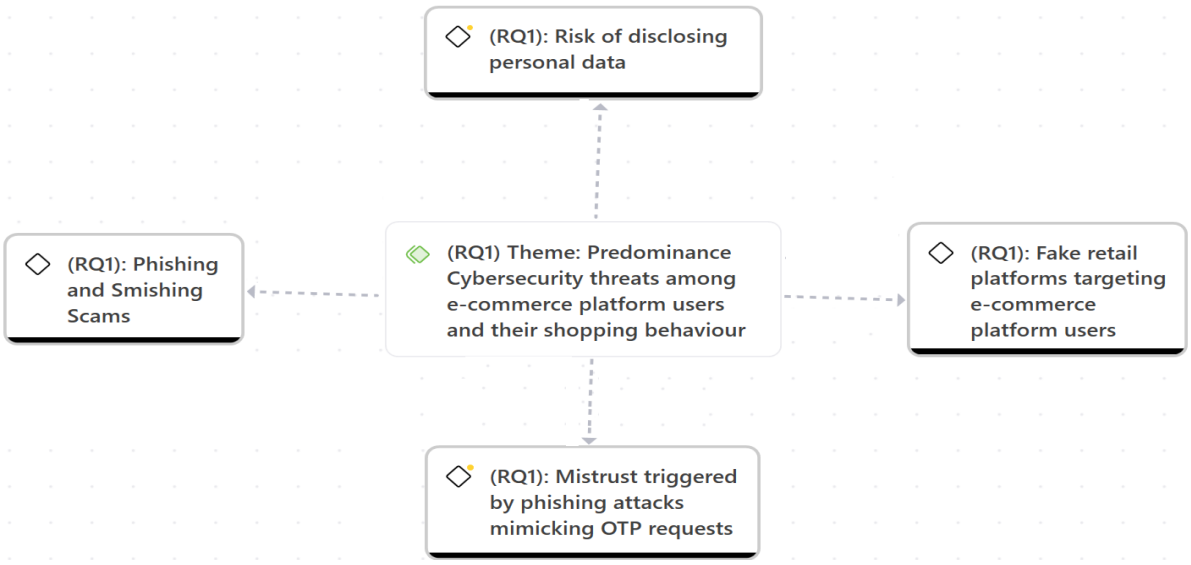


Figure 5.6: Map of theme 1 and sub-themes

Sub-theme 1.1: Risk of disclosing personal data

This sub-theme shows that participants were entering sensitive information on e-commerce platforms in the internet cafés. This highlights the perceived vulnerability of many participants, who may be susceptible to cyber risks due to the disclosure of their personal information. Participants 1 and 2 confirmed their disclosure of personal data on unverified websites and the risk of using an unprotected internet café environment.

> *"I would say anyone can get access to it. Let me say you go to an internet café, you tried to log in, you order something, and you enter your detail, you might not be to clear your detail before you go home. So, anyone can get access to them."* ***[Participant 1]***

> *"I think let say you are on Facebook, and you get that messages that got and said entered your details and then you enter**,** remember you put your numbers, because you are conducting a survey, and you have already put your number, email or maybe your addresses as well."* **[Participant 2]**

This study found high perceived vulnerability among e-commerce platform users. As e-commerce platforms continue to grow, users are increasingly shopping across multiple platforms. This makes them more highly vulnerable or prone to the risks of disclosing their sensitive information, which increases their online risks, especially in a shared-access internet café environment.

Sub-theme 1.2: Phishing and Smishing scams

According to the PMT, the sub-theme aligns with the perceived vulnerability of the threat appraisal due to the frequent occurrences of phishing and smishing scams. Participants described the repeated incidents of these scams they encountered while shopping online on e-commerce platforms. Phishing emails were identified as a perceived cyber risk when using online platforms. This was confirmed by Participants 2 and 6 in their constant encounters with phishing attacks.

> *"What I can say, I think I have received email or SMS to say that you entered this competition or maybe is a survey. So, you still get those SMS or email. Or they will tell you prize is on the way, so you need to pay a certain amount."* **[Participant 2]**

> *"Something they send me website link, but I am like, no, it is not what I want. I don't log in. To my email, I don't even open it at all because opening it is a risk."* **[Participant 6]**

Participants 1, 4 and 7 described their view of how they are being flooded with several fake SMS and messages aiming to extort them.

> *"I have received many fake message or SMS you know those kind of messages where they will say they will need your pin or OTP for something you order online. For example, fake message from banks to say you order something online which are not true, and you have to make this kind of payment for your order to be courier to you."* **[Participant 1]**

> *"You get SMS to say courier is on his way, but you have this outstanding amount of R60 or R30. You think it is a small amount you notice, you are expecting a parcel now you are getting an SMS that seems it is very legit, but I know that you have already paid for the stuffs, so you do not have to pay for the shopping again."* **[Participant 4]**

> *"Actually, this day there is a lot of scammers outside, several times I received messages my parcel has arrived I must pay certain amount for collection, which I never paid because those time I never buy anything online."* **[Participant 7]**

The findings reveal that e-commerce platform users perceive high vulnerability to cybersecurity risks, including phishing and smishing attacks, due to their use of public internet cafés for online shopping.

Sub-theme 1.3: Fake retail platforms targeting e-commerce platform users

Participants reported being misled by sophisticated fraudulent sites that were increasingly targeting them while they shopped online. This represents a perceived vulnerability of cyber threats confirmed by Participants 4 and 5, which can have a major impact on them and can lead to compromised credentials and monetary loss.

> *"Honestly, now that these websites are getting more and more now sophisticated, they can clone the whole websites, and you will think it is the original websites you are going."* **[Participant 4]**

> *"I think I was redirected to fake websites because did everything from that website and they took money from my account. I waited for the items."* **[Participant 5]**

The finding highlights that fake retail platforms pose significant challenges to e-commerce platform users, exposing them to a high perceived vulnerability of the PMT.

Sub-theme 1.4: Mistrust triggered by phishing attacks mimicking OTP requests

The perceived severity of PMT was confirmed by Participants 5 and 6, who reported challenges with phishing text OTP requests disguised as being from legitimate platforms, which caused fear and mistrust, as attackers precisely use this kind of attack to target e-commerce platform users.

> *"Since I am traumatised, I do not even trust those OTP them… Because I do not trust if the OTP is sent by the original people.... Because people can fake everything."* **[Participant 5]**

> *"OTP sometimes it is also dangerous because someone else can have your OTP and information and go with it."* **[Participant 6]**

The finding reveals that OTP mimicking request was a severe issue among e-commerce platform users, which caused anxiety, and it was considered as perceived severity among users shopping on e-commerce platforms in the public internet café.

5.3.2.2 Theme 2: Implications of cybersecurity risks faced by e-commerce platform users

The theme demonstrated the effect of cybersecurity risks, highlighting the real-life consequences faced by e-commerce platform users and how they were affected by those risks. The theme highlights the high perceived severity aspect of PMT, ranging from account theft to financial loss (2.1) and user behaviours in digital platforms (2.2) (See Figure 5.7). It reinforces how threat perception can shape e-commerce platform

users' responses and adjust their behaviour accordingly due to their experiences of cybersecurity risks in the internet café settings.

Figure 5.7: Map of theme 2 and sub-themes

Sub-theme 2.1: Cybercrime fallout: from account theft to financial loss

The extract from Participants 3, 5, and 7 shared stories and experiences of unapproved payment, loss of money and stolen identity and how these incidents affected their online shopping experiences and trust in the platforms. This sub-theme demonstrated the perceived severity of the PMT due to the serious implications of those experiences faced by e-commerce platform users.

> *"I will give you one that I got. I went on to a website to book a flight, and we concluded everything and about maybe like two weeks later, I saw money leaving my account and was from that same website**...**It is very serious on my side because I said they took money without my consent, so basically, they can clean out the bank account.**"*** **[Participant 3]**
>
> *"The first time they did send me the items, but they send a fake item, and when I send to them on email there was no response, and they don't pick up the call from the number that I got from them."* **[Participant 5]**
>
> *"But it happens to my wife, a message was sent to her phone, that message says that your parcel has arrived, you have to pay so amount to receive it. So she paid the money through her card; since that time sum of R350 has been deducted from her account every month. So, because of that, she has stopped using the bank."* **[Participant 7]**

This study found that account theft and stolen identity were major causes of financial losses, such as unapproved payments among e-commerce platform users, which caused severe consequences. They were revealed as having high perceived severity based on various experiences confronted by e-commerce platform users.

Sub-theme 2.2: User behaviour in digital platforms

The low perception of severity was confirmed among e-commerce platform users' behaviour, which resulted in their negative experiences with cyber risks, as they underestimated the consequences of these habits. Participant 6 confirmed how users' behaviour can lead to being a victim of account theft.

> *"I save my password online always; I do not think it will cost a lot because I just put automatic fill in on the page, when I click it, it goes straight to the site. I know it has consequence in case of any security breach. It may cause a lot because sometimes I think there was a time that they had my Facebook being hacked. They are talking to my people asking money. Please I need help, can you borrow my money. The person now have, to call my direct that what happened you have not asked me money before. What is happening and I said, no, I am not the one; now I have to block that account. I have to post the account and blocked it and reopening another one."* **[Participant 6]**

The findings suggest that the low perception of severity among e-commerce platform users is largely due to their vulnerability to online attacks. This implies that when users ignored or undermined protective behaviour, they were more likely to encounter or face severe consequences.

5.3.2.3 Theme 3: The effect of platform security measures and user satisfaction during transactions

Platform security measures affected e-commerce platform users when conducting online transactions in the internet café environment. The findings reflected the degree of interaction between the platform's security features and user satisfaction, as well as how these features shape their online shopping experiences. The theme and sub-themes in Figure 5.8 confirmed the self-efficacy and response efficacy of the PMT constructs, which captured how e-commerce platform users evaluate security measures and impact their online safety.

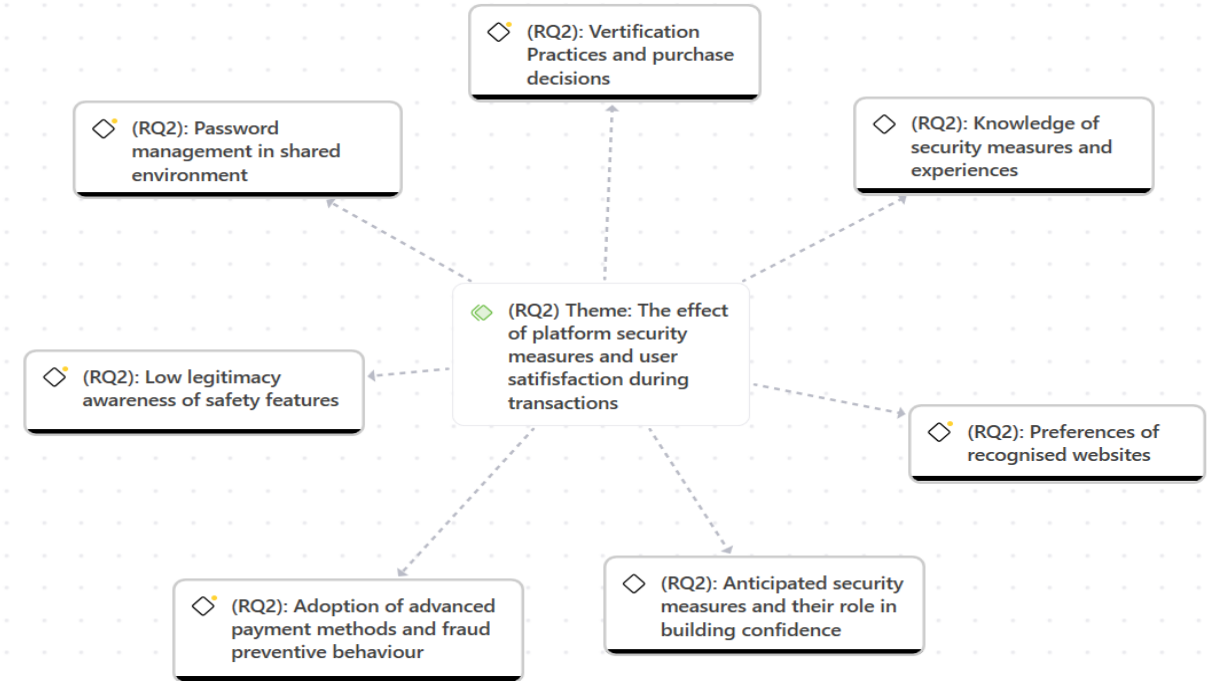


Figure 5.8: Map of theme 3 and sub-themes

Sub-theme 3.1: Verification practices and purchasing decisions

The purchasing decision was made based on users' previous shopping experiences and confidence in basic security measures. For example, Participants 1 and 2 confirmed that security measures reduced their exposure to cyber risks and boosted their trust. This influences their selection of e-commerce platforms during online transactions. This can be linked to high self-efficacy of the PMT, as participants believe it is necessary to carry out the protection actions before shopping online.

> *"Usually, the first thing I look for before using the platforms, I check other people reviews. If I see that there are good results, then I can order. I do check if the website is secured, looking for the secure logo because the logos are different. If you have used the app for a while you can tell that this is not the platform that I shop from."* **[Participant 1]**

> *"Sometimes you have to check do you know that platforms. I think it is very importance before you do anything online, you must do research about the platforms or websites. Other thing that is important is to check the reviews. Sometimes, once you are there, you even get the comments and complains of what people are saying about that websites it would go about knowledge if there are reliable, trustworthy and authentic."* **[Participant 2]**

The finding shows that e-commerce platform users with high self-efficacy and confidence in various security measures are more likely to enjoy positive shopping experiences and be protected from online attacks.

Sub-theme 3.2: Anticipated security measures and their role in building confidence

Expected platform security measures confirmed to foster confidence among e-commerce platform users. The provision of these measures can strengthen and promote protective behaviour, which can boost users' response efficacy when shopping online on e-commerce platforms. For example, high response efficacy of the PMT was identified from Participants 3, 6 and 7 who expressed the importance of these measures most likely to aid their completion of online transactions. Those security measures enable users to feel safe and enjoy their shopping experiences.

> *"First shopping online, is very convenience seated at the comfort of my home, and I go through the websites so for me. And so, these security practices: multi-factors authentication and a strong password. It makes more pleasurable because you have a certain level of assurance that okay, I will have to authorise the transactions myself completing my order."* **[Participant 3]**

> *"Shopping online makes thing easy, affordable, but there are some things you do not see, but online you find everything, and you see everything you want. If the cybersecurity practices are there, it will make everything easy because it makes you aware that okay, I want to do this, and they are trying to confirm if it is true or not."* **[Participant 6]**

> *"It should be the first things to look for when you log in to a website, even before adding on cart, viewing it should be the first things to check; do these websites have all those security features for safety. If they do have security features, then it means that it is safe there to buy."* **[Participant 7]**

The role of expected platform security measures was found to boost the response efficacy of e-commerce platform users and promote protective habits if they are provided or displayed on the e-commerce platforms.

Sub-theme 3.3: Adoption of advanced payment methods and fraud preventive behaviour

The findings show that participants who have heard or experienced cybersecurity risks were more likely to adopt protective behaviour in their future online transactions. According to PMT, Participants 3, 4 and 6 demonstrated high self-efficacy by adopting safety measures like virtual card payment as protective habits to prevent financial fraud whenever they shop online based on their confidence and past experiences.

> *"One thing I have started doing now, bank has introduced, sometimes we call a virtual card, you don't get a physical card, it is an online card that shows on your banking app. The advantage of using that card is that the last three digits CCV numbers. It changes every hour,*

that means your card details are changing. So, if I enter it into a website, after an hour, CCV we change, so if they try to steal money cannot access." **[Participant 3].**

"I have on my phone the banking app and the virtual card, right, so the virtual card, the limit is for online shopping is set to zero. So, if I want to buy something now, I will increase the limit for now, pay for the things, and put the limit back to zero." **[Participant 4].**

"The only things that I do to be on a safer side is when I want to pay. Sometimes I don't use my bank card. I used this thing they taught me in FNB. It is like a card, like your normal card that you use." **[Participant 6]**

This study shows that e-commerce platform users who had previously encountered or perceived online dangers were more likely to demonstrate high self-efficacy during their online shopping activities.

Sub-theme 3.4: Preferences for recognised sites

Familiarity with platforms or websites serves as a critical factor that shapes e-commerce platform users' perception of legitimacy, transactional safety, and enhances their satisfaction. Participants 4 and 7 clarified how they avoid unfamiliar websites or platforms to enhance their safety and satisfaction. This demonstrates how protective habits can be directly connected to the perceived trusted platforms. However, it can undermine security measures, especially when users rely solely on a trusted platform rather than adopting protective habits.

"So, I will only go to those five websites that I know that are legit firstly….So because I feel like am using a big website like takealot.com like that I don't really verify the websites because it is something have been doing for now I don't have a problem with those websites, I just don't go to a website that I have never had of to buy something expensive it have to be a proper recognised and a big website." **[Participant 4]**

"If you are buying sometimes from the online platforms. It should be the one that is registered, famous and be the one that everybody knows. So that whenever any problem comes, it could be traceable like Takealout, Amazon and e-bay you will never get wrong with those websites….So actually, as a buyer, if I am buying on a registered platforms, you would not have any issues, you would not have any problems with your card." **[Participant 7]**

This finding reveals that e-commerce platform users' transactional safety and satisfaction were linked to their trust in the well-known e-commerce platforms. However, this can undermine their self-efficacy as they put their trust only in the websites and are more likely to ignore protective behaviours during their online shopping activities.

Sub-theme 3.5: Password management in shared environment

Participants 1, 4 and 7 demonstrated password safety based on their perceived protection when shopping online, especially in an unprotected internet café environment. This shows e-commerce platform users' views of basic security measures and how these influence their self-efficacy and response efficacy to adopt protective habits.

> *"You know it is only me who know this password. I can either write it down somewhere without you writing the app that have the password."* **[Participant 1]**
>
> *"I got a Samsung phone, it will ask me if I want to save the password to these websites then I will save it and when it asks me if I want to save my banking or card details, I will say no. No, I would not do that in an internet café to save my password in their system."* **[Participant 4]**
>
> *"There is password manager, there is something called Google Authenticator, and that is very good. Once you have that one Google Authenticator, it is secure your password; nobody will be able to access your password and profile."* **[Participant 7]**

The study examined the impact of self-efficacy and response efficacy among users of e-commerce platforms. They demonstrated their ability and confidence to adopt protective behaviour based on their shopping experiences when shopping online in an unprotected environment, such as internet cafés.

Sub-theme 3.6: Low legitimacy awareness of safety features

Participants with limited knowledge of security measures were more susceptible to cybersecurity attacks, which negatively impacted their shopping experiences. Participants 2 and 5 expressed their lack of knowledge about legitimate websites and security measures, which impacted their online shopping experience and led to dissatisfaction. This implies low response efficacy and self-efficacy to adopt protective behaviour among users who lack knowledge of basic security measures during online transactions, which can lead to negative experiences in an unprotected internet café.

> *"I can say in that I am not well-equipped or well-informed because normally when you do shopping. You go with confident or maybe with the brand, do you know the brand**?** But did not know if the sites were legit or what…I am not sure if it was authentic. I think we need to be schooled as a consumer that you have to know that before you enter to these websites. How are you protected sometimes? We get there because we did not know if whether is it right or wrong, whether you are risks or not at risks. You just go there, that is why people are losing lot of monies because lack of knowledge."* **[Participant 2]**
>
> *"The second time, they did not even deliver the item that I purchased online, and I went to the stock. They said in the stock that they did not online shopping on Facebook website. They are*

having their own website. I would not lie, I have never check if the website is a real thing or not because I do not even know how to check if it is a real thing online." **[Participant 5]**

This study shows that e-commerce platform users with low knowledge of basic security measures were more likely to encounter cyber-attacks, which negatively impacted their shopping experiences. Lack of knowledge was a result of low response efficacy and self-efficacy among users in the internet café in Gqeberha.

Sub-theme 3.7: Knowledge of security measures and experiences

Proper and exact knowledge of security measures was found to contribute to positive experiences among some participants. E-commerce platform users with a solid understanding of basic security measures take control of their online safety, whether the sites provide visible security features or not, and tend to enjoy their shopping experiences. Participants 1, 4 and 7 showed high self-efficacy and felt confident in adopting protective behaviours to improve their user experiences. This reveals that perceived trust and competence in e-commerce platform users are directly tied to cybersecurity knowledge and can reduce anxiety when shopping online and enhance their overall experiences and satisfaction.

"I will say it come a positive "impact" for my shopping experience, having the OTP, it will send you that message once. So you cannot enter that message twice. So it is quite a good experience." **[Participant 1].**

"I will myself to the websites maybe if I am browsing a Facebook and I see a Temu sales there R90 for phone. I will never click on that because I know that is now wrong. If I see something, I go to the Temu websites myself and look for it if I would find it there. I have never experienced any security issues or challenges." **[Participant 4].**

"I look for online platforms that is registered by government. Then, I do check their logo and customers reviews. A lot of people that have already bought items there. So, I check all those things before I buy from them. On my side, I am saved, because I very intelligent when it comes to online risks." **[Participant 7]**

This finding reveals that accurate knowledge of basic security measures led to a positive shopping experience and perceived safety among e-commerce platform users. Cybersecurity knowledge was found to increase self-efficacy among users with many years of shopping experience.

5.3.2.4 Theme 4: Perceived threats and effectiveness of cybersecurity practices

Many participants shared diverse perspectives on their perceptions of cybersecurity threats and the impact of cybersecurity practices in an insecure internet café setting. They reflected on their personal experiences, feelings and beliefs concerning the success of these practices, and how those perceptions shape their security practices. This theme connects directly to the threat and coping appraisal component of the PMT (See Figure 5.9). It demonstrates the link between perceived vulnerability and severity in relation to self-efficacy, response efficacy and response cost. E-commerce platform users believe that the efficacy of cybersecurity practices can reduce cyber risks. This stimulates and triggers their actual engagement to adopt protective habits based on their perceived cybersecurity risks. For example, the sub-themes explore e-commerce platform users' perception of risks and feeling of online safety, confidence in security routines and frustration and missing instructions in e-commerce security design (See Figure 5.9).

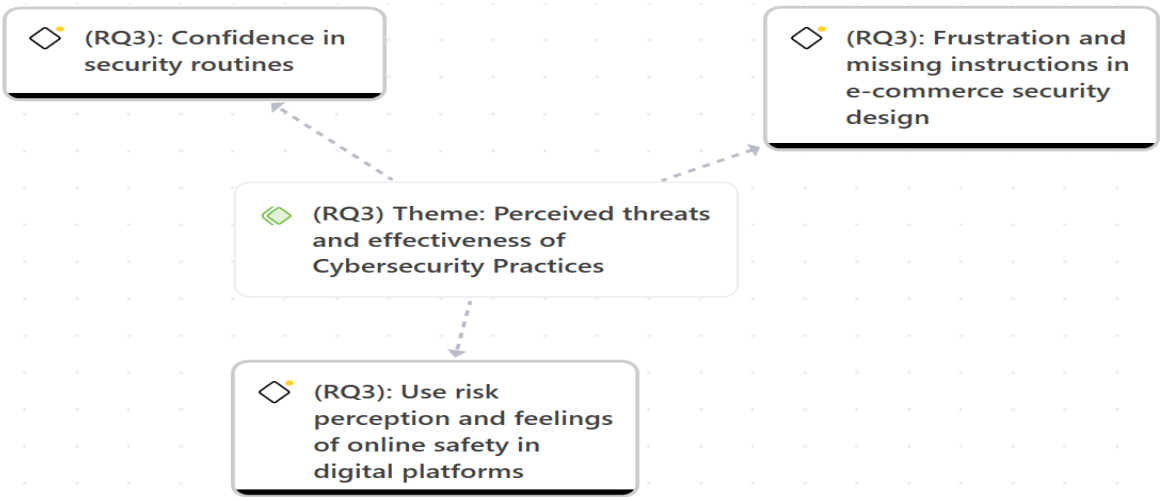


Figure 5.9: Map of theme 4 and sub-themes

Sub-theme 4.1: User risk perception and feelings of online safety in digital platforms

Participants expressed different perceptions of the cybersecurity risks that were of concern to them and their profound impact as they shop in an unprotected internet café environment. E-commerce platform users' anxiety about cyber risks stems from

their past experiences and digital literacy. This implies how these risks fit within perceived vulnerability and severity of the PMT, based on their opinions on cybersecurity threats as they shop on e-commerce platforms. Participants 1, 2, 3, and 5 highlighted the mixed feelings of perceived vulnerability to cyber risks such as security breaches, identity theft, hacking of the sites, and the seriousness of these risks if they were to occur. These threats were observed as perceived severity, which may influence their adoption of cybersecurity practices. This asserts users' perception and assessment of cybersecurity risks for the safety of digital platforms.

> *"When I started using the platforms, only thing I think of is my security. If there is a security breach is going to be very severe because with these apps, you kind of putting your banking details into the apps. So, if they ended up into the wrong hands. You will lose most of the monies in your account."* **[Participant 1]**
>
> *"I think it not safe, there is a risk that will take as a consumer. You do not know which one actually is safe when you are shopping online. I think as consumers we are not safe or secure in other platforms. Our security is not assured, it puts you at risk as a consumer because you can lose your monies."* **[Participant 2]**
>
> *"So, I felt very vulnerable. However, we do not know about the hacking of their sites, that is where I say I have no control over it. We can have dire consequence because they can also identity theft as sometimes people sell out our information to other parties and you see some fraudulent debit orders having been going from the bank account."* **[Participant 3]**
>
> *"Any platforms now from those scams that I have experienced that I got so I do not trust anymore now, so it is not easy for me to buy online again…. because people that are scamming can fake everything."* **[Participant 5].**

This finding reports various perceptions of cybersecurity threats among e-commerce platform users, because of their previous experiences and digital literacy. This reveals that the degree of perceived vulnerability and severity varied among e-commerce platform users, which was more likely to impact their protective behaviours.

Sub-theme 4.2: Confidence in security routines

The study found a strong link between threat and coping mechanisms of PMT. Some participants displayed positive attitudes towards adopting cybersecurity practices. The willingness and confidence to follow cybersecurity practices were influenced by their perceived cybersecurity risks. Participants 3, 4, 6 and 7 confirmed their intention to adopt security practices when shopping online in the internet cafés. They believed cybersecurity practices were easy to follow, as part of the protective process that should be provided on e-commerce sites. This is an indication of high self-efficacy and

response efficacy among e-commerce platform users in the use of security practices. This implies users have confidence in these practices to be effective in lessening cyber risks (response efficacy) and they feel confident to execute protective actions without difficulty based on their experiences (self-efficacy).

> *"From my experience it is easy to follow, because I work with such thing, so for me it works very easy to follow. They have to be more than one factor of authentication, for instance, if I am registering on that sites, before I can get in, I am expecting them to me maybe an email to say follow this link and go to verify so I can verify my account that I have and if I am doing a transaction, they must authenticate me more than once so that I can enter my card details and another factor authentication sending the OTP that goes to my banking app."* **[Participant 3]**
>
> *"I find the security measure easy to follow. So the websites that I used I can say they are very effective when you talk of security protocols that I consider using. Others I will not use because of security practices"* **[Participant 4]**
>
> *"The practices is not too difficult it is just a process, you just follow the normal process then everything is done to me. If that information comes from their sites, I will follow it I do not have problem to follow those security practices"* **[Participant 6]**
>
> *"It is not difficulty it is easy to follow even though for my safety also, for the safety of my data on their website. I find it as a good thing for me as a shopper.* **[Participant 7]**

This study explores the interplay between threat and coping mechanisms of PMT among e-commerce platform users, reporting their willingness to adopt cybersecurity practices based on the perceived threats they encounter when shopping online in internet cafés.

Sub-theme 4.3: Frustration and missing instructions in e-commerce security design

This study revealed that participants lacked clear instructions and experienced delays in implementing cybersecurity practices on e-commerce platforms. Participants 2, 3, 5, and 7 reported that the lack of guidance and instructions on following cybersecurity practices reduced their self-efficacy and the effectiveness of their coping mechanisms, despite a high awareness of threat appraisals. Participants' responses indicated that the lack of support stimulated high perceived response costs, such as time delay and inconvenience, which in turn weakened their self-efficacy and response efficacy. This eventually diminishes e-commerce platform users' motivation to adopt security practices. For example, participants expressed the inconvenience, confusion, verification delay and time consumption, and how it demotivated the effectiveness of

cybersecurity practices, even when e-commerce platform users demonstrated the willingness to adopt protective behaviours.

> *"The security practices for the websites are not effective, and then everything is ineffective. Then it is not good for use, for us as a consumer. There is no OTP to the websites. The only OTP that I have seen whenever it comes to online platforms it only when it comes to the payment…It is difficulty, and it is not easy for them."* **[Participant 2]**
>
> *"It makes it very difficult because you can easily make mistakes because you do not understand what to do, so personally, for my experience. So, there are some websites that you find out that there is no clear directions and instructions of how to follow and they are not user-friendly, and then it becomes very frustrating. I don't like struggling because when you struggle, it even takes your time, and I am a very time-conscious person."* **[Participant 3]**
>
> *"I think the site do have the security practices, but I am not sure about it. Since there are many scams, I do not trust the site. I rather go to the stock and then they do it online for me. Or they should show me how to do it, showing me the right websites."* **[Participant 5]**
>
> *"So, when I get to the websites, even though not only Temu, all of them, when you get to the websites to buy stuff, it does not show you any OTP. It is only when you are purchasing with your card that the OTP will show."* **[Participant 7]**

The findings indicate that the lack of guidelines and hindrances in implementing cybersecurity practices on e-commerce platforms lead to high perceived response costs among users, which in turn affects their self-efficacy and response efficacy when shopping on these platforms in internet cafés.

5.3.2.5 Theme 5: Description of recommended cybersecurity practices for e-commerce platform users

The theme recommends strategies and actionable plans that could strengthen cybersecurity practices among e-commerce platform users in an unprotected internet cafés setting. Participants were asked to provide recommendations on cybersecurity practices that could be adopted to improve their shopping experiences. The recommendation was grouped into six sub-themes (See Figure 5.10).

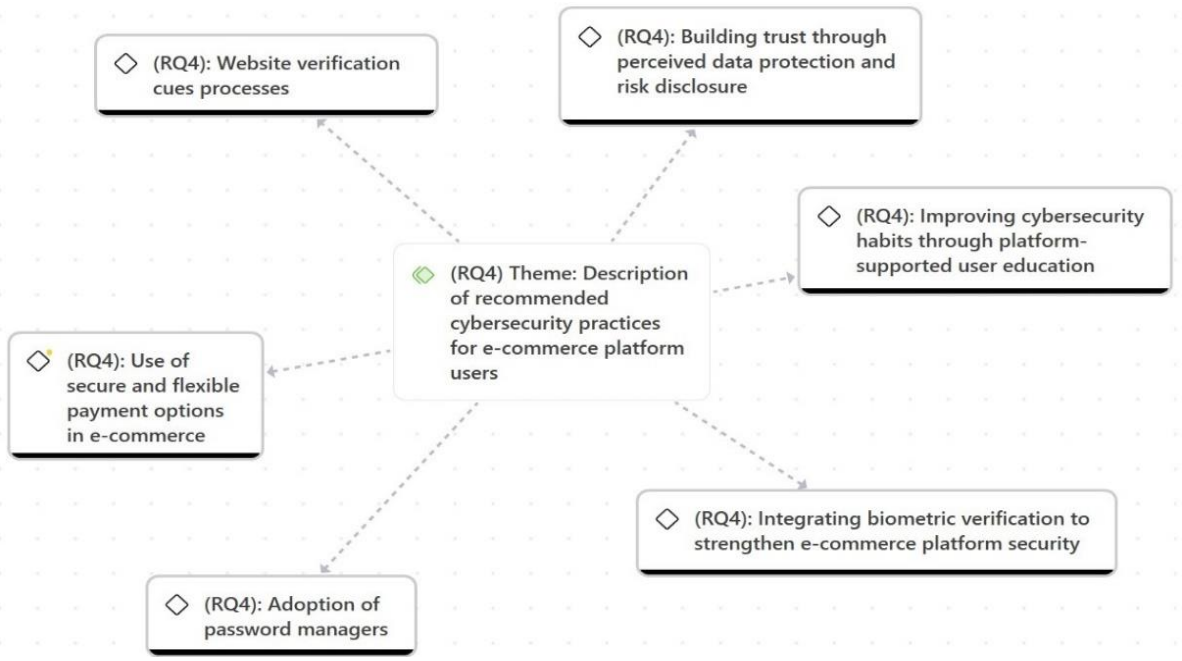


Figure 5.10: Map of theme 5 and sub-themes

Sub-theme 5.1: Building trust through perceived data protection and risk disclosure

Participants 3 and 4 suggested that e-commerce platforms should be transparent about their data protection processes and risk disclosure, especially on their sites. This could promote institutional trust between users and e-commerce platforms. Furthermore, it would reduce anxiety for e-commerce platform users in untrusted internet café environments.

> *"If, in any way, they found out that their websites have been compromised or duplicate somewhere that someone has fraudulently, you know, they have a fake of it. Communicate it, across. Declare it so that the customers can, who are using that websites, can be aware and be more vigilant."* **[Participant 3]**

> *"Obviously, they must keep our information secured, they must not get hacked and all our information details, card details and numbers. They must have a secure site, they must not get exposed or hacked."* **[Participant 4]**

This finding suggests that trust and transparency in data protection and risk disclosure could encourage users to prefer one e-commerce platform over others for their online shopping activities.

Sub-theme 5.2: Integrating biometric verification to strengthen e-commerce platform security

The extract reveals that e-commerce platforms should implement biometrics such as face recognition. Many e-commerce platform users considered biometrics to be user-friendly, which could improve their shopping experiences and enhance the security of their accounts. For example, Participants 3, 5, and 6 emphasised the importance of incorporating biometric verification, which could enhance their satisfaction and increase response efficacy, particularly among low-literacy users of e-commerce platforms in shared-access internet cafés.

> *"Also, another thing I would like to talk about is the facial verification you see if you are using a device, and maybe they are sending you an OTP on your email or on your cell phone and the number you cannot access it. If there is a facial verification, it is even better than those things can verify yourself and then you know that it is you. It is more dependable and more convenient. So, you don't need a cell phone to authorise it; whatever devices you are using to shop in will be enough to complete to take you through."* **[Participant 3]**
>
> *"If they can try that things, such as face recognition, I would gain my trust and be able to tell others people that they can trust that platform; it is working and real."* **[Participant 5]**
>
> *"I think that facial recognition it is better to see. Once the facial recognition is on; it has to correspond then, if not, there is a problem."* **[Participant 6].**

This study suggests that implementing facial recognition on platforms could enhance response efficacy among e-commerce users with low literacy in unprotected internet café environments. This could boost user satisfaction and enhance the security of their accounts and overall shopping experiences.

Sub-theme 5.3: Website verification cues processes

Participants 2, 3, and 7 suggested that the sites should have clear visual cues such as verification links, recognised logos and customer reviews for them to have confidence and trust in the legitimacy of their sites. These visual cues could enhance the response efficacy of the PMT, as users are more likely to believe in the effectiveness of the platform's security measures. Additionally, the availability of those cues could boost self-efficacy, as users will feel confident to navigate the websites or platforms where legitimacy is evidently protected. E-commerce platform users who frequently access online platforms in public internet cafés will find that visible cues

serve as a trustworthy indicator that can reduce perceived response costs, as they do not need to carry out extensive verification on the sites, which will improve their satisfaction and shopping experiences.

> *"You can see then is it a tick that it is authentic….if they can do that often in lot of the sites, I think it can work. And maybe OTP when you are logging your details or you are creating your information before it gets to the payment, and then that OTP test when to be verify as well."* **[Participant 2]**

> *"Number one is the verification of the websites, to have a way where you can verify that this is authentic websites."* **[Participant 3]**

> *"I would say that online shopping platforms, the logo must be the logo that everybody knows, the logo must be a legit one. And the platform must be the one have a lot of customers' reviews. When a platform have lot of customers review, if you as a shopper to buy there, you will not be scared. Because those of people had already their stuffs there and they are very safe."* **[Participant 7]**

The study suggests that website verification cues could improve response efficacy among e-commerce platform users, thereby increasing their confidence in the authenticity of the e-commerce platforms. The visibility of these cues could reduce perceived response costs, especially for users who frequently engage in public internet cafés.

Sub-theme 5.4: Use of secure and flexible payment options in e-commerce

The findings from Participants 1 and 4 revealed that e-commerce platforms should offer substitute payment options apart from traditional card payment methods. They further recommended using a virtual card and setting the transaction limit to zero after completing their online shopping, and only increasing it when conducting online transactions. All these actions align with the response efficacy of the PMT as effective cybersecurity strategies to prevent unauthorised payment or financial fraud. Also, participants demonstrated self-efficacy as they have confidence in their ability to proactively and personally adopt cybersecurity practices. This could help users manage their perceived cyber risks and improve their shopping experiences in unsecured internet cafés.

> *"I will say they must try to make a plan in terms of the card payments because sometimes we enter our cards on these platforms and look at it when some hacked into your phone, they get accessed to your banking details."* **[Participant 1]**

> *"The big thing for is that if you are using your banking app, giving your bank details in the internet it is very important to make sure that after finished shopping, set your limit back to zero. Don't keep a limit to R5000 to allow these people to take monies from your account. Even if somebody got my virtual card details, the limit is set to zero, and I must approve it on my phone. I feel safe about it that way."* **[Participant 4]**

This finding recommends promoting other flexible payment options, such as virtual card enhanced security features on e-commerce platforms and encourages e-commerce platform users in Gqeberha to make use of them. This could increase the self-efficacy of users to adopt active cybersecurity practices, thereby preventing illegal payments or financial fraud when shopping online.

Sub-theme 5.5: Adoption of a password manager

Participant 7 recommended that e-commerce platform users adopt the use of a password manager, such as Google Authenticator, to protect their shopping accounts. The participant revealed a conscious effort or decision to reduce online risks like account theft when shopping in a public internet café. This is linked to self-efficacy and response of the PMT, as users perceived the password manager to be effective in securing e-commerce accounts (response efficacy) and felt capable of adopting a password manager (self-efficacy), which emerged from user experiences.

> *"Then, another thing, I said it also that Google Authenticator is very necessary. Understand if I am buying on platforms like that, whenever I want to open to the apps, it will take me back to Google Authenticator, which the code you will get, you will use it to enter into the platforms. So, nobody can access your account. If the platforms would not be able to access your account. So Google authentication, it is very important to be added to all shopping platforms."* **[Participant 7].**

This finding suggests that e-commerce platform users should make use of a password manager when shopping on e-commerce platforms, especially in an unprotected internet café environment. Encouraging users to adopt a password manager would improve their response efficacy and self-efficacy to secure their accounts and enjoy positive online shopping experiences.

Sub-theme 5.6: Improving cybersecurity habits through platform-supported user education

E-commerce platform users suggested that platforms should provide cybersecurity practices education. Participants 4 and 5 stressed how teaching basic cybersecurity

practices could play a critical role in enhancing the self-efficacy of PMT. The platform-based education could encourage users to carry out security practices, empowering them to manage online threats effectively as they shop online in an internet café environment. Individuals with cybersecurity knowledge and experience feel more confident in adopting cybersecurity practices when shopping on e-commerce platforms. E-commerce platform users stressed that it enables them to trust their platforms with greater safety and satisfaction. So, e-commerce platform design should always incorporate instructions in the design of their platforms on cybersecurity practices for users on their sites.

> *"I would trust website which provide a message that guide me on cybersecurity practices."* **[Participant 5]**

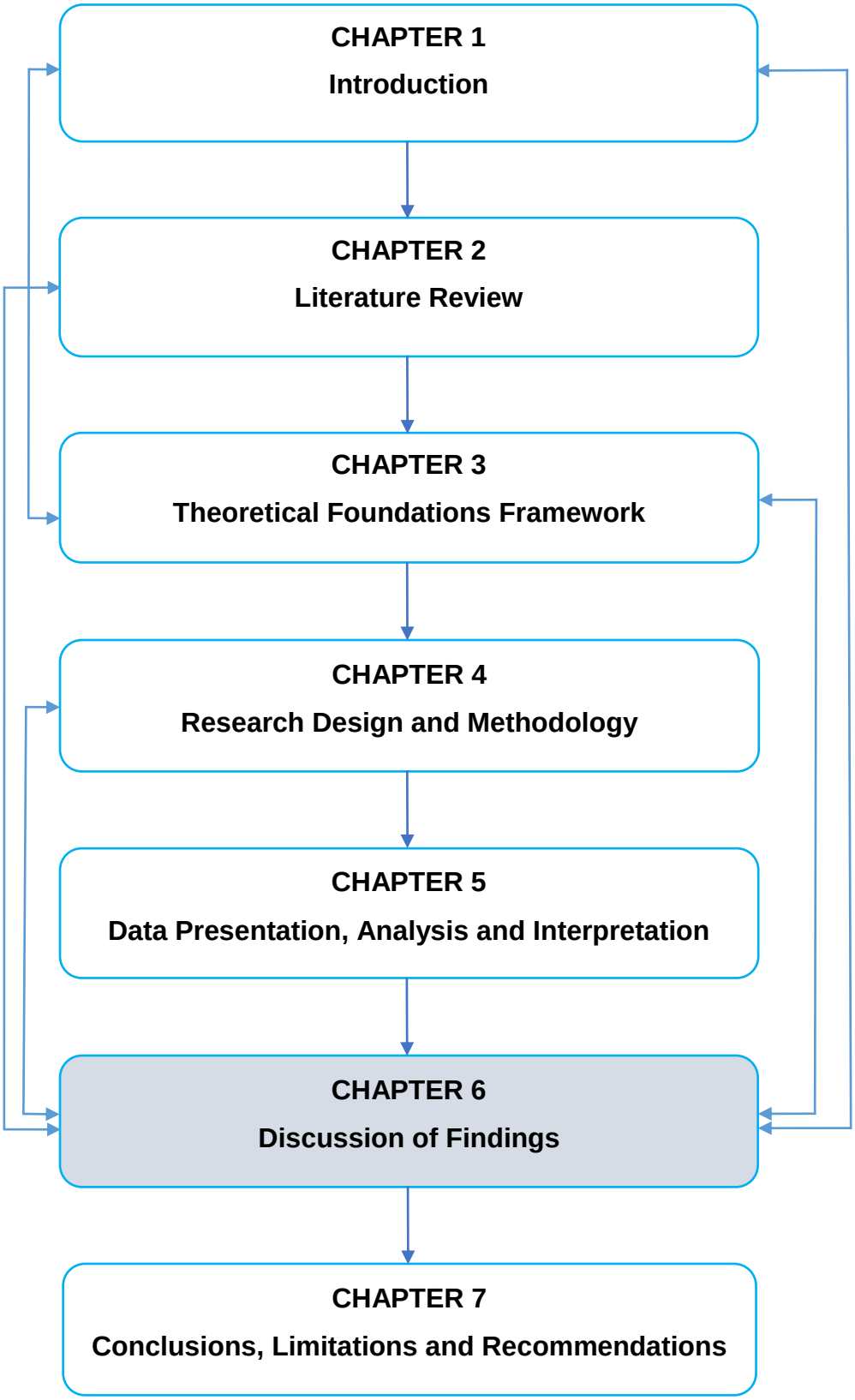
> *"I think everyone must be aware that they must not follow a link to go to websites. They must just not listen when they get a message to say there is a big sales follow that link and go to that site that they do not know. The must be careful, there is a phishing scam and other stuffs like that."* **[Participant 4]**

This study recommends that user education is vital for the adoption of cybersecurity practices. There is a need for platform-supported user education, which could play a vital role in e-commerce platform users' self-efficacy to feel confident in their capability to implement cybersecurity practices, especially for those shopping in an unprotected internet café environment.

5.4. Conclusion

This chapter presented the results from explanatory sequential mixed methods for this study. The data analysis and interpretation from the quantitative and qualitative phases were presented separately. The findings encompassed cybersecurity risks, shopping behaviour and basic security measures implemented in e-commerce platforms that were impacting users' satisfaction and overall shopping experiences in a shared-access internet café setting. Moreover, qualitative data provided insight into PMT constructs such as threat and coping appraisals based on the degree of perceived cybersecurity threats of e-commerce platform users and their influence on the effectiveness of cybersecurity practices. However, the challenges that users faced, such as a lack of clear instructions from the platform, frustration and time consumption, were revealed to be hindering the protective behaviours. The next chapter will present the discussion of the findings for this study.

CHAPTER 6: DISCUSSION OF FINDINGS



6.1. Introduction

The previous chapter presented and analysed the findings for both quantitative and qualitative phases of this study. As mentioned in the introduction section of Chapter 1, the purpose of this research *is to use the PMT to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha".* Chapter 6 presents a literature review discussion for this research findings centred around the research questions and protective motivation theory (PMT).

The sub-questions to be answered are:

1. *What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?*
2. *How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?*
3. *How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?*
4. *What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping*?

In this chapter, the findings from both quantitative and qualitative phases will be discussed using a joint display template for explanatory sequential mixed methods as presented in **Section 4.5.3** in the previous chapter. A joint display template for explanatory sequential mixed methods will be applied to each sub-question for this study, as illustrated in Table 6.1 below. The joint display template, as shown in Table 6.1, represents the pattern of how the discussion of findings for both quantitative and qualitative data will be addressed for this study, adapted from Creswell and Creswell (2023).

Table 6.1: A joint display template for explanatory sequential mixed methods

Internet cafés	**Quantitative Scores**	**Qualitative follow-up themes**	**Meta-inferences**
Perceived cybersecurity threats	85 – 80 = High	Cybersecurity fallout Phishing and smishing scams	How themes explain the scores
	78 – 70 = Medium	Fake retail platforms Mistrust OTP messages	
	58 – 50 = Low	Risk of disclosing personal data User behaviour in e-commerce	
Basic cybersecurity practices	86 – 80 = High	Knowledge of security measures and experiences Password management in shared environment	How Themes Explain the Scores
	78 = Medium	Anticipated security measures in building user confidence Adoption of advanced payment methods	
Application of cybersecurity measures	67 – 41 = High	Verification practices and purchasing decisions	How Themes Explain the Scores
	25 – 15 = Medium	Preference for recognised sites	
	12 – 1 = Low	Low legitimacy awareness of safety features	
Impact of cybersecurity practices on users' perceived cyber risks	92 – 84 = High	Confidence in security routines	How Themes Explain the Scores
	76 – 65 = Medium	Risk perception and feelings of online safety in digital platforms	
	52 = Low	Frustration and missing instructions in e-commerce security design	

Adapted from **Creswell and Creswell (2023)**

Protection motivation theory is briefly explained as a reminder to show how PMT components are applied in this study to answer the sub-questions stated above, which will be covered in detail in this chapter.

6.2. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) clarifies that cognitive processes motivate individuals to protect themselves when faced with potential threats and influence their motivation to adopt protective behaviour (Alsmadi et al., 2024; Shiri et al., 2024).

According to PMT, the core two cognitive processes are threat and coping appraisals. In this section, PMT components will be used to discuss the findings, which will be grouped and applied according to the four sub-questions for this study.

6.2.1 Threat Appraisal

The threat appraisal consists of perceived vulnerability and perceived severity, which are vital to assess and understand how cybersecurity threats influence e-commerce platform users and their behaviour when shopping online in a public internet café environment (Marikyan & Papagiannidis, 2023; Ruan et al., 2020).

6.2.1.1 Perceived vulnerability to cybersecurity threats

Perceived vulnerability refers to e-commerce platform users' feeling, views, and perception that they are exposed to being victimised or impacted by specific cybersecurity threats, such as account theft, as they engage on e-commerce platforms (Ghazali et al., 2023; Prasetyo & Wahab, 2022). E-commerce platform users' perception of cybersecurity threats was assessed based on the likelihood of being exposed to online risks when shopping in an unprotected internet café environment (Dakov & Malinova, 2021).

6.2.1.2 Perceived severity of cybersecurity threats

Perceived severity refers to how e-commerce platform users perceive severe cyber threats and their negative consequences when shopping on e-commerce platforms (Boerman et al., 2021; Kariuki et al., 2024). E-commerce platform users were examined to explain how they are being victimised or experiencing severe consequences as a result of cyber risks they were being exposed to when shopping online in unprotected internet café settings (Hariharan et al., 2023; Tsai et al., 2016).

6.2.2 Coping Appraisal

For this study, the PMT coping appraisal encompasses three key factors, namely: self-efficacy, response efficacy, and response cost, which play a critical role in influencing

e-commerce platform users' decision to adopt protective habits in a public environment such as an internet café (Ghazali et al., 2023).

6.2.2.1 Response efficacy

Response efficacy is the belief that the recommended actions, such as cybersecurity practices, will effectively reduce e-commerce platform users' exposure to online risks and prevent them from falling victim to cybersecurity threats (Haag et al., 2021; Haque et al., 2020). E-commerce platform users were examined on their belief in the effectiveness of cybersecurity practices to protect them from cyber threats in e-commerce platforms, especially in unsecured internet cafés (Hossain et al., 2024; Laudon & Traver, 2020; Zawaideh et al., 2023).

6.2.2.2 Self-efficacy

Self-efficacy refers to the belief and confidence that e-commerce platform users will successfully execute those recommended actions, such as adopting cybersecurity practices during online transactions (Prasetyo & Wahab, 2022; Tsai et al., 2016). In this study, e-commerce platform users were asked about their confidence and capability in the adoption of cybersecurity practices to protect themselves during online shopping activities in public internet cafés (Laudon & Traver, 2020).

6.2.2.3 Response cost

According to PMT, response costs cover the perceived costs associated with implementing protective behaviours, such as time, inconvenience or effort, that could prevent e-commerce platform users from adopting cybersecurity practices on the e-commerce platforms (Haag et al., 2021; Marikyan & Papagiannidis, 2023). E-commerce platform users were asked about the challenges or inconveniences that they are confronted with when trying to adopt cybersecurity practices implemented on the e-commerce platforms in a public internet café setting (Marikyan et al., 2022; Wang, 2023).

6.3. Characteristics of the E-Commerce Platform Users

Demographic information is essential to explain some observed behaviour of e-commerce platform users who shop online. Literature highlights the importance of demographic data and digital presence in e-commerce platforms (Prasad & Rohokale, 2020; Vasupula et al., 2022; Zende, 2022). In this study, most of the e-commerce platform users (54.4%) in the public internet cafés environment were male, while females were the minority (45.6%). According to Wijaya and Polina (2014), the users utilising internet cafés for their online transaction purposes were 53 males and 47 females. This confirms that more males were visiting the internet café than females for their online transactions and shopping purposes in Gqeberha. Moreover, the age of the e-commerce platform users ranged from 18 to 50+, with the majority, 77.7%, aged between 20 and 40. The finding was consistent with that of Oki et al. (2021), which showed that 73% of users shopping on online retail platforms in the Eastern Cape were aged 20 to 39. This confirms that younger shoppers were more likely to use internet cafés than elderly shoppers in Gqeberha, Eastern Cape.

Another finding of the study was on the frequency of shopping in internet cafes, which varied from frequently to occasionally among 47.8% of the respondents. The use of the internet café for online shopping was found to be higher than expected, considering that these places are unsafe due to cybersecurity issues (Sam et al., 2019; Wijaya & Polina, 2014). Previous studies report different findings for similar situations. For example, Oki et al. (2021) found that e-commerce platform users often shop online using internet café facilities for their shopping activities from multiple sites. Similarly, Wijaya and Polina (2014) reported an increase in the use of internet access among users in the public internet cafés for online activities. This implies that e-commerce platform users may be expected to conduct one or two online transactions using internet café facilities, in which they may be at risk, unless they adopt cybersecurity practices.

The study found that the majority of e-commerce platform users had a matric level of education (44.4%), followed by those with a bachelor's pass (27.8%), and those with a diploma (21.1%), who used internet cafés for their shopping purposes. Previous studies highlight that educational levels could have a substantial impact on the use of

internet café facilities among users for online transactions (Houmz et al., 2016; Munyendo et al., 2023; Ojo, 2021). According to Munyendo et al. (2023), users with high school, bachelor's, and college degrees were reported to use the internet café facilities for online transactions. This study found that the highest educational level among e-commerce platform users was matric, which could be the reason why users were using an internet café for their online shopping purposes.

Among e-commerce platform users, online shopping experiences and the use of multiple platforms were prevalent, with the majority, 75.5%, indicating 1 to 6 years of online shopping experience. Most e-commerce platform users (54.4%) indicated that they were shopping online using 2 to 3 e-commerce platforms in shared-access internet cafés in Gqeberha, Eastern Cape. This finding was in line with that of studies by Daramola and Etim (2022) and Oki et al. (2021), who reported that e-commerce platform users with online shopping experiences were increasingly using multiple e-commerce platforms for their shopping activities. This suggests that e-commerce platform users with shopping experiences tend to use multiple platforms for their online shopping activities in internet cafés, where they could be at risk of online attacks if they ignore cybersecurity practices.

The Chi-square test indicated no strong connection with statistical significance (X2 = 6.259, df = 12, p = 0.902) between age and shopping frequency among e-commerce platform users. According to Tutar et al. (2024), as age increases among online shoppers, their shopping frequency on e-commerce platforms decreases inversely among both males and females. Conversely, this study confirmed that age did not have an impact on shopping frequency among e-commerce platform users, who used internet cafés for their shopping activities.

Also, the study confirmed a positive connection with statistical significance ($X^2 = 8.885$, df = 3, p = 0.031) between gender and shopping frequency. This finding was consistent with that of a study by Tutar et al. (2024), who concluded that shopping frequency on e-commerce platforms differs among genders. Shopping frequency on e-commerce platforms was higher in men than in women. Men who actively search for information online about products or services on e-commerce sites were most likely to use the public network for their online activities (Nello-Deakin et al., 2024; Tutar et al., 2024).

This finding suggests that gender plays a crucial role in determining the frequency of online transactions among e-commerce platform users. Notably, men are more likely than women to use internet cafés for shopping purposes.

6.4. General Awareness and Understanding of E-Commerce Platform Users of Cybersecurity Risks and Best Security Practices in the Internet Cafés

The awareness and understanding of cybersecurity risks were found to be moderate**,** with most e-commerce platform users (65%) indicating they had knowledge of these risks. Most of the e-commerce platform users (69%) reported that they understood cybersecurity risks when shopping online in an internet café. Literature reports similar findings on the awareness and understanding of cybersecurity risks in the context of e-commerce and internet cafés (Kuraku et al., 2023; Parker, 2020; Parker & Flowerday, 2021). For example, according to Brandreth and Ophoff (2020), users who were aware of perceived cybersecurity risks when shopping on e-commerce platforms expressed their concerns about those risks. Awareness of perceived cybersecurity risks distresses users when shopping online (Malapane, 2019). More than 120 online shoppers reported being aware of potential cybersecurity risks which affect their perceptions, shopping experiences and intentions during online transactions on e-commerce in the internet cafés (Aliyu, 2019; Hariharan et al., 2023). Hence, this study confirmed that e-commerce platform users were aware of and understood the cybersecurity risks that could be of concern to them, but there were still other users who could be at risk due to a lack of knowledge on cybersecurity risks when shopping online in the internet cafés.

Most of the e-commerce platform users (71%) had knowledge of best security practices, and 69% understood these practices when using internet café facilities in Gqeberha. This finding was consistent with studies by Butler and Butler (2019) and (2015), who reported that e-commerce platform users perceived themselves to be capable of best security practices when shopping on online platforms, which in turn influenced their security practices. Awareness and understanding of best security practices can significantly improve users' shopping activities on e-commerce platforms in the internet café (Al Shakosh, 2024; Resmo, 2024; Sahoo & Gupta, 2019). However,

very few respondents, 29%, indicated a lack of awareness, and 30% showed a lack of understanding of best security practices on the e-commerce platforms in the internet cafés. According to Brandreth and Ophoff (2020) and Verkijika (2019), an inadequate understanding of best security practices has led to poor password practices among e-commerce platform users when shopping online in internet cafés. Yuniar and Fibrianto (2021) reported that online shoppers often lack knowledge of best security practices, yet they continuously engage on e-commerce platforms. Literature reveals that shoppers often engage in unsafe security practices, due to their lack of knowledge on best security practices, when shopping online in internet cafés (Al Shakosh, 2024; Kuraku et al., 2023; Verkijika, 2019). Similarly, Munyendo et al. (2023) reported that inadequate knowledge of best cybersecurity practices affected users in the internet café. Although e-commerce platform users generally had an equitably good knowledge of best security practices, there were still other users who showed inadequate knowledge of best security practices, which could be targeted for potential risks when shopping online in internet cafés.

The Spearman correlation test indicated a positive connection with statistical significance ($r=0.712$; $n=90$; $p <.001$) between awareness and understanding of cybersecurity risks. This finding confirms that cognitive knowledge and cybersecurity risks were closely linked. Furthermore, the study also found that e-commerce platform users were aware and understood cybersecurity risks, but they did not regularly apply cybersecurity practices when shopping on e-commerce platforms in the internet café. This finding was in agreement with studies such as Vanishree (2012) and Wahab et al. (2023), who found that the awareness and understanding of cybersecurity threats did not affect users' intentions to shop on e-commerce platforms. Shoppers were repeatedly making online purchasing decisions and transactions while ignoring cybersecurity practices on e-commerce platforms in the internet café (Al Shakosh, 2024; Netshirando et al., 2021). So, e-commerce platform users could be aware of and understand cybersecurity risks; however, they were less likely to adopt cybersecurity practices when shopping online in internet cafés.

Moreover, the study confirmed a significant connection between shopping frequency and awareness of cybersecurity risks ($X^2 = 18.15$, $df =9$, $p < 0.033$). This finding aligns with a study by Al Shakosh (2024), which reported that users who frequently used

public Wi-Fi or networks showed awareness about cybersecurity risks, causing them to respond differently towards preserving their sensitive information. Increasing awareness about cybersecurity risks can promote better security habits when shopping online in the public network (Al Shakosh, 2024). This implies that e-commerce platform users who repeatedly shop online were more likely to be aware of cybersecurity risks and adopt cybersecurity practices in the internet café settings.

The Spearman correlation tests revealed a positive association with statistical significance ($r=0.770$; $n=90$; $p <.001$) between awareness and understanding of best security practices and cybersecurity practices. According to Kakar et al. (2020), users with knowledge of best security practices were found to be more cautious in applying cybersecurity practices in the internet café. Vega et al. (2022) found that education-based approaches and awareness of best security practices improve users' application of cybersecurity practices on e-commerce platforms. This finding suggests that e-commerce platform users who were aware and understood best security practices were more likely to apply cybersecurity practices when shopping online in the internet café environment.

6.4.1 Sub-question 1: What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?

The findings were consistent across both quantitative and qualitative phases of this study, with quantitative scores supported by themes that discussed the quantitative findings extracted from participants in the qualitative phase. Table 6.2 illustrates the joint display of e-commerce platform users' perceived cyber risks and their impact on shopping behaviour.

Table 6.2: Joint display of quantitative scores was high (85-80%), medium (78-70%) and low (58-50%) with qualitative themes and supporting literature

Quantitative scores	Qualitative Themes	Meta inferences/ Interpretation and supporting Literature
High Scores • 85.56% (mean score 4.23) believed phishing attempts, such as fake emails or websites asking for personal data, were major risks for their online shopping • 82.22% (mean score 4.22) were concerned about their personal and financial information being stolen • 81.11% (mean score 4.17) believed that cybercriminals target online shopping to steal their data • 80% (mean score 4.01) were worried about receiving fake order confirmation emails or scam messages after shopping online	**Cybercrime fallout: from account theft to financial loss** Participants reported various perceived threats, including account thefts, unapproved payments, and stolen identities, which resulted in financial losses. This was caused by the increasing online attacks targeting them to extort them. **Phishing and Smishing Scams** Participants were frequently faced with incidents of these scams while shopping online. They were concerned about the safety of their shopping accounts as many of them were constantly flooded with fake SMS, messages or emails after shopping online on e-commerce platforms.	The findings revealed high perceived vulnerability and severity among e-commerce platform users, who face numerous challenges and perceived threats, including account theft, phishing, and smishing scams. E-commerce platform users reported experiencing monetary losses and stolen credentials while shopping online at internet cafés. These findings were consistent with studies by Babaei and Vassileva (2024) and Ghaderi et al. (2024), who found that user perception of high perceived vulnerability and severity of various cyber-attacks significantly affects their decision not to engage on e-commerce platforms. Similarly, studies have reported that high perceived severity and vulnerability to perceived threats can negatively influence user intention during online activities, leading to avoidance of shopping on some e-commerce websites (Chennamaneni and Gupta, 2023; Omar et al., 2021; Phamthi et al., 2024). As a result, this suggests that e-commerce platform users encountered severe dangers and perceived cybersecurity risks to be highly susceptible during online shopping activities, and were more likely to be cautious or withdraw from future transactions on e-commerce platforms in public internet cafés.
Medium Scores • 78.88% (mean score 4.09) were concerned about being redirected to a fraudulent or suspicious website, especially when making a payment • 75.56% (mean score 4.00) believed that they were at risk of unauthorised transactions or	**Fake retail platforms** Participants reported challenges from being redirected to fake websites and a growing concern about sophisticated, identical websites that target them to disclose personal data and credentials. **Mistrust OTP messages** OTP messages mimicking platform requests prompt e-commerce platform users to access	E-commerce platform users shared their experiences of perceived vulnerability and severity of cybersecurity threats, particularly from sophisticated, redirected fraudulent websites and suspicious activities that impacted their online shopping. They acknowledge that mimicking OTP requests caused them fear and mistrust when shopping online on e-commerce platforms in internet cafés. These findings were supported by a study by Tsai et al. (2016), which reported that personal experiences influenced online perceptions of severity. Similarly, previous studies found that fear of manipulative messages and perceived vulnerability influenced user intentions and behaviour towards phishing attacks and engagement on shopping platforms (Boerman et al., 2021; Jansen and Van Schaik, 2019). This implies that e-commerce platform users were

Quantitative scores	Qualitative Themes	Meta inferences/ Interpretation and supporting Literature
suspicious activities on their bank or payment accounts • 70% (mean score 3.91) were worried about falling victim to phishing scams or fake shopping websites	their accounts after shopping. Participants reported that these attacks instilled extreme fears and mistrust in their online shopping activities.	affected by perceived cybersecurity threats, such as OTP messages and fake retail platforms, when shopping online in internet cafés in Gqeberha.
Low Scores • 58.89% (mean score 3.74) believed that shopping on e-commerce platforms in an internet café significantly increases their cybersecurity risks • 57.78% (mean score 3.59) were concerned about having their account being compromised when using e-commerce platforms • 56.67% (mean score 3.56) believed that e-commerce platforms do not provide enough protection against cybersecurity threats	**Risk of disclosing personal data** Participants were lured into entering sensitive information on an e-commerce platform in internet cafés. They revealed that putting personal information on unverified websites and in unprotected internet cafes further amplified their vulnerability to various cybersecurity threats. **User behaviour in e-commerce** Participants were concerned about perceived cybersecurity risks, but some shopping habits led to their accounts being hacked due to disregarding perceived risks on e-commerce platforms in internet cafés.	The findings revealed that perceived vulnerability serves as evidence among e-commerce platform users regarding the risk of personal data disclosure, which could lead to identity theft or compromised accounts in unprotected internet cafés. These findings correspond with those of a study by Torten et al. (2018), who reported that user transactions and personal data were influenced by perceived vulnerability when facing unfavourable online security hazards. This implies that perceived threats could pose significant challenges for e-commerce platform users, especially if their data falls into the wrong hands in shared-access internet cafés. However, e-commerce platform users' behaviour showed low perceived severity by choosing to ignore online threats, even when they perceived risks, until it happened to them. These findings were in line with previous studies, which emphasised that if perceived severity is low, it could reduce motivation to act, affecting overall perceived threats (Haag et al., 2021; Papagiannidis et al., 2023). According to Mamat et al. (2023), perceived benefits of risky behaviour, such as the convenience of online shopping, can affect the threat appraisals. Users believe that the benefits of using e-commerce sites outweigh the risks when shopping online on e-commerce platforms (Grobler et al., 2021). This implies that e-commerce platform users may worry about perceived threats, but their shopping behaviours online might not change unless they face severe consequences or learn about the potential damage these threats have caused to other users.

6.4.2 Sub-question 2: How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?

These findings were consistent with both quantitative and qualitative findings on e-commerce platform users on basic cybersecurity measures in a shared internet cafés environment. It shows how these measures affect user satisfaction and overall shopping experiences. The joint display demonstrates that the quantitative scores, ranging from high (86-80%) to medium (78%), support with the qualitative data from e-commerce platform users in this subsection.

Table 6.3: Joint Display visual for basic cybersecurity practices and supporting literature

Quantitative Scores	Qualitative Themes	Meta inferences/ Interpretation and supporting Literature
High Scores • 86.67% were aware of creating a unique password for their accounts • 84.45% understood the risks of clicking on links in unsolicited emails or texts that appear to be from e-commerce platforms • 82.22% were aware of reviewing their bank statements for unauthorised charges regularly	**Knowledge of security measures and experiences** Participants' accurate knowledge of cybersecurity practices was found to be a contributing factor to their positive experiences. Participants expressed awareness of effective cybersecurity measures when shopping on e-commerce platforms. Their internet skills and cybersecurity knowledge enabled them to take charge of their online safety, satisfaction and overall experiences. **Password management in shared environment** Participants shared their experiences of managing passwords while shopping on multiple e-commerce platforms and their awareness of password managers. They explained the use of password managers, such as Google Authentication, to secure their accounts when	E-commerce platform users who showed awareness and knowledge demonstrated high self-efficacy in their ability to adopt protective behaviour even when the platforms did not provide basic cybersecurity measures. These findings were in line with a study by Boerman et al. (2021) that individuals with high self-efficacy were better at managing security risks. Similarly, individuals with self-efficacy and knowledge about cybersecurity measures were more likely to protect their online activities (Lee & Seomun, 2021). Cybersecurity awareness and experiences enhance an individual's self-efficacy to adopt protective behaviours, such as cybersecurity practices, for their safety (Debb & McClellan, 2021; Kalhoro et al., 2021). This suggests that e-commerce platform users' high self-efficacy was linked to cybersecurity knowledge, contributing to their satisfaction and overall shopping experiences, while reducing perceived threats when shopping online in an unprotected internet café. The awareness of basic cybersecurity practices, such as using a password manager, was linked to self-efficacy and response efficacy among e-commerce platform users shopping from an internet café. These findings were similar to previous studies on self-efficacy and response efficacy of PMT that cybersecurity awareness and perceived threats influence the adoption of protective behaviours (Mou et al., 2022; Roberts and Rahman, 2021). Jamil (2023) found that prior knowledge and experiences influence self-efficacy and

Quantitative Scores	Qualitative Themes	Meta inferences/ Interpretation and supporting Literature
	shopping on e-commerce platforms, thereby preventing them from falling victim to account theft. Some participants admitted that they only saved their passwords on their devices and not the internet café's system when shopping online in public internet cafés.	response efficacy in adopting cybersecurity practices, such as installing a password manager, in a business environment. This finding showed that awareness, shopping experiences and perceived risks contributed to e-commerce platform users' adoption of password managers, as safety measures to safeguard their online shopping activities in the public internet cafés. This could enhance users' satisfaction and shopping experiences in the internet cafés environment.
Medium Scores • 78. 89% had knowledge of secure websites (HTTPS) • 77.88% were aware of the importance of using reputable third-party payment processors (e.g. PayPal, Google Pay and Apple Pay)	**Anticipated security measures in building user confidence** Foreseen platform security measures increased participants' beliefs in recommended protective actions. Participants revealed that the visibility of these security measures enhanced their trust in shopping on e-commerce platforms in an internet café environment. **Adoption of advanced payment methods** Participants who have heard or experienced cyber risks tend to seek more knowledge on advanced payment methods to safeguard their future transactions. There was evidence that participants adopted protective behaviours to prevent future incidents, such as using virtual cards and setting their card limit to zero after completing online transactions.	The visibility of security measures on e-commerce websites could guide e-commerce platform users and boost response efficacy when provided on the platforms for the users. These findings were similar to a study by Humaidi and Abdallah Alghazo (2022), who stressed that security measure awareness influences individual response efficacy, leading to enhanced protective behaviour and active engagement in cybersecurity practices. According to Idayani et al. (2024), consumers may be more motivated to respond effectively to perceived threats if platforms implement transparent security features, thereby enhancing user acceptance of protection measures. This implies that e-commerce platform users perceived security measures as a means to strengthen their protective behaviours, enabling them to complete online shopping activities with confidence and enjoy positive experiences. The adoption of advanced payment methods was influenced by the e-commerce platform users' prior experiences and knowledge, leading to high self-efficacy in adopting cybersecurity practices during online transactions. According to Marikyan et al. (2022), user experiences of perceived dangers positively increase self-efficacy and intentions to adopt cybersecurity practices, such as advanced technology. User experiences, knowledge, and perceived threats in online shopping platforms can significantly enhance self-efficacy and behavioural control, leading to the adoption of protective measures such as blockchain technology (Mat Dawi et al., 2024; Oh et al., 2023). This study found that past experiences and knowledge heightened self-efficacy among e-commerce platform users to adopt advanced payment methods to prevent financial fraud when shopping on e-commerce platforms in the internet cafés environment.

Moreover, the extent of the implementation of cybersecurity measures on users' satisfaction and overall shopping experiences was discussed, with quantitative scores ranging from high (67-41%) to Medium (25-15%) to low (12-1%), supported by qualitative themes and relevant literature.

Table 6.4: Joint display visual on active use of cybersecurity measures among e-commerce platform users

Quantitative Scores	Qualitative Themes	Meta inferences/Interpretation and supporting Literature
High Scores • 41.11% to 66.67% of the respondents always follow cybersecurity measures.	**Verification practices and purchasing decisions** Participants reported consistently applying cybersecurity measures, including verifying websites, checking for platform logos, and reviewing customer feedback, before making purchasing decisions on these platforms. Participants' previous shopping experiences on cyber risks informed their purchasing decisions to adopt cybersecurity measures in the internet café environment.	E-commerce platform users demonstrated high self-efficacy in actively using cybersecurity measures, which in turn influenced their shopping decisions and platform selections during online shopping activities. According to Haque et al. (2020) and Schneider and Rahman (2021), self-efficacy plays a critical role in shaping individuals' decisions to adopt protective behaviours, motivating them to protect against cyber threats through increased awareness, education, and well-designed cybersecurity measures. Studies show that high self-efficacy is essential for effective decision-making regarding online security during online transactions to protect sensitive information (Haag et al., 2021; Prasetyo and Wahab, 2022; Tsai et al., 2016). The findings reveal that e-commerce platform users with high self-efficacy were due to their knowledge of cybersecurity measures. So, this could enhance their purchasing decisions, satisfaction and trust, and could lead to positive shopping experiences when making online transactions and averting perceived threats in the internet cafés environment.
Medium Scores • 15.56% to 27.78% respondents often follow cybersecurity measures. • 18.89% to 24.44% respondents sometimes follow cybersecurity measures.	**Preference for recognised sites** Participants who demonstrated the ability to recognise websites enjoyed transactional safety and satisfaction, compared to those who applied cybersecurity measures only when they remembered. They expressed avoiding unfamiliar websites, which helps them to prevent perceived cybersecurity threats and enhance online safety and their shopping experiences. However, participants' over-	E-commerce platform users perceived that online safety and institutional trust were linked to the recognition and validity of e-commerce websites. They showed self-efficacy by adopting protective behaviour such as avoiding unfamiliar websites for transitional safety. These findings were similar to those of a study by Prasetyo and Wahab (2022), who purported that self-efficacy, perceived severity, and safety habits influence users' loyalty to e-commerce platforms. Self-efficacy meaningfully impacts users' behavioural intention to adopt e-commerce platforms (Pobee, 2021). However, literature revealed that individuals with high self-efficacy and confidence in the existing preventive measures, such as over-reliance on recognised websites, were less likely to take protective measures (response efficacy) due to their overconfidence in the platforms to protect them when shopping online (Bekkers et al., 2023; Tsai et al., 2016).

Quantitative Scores	Qualitative Themes	Meta inferences/Interpretation and supporting Literature
	reliance on well-known e-commerce platforms often leads them to overlook cybersecurity measures when shopping online.	This was also emphasised in a study by De Kimpe et al. (2021), who found that overconfidence in internet trust could undermine motivation for preventive measures, specifically on the role of self-efficacy. This study found that e-commerce platform users perceived renowned platforms as having already implemented cybersecurity measures to protect them from online dangers, which in turn improved their trust and satisfaction in the platforms. Conversely, perceived trust and reliance on renowned sites could undermine consistent adoption of cybersecurity measures even when users were capable of adopting protective habits (self-efficacy). They may not always follow protective behaviours such as adopting cybersecurity measures due to the perceived trust in the e-commerce platforms (response efficacy).
Low Scores • 3.333% to 12.22% respondents rarely follow cybersecurity measures. • 1.111% to 10% respondents never follow cybersecurity measures.	**Low legitimacy awareness of safety features** Participants expressed their ignorance of safety features, which led to financial losses and dissatisfaction with the platforms. The lack of knowledge on how to use cybersecurity measures for online shopping and safety features has made e-commerce platform users prone to or victims of cybersecurity attacks, leading to negative shopping experiences among them.	This finding showed that a lack of knowledge on cybersecurity measures exposed e-commerce platform users to various cybersecurity risks. E-commerce platform users exhibited low response efficacy and self-efficacy in implementing protective behaviours, including an inability to identify legitimate websites and other security measures. The findings were consistent with those of a study by Skjelvik and Vestad (2023), who found that a lack of cybersecurity knowledge led to low self-efficacy and response efficacy in adopting cybersecurity practices, even when the perceived threats were severe and consequential. Also, Kariuki et al. (2024) found that inadequate cybersecurity awareness led to low self-efficacy and response efficacy, causing users to be more susceptible to cybersecurity threats and recommending technical information to enrich safer digital practices. As a result, this finding suggests that inadequate knowledge of safety features hinders e-commerce platform users' ability to apply cybersecurity measures, potentially increasing their vulnerability and leading to negative experiences and dissatisfaction when shopping online in internet cafés.

6.4.3 Sub-question 3: How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?

These findings were in accordance with both quantitative and qualitative results on the extent of e-commerce platform users' perceived cybersecurity threats and the impact of the effectiveness of cybersecurity practices when conducting online transactions. Table 6.5 presents the joint display visual for the quantitative scores: high (92-84%), medium (76-65%), and low (52%). This is supported by the analytical themes derived from the participants' qualitative data and relevant literature.

Table 6.5: E-commerce platform users' perceived risks and the impact of the effectiveness of cybersecurity practices

Quantitative Scores	Qualitative Themes	Meta inferences / Interpretation and supporting Literature
High Scores • 92.2% (mean score 4.47) believed that cybersecurity practices, including strong passwords and two-factor authentication, effectively reduce cyber threats. • 84.4% (mean score 4.41) avoiding untrustworthy websites.	**Confidence in security routines** Participants expressed positive attitudes towards the effectiveness of cybersecurity practices when confronted with perceived cyber risks. They believe that cybersecurity practices, such as using strong passwords and avoiding untrustworthy websites, are easy to follow because they help ensure positive shopping experiences. Participants with extensive shopping experience and a history of encountering cybersecurity risks demonstrated interest and positive attitudes towards adopting cybersecurity routines for their safety in unprotected internet cafés.	The finding reveals a strong link between threat and coping mechanisms; there was evidence of willingness and positive attitudes among e-commerce platform users towards protective habits like embracing cybersecurity practices to avert perceived threats. According to Van Bavel et al. (2019) and Visinescu et al. (2016), coping mechanisms were more effective in taking action against perceived threats to improve security behaviours, influencing individuals' decisions, perceived risks, and attitudes to enhance protective strategies. Strong threat appeals significantly influence attitudes and intentions toward precautionary behaviours (Jansen and Van Schaik, 2019). Similarly, Jamil et al. (2024) stressed that all PMT constructs except threat susceptibility were successful predictors of the effectiveness of safe cyber practices. This study found that threat and coping appraisals could influence e-commerce platform users' towards the effectiveness of cybersecurity practices. User trust and attitude in cybersecurity practices could reduce perceived risks, influenced their decisions to believe in protection behaviours during online transactions in the internet café.

Quantitative Scores	Qualitative Themes	Meta inferences / Interpretation and supporting Literature
Medium Scores • 76.6% (means score 4.10) limit online shopping activities due to cybersecurity concerns on unsecured websites. • 76.6% (mean score 4.04) reconsidered completing their online purchase even when the website is secure due to concerns about cybersecurity threats. • 73.4% (mean score 4.04) were influenced to take extra security measures due to fear of cybersecurity risks. • 67.8% (mean score 4.06) checking for security indicators (padlock, SSL) for cybersecurity risks before making a purchase. • 65.5% mean score 3.89) regularly update their passwords and enable two-factor authentication to enhance their cybersecurity. • 65.6% (mean score 3.97) regularly check for cybersecurity updates or tips to improve online shopping security.	**Risk perception and feelings of online safety in digital platforms** Participants showed mixed feelings about the perception of cybersecurity threats. They expressed their worry about various cyber threats, including identity theft and credit card fraud. Perceived cybersecurity threats influence participants' views on the adoption of cybersecurity practices for their own safety on digital platforms.	The extent to which e-commerce platform users perceive cybersecurity threats as severe or believe they could happen to them influences the effectiveness of their protective habits on digital platforms. These findings align with a study by Wang (2023), which emphasised that users perceiving threats with negative consequences trigger fear, leading to effective coping appraisals that promote protective habits and reduce online service usage. Other studies revealed that threat and coping appraisals significantly impact risk perceptions and protection behaviours (Boerman et al., 2021; Mousavi et al., 2020). User experiences and risk perceptions contributed to the effectiveness of security mechanisms (Liu et al., 2018). This implies that e-commerce platform users' adoption of coping mechanisms was based on their different views on threat appraisals and experiences of online safety in the digital platforms. The fear of being vulnerable to online attacks and their consequences could influence the effectiveness of cybersecurity practices in digital platforms when shopping in internet cafés.
Low Scores • 52.3% (mean score 3.47) find difficulty in applying security measures.	**Frustration and missing instructions in e-commerce security design** Participants expressed frustration with platforms that fail to provide clear instructions on implementing cybersecurity practices. This led to confusion, time consumption, verification delay, and inconvenience among participants in adopting protective behaviour when shopping on those platforms. Participants were discouraged, even	The findings revealed a lack of clear directions and delays in implementing cybersecurity practices on affected e-commerce platforms, hindering users' ability to apply these practices effectively. This diminishes coping mechanisms, resulting in high response costs even when users are motivated to adopt them. These findings were consistent with those of a study by Blythe and Coventry (2018), who stressed that coping appraisals were more predictive, but response costs could be a barrier to protective behaviours. Increased response co

Quantitative Scores	Qualitative Themes	Meta inferences / Interpretation and supporting Literature
	when they perceived threats to be severe, and showed interest in adopting protective behaviours. .	sts negatively impact the use of cybersecurity practices (Jamil et al., 2024). Babaei and Vassileva (2024) and Pobee (2021) highlighted that higher perceived severity and lower response costs encouraged users to engage with information manipulative design in e-commerce and e-vendors. E-commerce platforms should create user-friendly websites to enhance user protection by improving their transparency and accountability with protective measures to reduce user stress faced when shopping on their platforms (Babaei & Vassileva, 2024; Pobee, 2021). Therefore, this study found that high perceived response costs, such as inconvenience, time delay, frustration, and confusion, were identified as major challenges among e-commerce platform users. This affected the effectiveness of cybersecurity practices and protective behaviours, and it could weaken self-efficacy and response efficacy, even with high awareness of threat appraisals among users in the internet café environment.

6.4.3.1 E-commerce platform users perceived risks and the impact of the effectiveness of cybersecurity practices in the internet café settings

The Spearman correlation test revealed a strong, statistically significant connection (r=0.471; n=90; p=0.000) between perceived cybersecurity threats and the effectiveness of cybersecurity practices among e-commerce platform users, particularly in terms of checking for security indicators, regularly updating passwords, and enabling two-factor authentication. According to Kuppusamy et al. (2022) and Tawalbeh and Muheidat (2023), threat and coping appraisals strongly influence users towards protective measures such as embracing cybersecurity practices. Users who perceive high threats or online attacks are motivated to adopt response efficacy and self-efficacy, engaging in cybersecurity exercises such as enabling two-factor authentication and regularly updating passwords to mitigate online risks (Mashiane & Kritzinger, 2021; Mtambeka et al., 2023; Sajikumar et al., 2024). This implies that e-commerce platform users' perception of cyber threats was more likely to influence their effectiveness in cybersecurity practices, such as using 2FA or habitually updating passwords when shopping online in internet cafés.

The finding confirms that e-commerce platform users' perceived threats were key influencers of the effectiveness of cybersecurity practices in the internet café environment. There was a strong statistical relationship with significance between fear of perceived threats, such as untrustworthy e-commerce websites (r=0.379; n=90; p=0.000), reconsidering purchases even on secure e-commerce platforms (r=0.452; n=90; p=0.000), and cybersecurity practices, such as checking for cybersecurity updates (r=0.452; n=90; p=0.000). The findings were similar to previous PMT studies on how perceived threat affected users to react differently towards protective behaviours to engage cybersecurity behaviours on e-commerce sites (Almansoori et al., 2023; Alsmadi et al., 2024; Avalos et al., 2022). For example, according to Omar et al. (2021) and Phamthi et al. (2024), users who perceived strong fear or severe threats were more likely to be motivated to take protective actions such as avoiding untrusted sites or adopting extra cybersecurity practices. Therefore, this study suggests that perceived cybersecurity fears or severe risks were more likely to strongly

motivate e-commerce platform users to believe in the effectiveness of cybersecurity practices for their safety during online transactions in the internet cafés environment.

6.4.4 Sub-question 4: What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping?

The findings for this research question reveal recommended cybersecurity practices that can be implemented to strengthen shopping experiences for e-commerce platform users when shopping on e-commerce platforms in internet café settings.

6.4.4.1 Building trust through perceived data protection and risk disclosures

E-commerce platforms should be transparent about their data protection and risk disclosure practices on their sites to promote user trust and confidence in their e-commerce platforms. This study suggests that trust, combined with clear data protection and risk disclosures, can encourage e-commerce platform users to select specific platforms for their online shopping activities. This finding aligns with a study by Sajikumar et al. (2024) on PMT and privacy concerns, which reported that increased awareness of cybersecurity risks enhances user protection and security during digital or mobile transactions, thereby reducing privacy concerns. According to PMT constructs, data privacy and cybersecurity activated fears of data loss and reduced trust in the platform (Terlizzi et al., 2019). Users' self-withdrawal intentions from platforms were influenced by their perception of privacy threats, concerns and protection effectiveness (Chennamaneni & Gupta, 2023; Meier et al., 2020). This implies that disclosing risks and data protection could reduce the fear of perceived risks among e-commerce platform users, encouraging them to use selected platforms when shopping online in untrusted internet cafés.

6.4.4.2 Integration of biometric verification to e-commerce platforms

E-commerce platforms should consider integrating biometric verification into their websites to enhance user security and strengthen their online presence. The design of e-commerce platforms should incorporate face recognition and be user-friendly,

providing a competitive edge over other platforms. This finding was similar to studies by Oh et al. (2023) and Zawaideh et al. (2023), who concluded that advanced technology acceptance will enhance self-efficacy, promoting its adoption in e-commerce platforms. In PMT studies, e-commerce businesses were encouraged to fortify their security measures through advanced technology to ensure the safe use of online shopping activities (Osita et al., 2022) and to boost response efficacy in their platforms (Gumasing et al., 2023). The study recommends implementing face recognition as a high-level cybersecurity measure to enhance users' trust in e-commerce platforms. As a result, e-commerce platform users believe that biometric verification, such as face recognition, could enhance their response efficacy and self-efficacy, particularly for those with low digital literacy. It could further reduce perceived response costs and improve their online shopping experiences and satisfaction.

6.4.4.3 Websites’ verification cues processes

E-commerce platforms should display clear visual cues, such as verification links, recognised logos, and customer reviews, which can increase users' confidence and trust in their sites or platforms. Consistent with that of studies by Shiri et al. (2024) and Teofilus et al. (2020), who reported that e-commerce businesses should be more attentive to terms and conditions and use visual cues to make secure information more prominent to improve online shopping intentions. The study found that the availability of visual cues improves self-efficacy and response efficacy for e-commerce platform users to navigate these websites or platforms. Perceived evidence of visible verifying cues on their sites promotes the adoption of protective behaviour and cybersecurity practices. According to Blythe and Coventry (2018) and Jamil et al. (2024), self-efficacy and response efficacy are successful key facilitators for safe cybersecurity practices. This implies that e-commerce platform users who frequently use internet café facilities feel secure when they observe visible clues as an indication of trusted websites, thereby reducing perceived cybersecurity threats when shopping online in an unsecured public internet café.

6.4.4.4 Promotion of enhanced, secure, and flexible payment options in e-commerce

E-commerce needs to provide alternative secure payment options, such as a virtual card, apart from the traditional card payment methods. The study recommends other payment options, such as virtual cards, as enhanced security features for e-commerce platform users. The promotion of virtual cards for online shopping among users could prevent unauthorised payment or financial fraud. This could increase self-efficacy for e-commerce platform users to actively adopt cybersecurity practices in an unprotected internet café in Gqeberha. This finding was in line with previous PMT studies that secure payment gateways improve security mechanisms if adopted by the e-commerce platforms (Hossain et al., 2024; Osita et al., 2022; Zawaideh et al., 2023). According to Hamzah (2024) and Shiri et al. (2024), self-efficacy improves user motivation to adopt effective mechanisms, such as secure payment adoption, to combat threats and reduce vulnerability through education. Therefore, this implies that educating users on other secure payment options, such as virtual cards on e-commerce platforms, could increase e-commerce platform users' confidence (self-efficacy) to complete online payments successfully. Furthermore, it could reduce perceived threats during shopping activities, especially in a public internet café.

6.4.4.5 Adoption of a password manager

The adoption of a password manager could prevent e-commerce platform users from having their accounts hacked in internet cafés. The study reveals evidence of self-efficacy and response efficacy connected to users' experiences and education. This could encourage them to make deliberate choices to adopt protective habits, such as using a password manager, to prevent perceived threats and account theft. This finding was supported by Roberts and Rahman (2021), who reported that effective training programs could improve self-efficacy and response efficacy to adopt protective habits. Self-efficacy, experiences, knowledge, and perceived risks directly impact user trust in the adoption of a password manager (Debb & McClellan, 2021; Marikyan et al., 2022; Tian, 2024). This suggests that education and experiences can significantly influence password manager adoption, potentially enhancing e-

commerce platform users' self-efficacy and response efficacy in adopting cybersecurity practices during online shopping in internet cafés.

6.4.4.6 Improving cybersecurity habits with platform-supported user education

The study suggests there is a need for platform-based education to continually provide information on the importance of cybersecurity practices for e-commerce platform users. Platform-supported education could play a critical role in enhancing the self-efficacy of users with prior knowledge on perceived threats to feel more confident in adopting cybersecurity practices during their online transactions in the internet cafés environment in Gqeberha. According to Kalhoro et al. (2021) and Skjelvik and Vestad (2023), better education, training and understanding of cybersecurity risks prepared users for social engineering attacks, with self-efficacy being strongly linked to confidence in performing cybersecurity practices. Likewise, Dodge et al. (2023) emphasised the importance of effective communication strategies, gamified simulation and personalised approaches to improving self-efficacy and cybersecurity practices while reducing threat fatigue. Promoting user-centred approaches that see users as contributors to cybersecurity practices and recommending educating about risks by sharing victim-impact stories to enhance user engagement in the cybersecurity practices (Dodge et al., 2023). This implies that platform-supported education could enhance the self-efficacy of e-commerce platform users, enabling them to successfully implement cybersecurity practices and trust the platforms for their online safety and satisfaction, even in the face of perceived cybersecurity threats in public internet café environments.

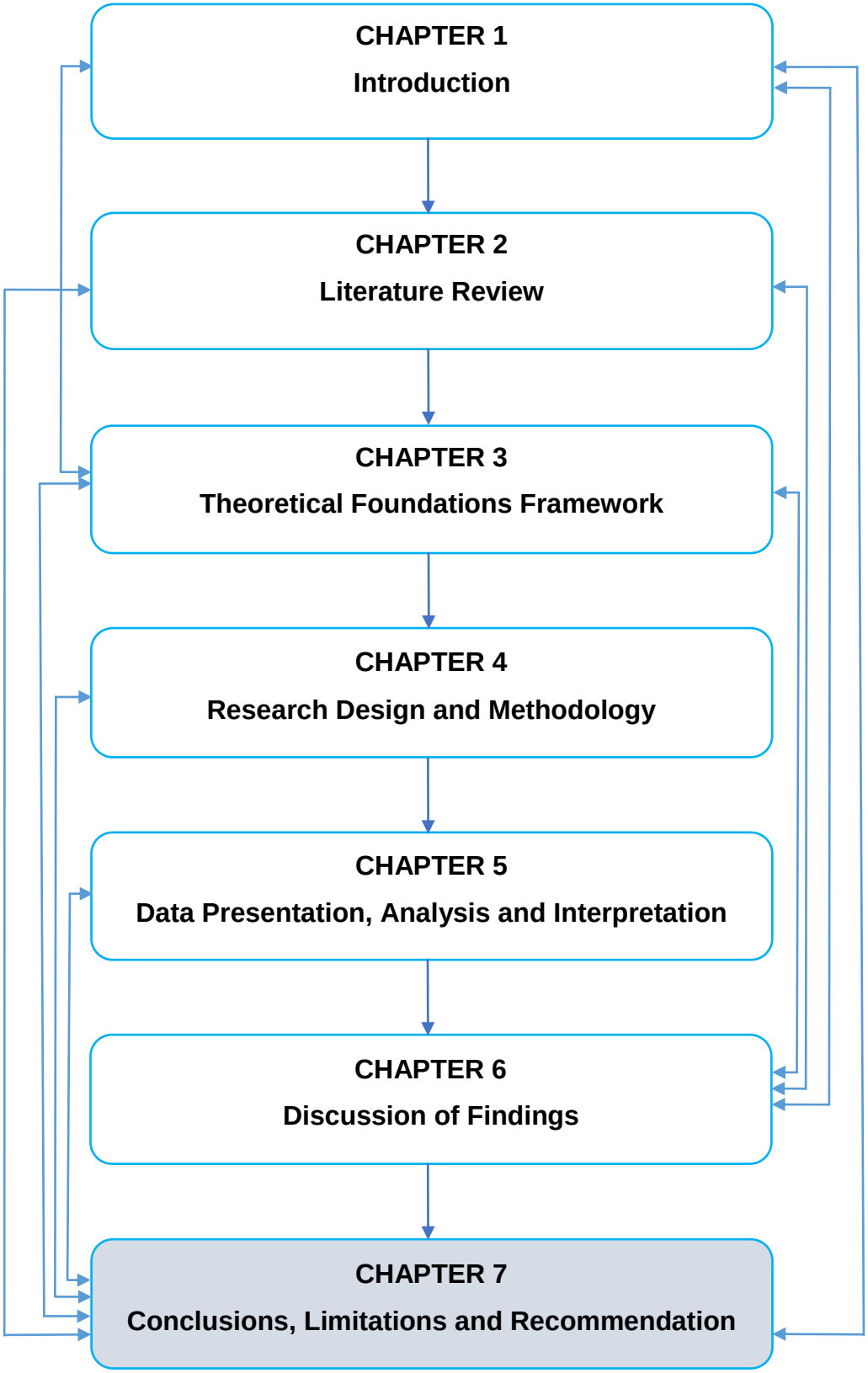
6.5. Conclusion

This chapter presented the findings of this research project, explaining how e-commerce platform users in Gqeberha were confronted with various cybersecurity threats in the internet café facilities for their online transactions. It highlighted serious concerns stemming from perceived threats, which led to high perceived severity and vulnerability, including financial losses and stolen credentials, ultimately resulting in

negative experiences among users. However, some users' behaviours did not change when shopping online until they faced severe consequences or the potential damage caused to other users. The study found that past experiences, awareness and prior knowledge influenced their coping mechanisms. Those who were knowledgeable and aware of basic cybersecurity practices were able to demonstrate high response efficacy and self-efficacy to implement cybersecurity measures when shopping online in the internet café setting. E-commerce platform users lacking knowledge of basic cybersecurity practices and shopping experiences were affected online, despite perceiving threats as severe, due to their low response efficacy and self-efficacy in using cybersecurity measures on these platforms. Furthermore, the study recommended cybersecurity practices that could be applied for future transactions to reduce perceived threats and improve shopping experiences in the internet café environment in Gqeberha, Eastern Cape.

The next chapter will discuss conclusions, limitations and recommendations emanating from this study.

CHAPTER 7: CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS



7.1. Introduction

The preceding chapter presented findings for e-commerce platform users, supported with literature. This chapter aims to provide a synopsis for this study conclusions, contributions, limitations and recommendations for the furtuer study.

7.2. Overview of the study

The main objective of this study was to assess the impact of cybersecurity practices on the experiences of online shoppers with e-commerce platforms in Gqeberha using PMT. The study selected three prominent internet cafés that cater to the diverse range of e-commerce platform users, utilising their services to conduct this research. The complete thesis contains seven chapters addressing different facet of this research study.

Chapter 1 presented the research context in which it explains the problem being faced by e-commerce platform users and emphasised the importance of cybersecurity practices when shopping on e-commerce platforms in the internet café. The study was designed to answer four sub-research questions. Table 7.1 presents the research questions that were addressed in this research. The research questions were examined using both theoretical and practical standpoints, conducted with scholarly sources and databases. The literature was presented in Chapters 2 and 3. Chapter 2 presented a literature review on cybersecurity threats, common cybersecurity threats and cybersecurity practices within the context of e-commerce and internet cafés. Chapter 3 explained the current state of literature on protective motivation theory and addressed the gap in the literature for this study. Chapter 4 provided a comprehensive account of the research design and methodology adopted for this research. Resarch Onion Model was followed as the research process, utilising explanatory sequential mixed-methods. Quantitative data were collected employing self-administered questionnaires for the first phase, followed by an in-depth interview for the qualitative phase. SPSS version 29 was utilised to analyse the quantitative data. Reflexive thematic analysis was conducted and analysed using Atlas.ti 25 for the qualitative data, presenting the findings in themes and sub-themes. Chapter 5 presented the findings of the results for the interpretation and analysis of both quantitative and

qualitative phases. In Chapter 6, the discussion of findings was explained and controlled with detailed literature for this study.

Table 7.1: The research questions itemise for this study

Sub-research questions
1. *What cybersecurity threats do e-commerce platform users in internet cafés perceive to be influencing their online shopping behaviour?*
2. How do basic cybersecurity measures on e-commerce platforms affect users' satisfaction and shopping experiences in internet cafés?
3. How do perceptions of cybersecurity threats among e-commerce platform users in internet café influence their belief in the effectiveness of cybersecurity practices when conducting online transactions?
4. What cybersecurity practices can e-commerce platform users adopt to improve their experience while using an internet café for online shopping?

7.3. Conclusions

The study conclusions are presented using each of the sub-research questions and the main study objective.

7.3.1 Perceived threats influencing e-commerce platform users in internet cafés and their online shopping behaviour

E-commerce platform users were confronted with perceived severe risks, such as phishing and smishing attacks, and were highly vulnerable to online threats on e-commerce platforms in the internet café environment. Perceived susceptibility of personal information posed significant challenges for e-commerce platform users, particularly when their information fell into the wrong hands in shared-access internet cafés. The study concluded that perceived threats, such as account thefts and fake platforms, caused negative experiences due to high financial losses and compromised accounts reported among e-commerce platform users shopping online in internet cafés. Another type of perceived threat was the fear of receiving OTP messages after shopping online in internet cafés. Their perception of online threats led them to be

more cautious or withdraw from platforms they did not trust when shopping online in internet cafés. However, the study found that while some e-commerce platform users were concerned about perceived threats, others' behaviour remained unchanged; they either ignored these threats or were unaware of the potential consequences or damage they could cause to other users in public internet cafés.

7.3.2 The effect of basic cybersecurity measures on e-commerce platforms on users' satisfaction and shopping experiences in internet cafés

Cybersecurity knowledge and experiences influenced e-commerce platform users' adoption of basic cybersecurity practices, such as password managers and advanced payment methods, to safeguard their shopping accounts and prevent financial fraud in internet cafés. The study concluded that e-commerce platform users with perceived risks, knowledge, and past experiences demonstrated high self-efficacy and response efficacy, contributing to positive online shopping experiences and satisfaction in an unprotected internet café environment. Perceived visibility of cybersecurity measures on e-commerce platforms increased e-commerce platform users' protective behaviours and heightened self-efficacy to complete online shopping activities, and led to positive shopping experiences in a public internet café.

Perceived security measures and verification practices increased user trust and shopping decisions, which in turn boost their self-efficacy to prevent perceived threats when making online transactions from public internet cafés. E-commerce platform users believed that renowned platforms had already implemented basic security measures to protect them from online attacks and ensure their safety when shopping online in public internet cafés. However, perceived trust and reliance on renowned sites destabilised e-commerce platform users' ability to consistently adopt cybersecurity measures (Self-efficacy). Even when platforms implement security measures, they may not always apply them when using internet café facilities for online shopping purposes (response efficacy). Moreover, the study concluded that a lack of knowledge about cybersecurity measures prevented some e-commerce platform users from following and implementing those security measures. This led to

low response efficacy and self-efficacy among them, making e-commerce platform users prone to online attacks, which resulted in negative experiences and dissatisfaction when shopping online in internet cafés.

7.3.3 E-commerce platform users' perceptions of cybersecurity threats and their impact on the effectiveness of cybersecurity practices in internet cafés

The study concluded that threat appraisals influenced e-commerce platform users' coping mechanisms towards the effectiveness of cybersecurity practices in the internet café environment. Their adoption of coping mechanisms was based on different views of threat appraisals and experiences of online safety in the digital platforms. Perceived severity and fear of being vulnerable to cyber threats stimulated their response efficacy and self-efficacy to actively believe in the use of cybersecurity practices, to prevent future incidents on e-commerce platforms in the internet cafés. E-commerce platform users' trust and positive attitude towards the effectiveness of cybersecurity practices reduce perceived risks, influencing their decisions to confidently adopt protective behaviours during online transactions in the internet cafés setting. The study concluded that the perception of threats influenced e-commerce platform users to effectively motivate them to use 2FA or habitually update their passwords when shopping online in internet cafes. Moreover, even when some e-commerce platform users perceived severity, the lack of instructions and frustrations on some platforms weakened their self-efficacy and response efficacy in using cybersecurity practices effectively. This, combined with high perceived response costs such as inconvenience, time delay, and confusion, was found to be a major challenge, affecting their capability to adopt cybersecurity practices for their safety successfully.

7.4. Contributions

Several contributions for this research are rooted in the theoretical framework of protection motivation theory and the methodology employed to collect and analyse primary data, thereby addressing the research questions. The study utilised the PMT to assess the impact of cybersecurity practices on the experiences of online shoppers

within e-commerce platforms in Gqeberha. Many of the study aspects were directly related to the context of the e-commerce platform users in the internet café. It was limited to three selected internet cafés, with diverse clients, and were strategically located at busy places in the centre of Gqeberha city.

The main contribution of this study was the recommendation of cybersecurity practices that could be adopted by both the e-commerce platforms and e-commerce platform users in Gqeberha. The recommended cybersecurity practices can enhance the e-commerce platform users' experiences, particularly in highly sensitive environments like internet cafés, thereby reducing online attacks. E-commerce platform users have called for e-commerce platforms to embed specific cybersecurity practices on their sites to facilitate their shopping experiences, particularly in public environments like internet cafés.

One of the study's main contributions was suggesting enhanced cybersecurity practices, such as face recognition, password managers, and visual cues, for both e-commerce platform users and platforms themselves. The Protective Motivation Theory was another significant contribution that revealed how various aspects of the component, such as perceived vulnerability and severity, powerfully influenced response efficacy, self-efficacy, and response costs among e-commerce platform users.

Furthermore, this study contributed to the existing body of knowledge on the application of protection motivation theory to cybersecurity practices and e-commerce platform users' experiences within the context of e-commerce and internet cafés in Gqeberha, Eastern Cape. The study conducted a literature review to understand how the Protection Motivation Theory (PMT) has been applied to users' cybersecurity practices in e-commerce, leading to a review of 60 articles from 2014 to 2024 on PMT within the e-commerce context produced by this study.

Methodologically, the researcher utilised explanatory sequential mixed methods and adopted a pragmatics philosophy to address the practical challenges of cybersecurity practices faced by e-commerce platform users shopping online in internet café

environments. These methods enabled the researcher to utilise statistical methods for quantitative data and reflexive thematic analysis for qualitative data. The methodology in this study could be adopted to solve the practical problems confronting e-commerce platform users in Gqeberha, Eastern Cape. This study is the first to be conducted in Gqeberha, Eastern Cape, on cybersecurity practices using Protection Motivation Theory for e-commerce platforms. It is also one of the few that combines explanatory sequential mixed methods to explore the protection motivation theory in the context of e-commerce.

7.5. Recommendations

Before discussing areas of future research, the scholar would like to highlight several recommendations on cybersecurity practices that both e-commerce platforms, e-commerce platform users and internet café managers could adopt to improve online shopping experiences in the internet café environment in Gqeberha. With regards to the findings, the researcher would like to highlight the following recommendations:

1. **Perceived data protection risk disclosures:** E-commerce sites need to be transparent about their data protection and risk disclosures to improve user trust in choosing their sites. E-commerce platform users trust platforms that provide clear information on how their data is protected and disclose any associated risks. It could reduce the perceived fear among e-commerce platform users, encouraging them to select their sites over other platforms for online shopping purposes in untrusted internet café environments.

2. **Biometric verification integrated into e-commerce platforms:** The design of e-commerce platforms should consider integrating face recognition to their sites, making it user-friendly to give them a competitive edge over other platforms. This could strengthen cybersecurity measures for shopping accounts and boost the response efficacy and self-efficacy of e-commerce platform users with low digital literacy. It could also reduce perceived response costs to

improve their online shopping experiences and satisfaction in a highly sensitive environment, such as an internet café.

3. **Websites' verification cues processes**: It is important for e-commerce platforms to regularly provide visual cues such as recognised logos, verification links and customer reviews on their sites. This could make e-commerce platform users feel secure when shopping online in an internet café. The visible clues serve as reliable sites and verification links to verify users' accounts as a sign of trusted websites. It would further improve self-efficacy and reduce perceived response costs for frequent e-commerce platform users who use the internet café services for their shopping purposes.

4. **Promotion of enhanced, secure, and flexible payment options:** Promoting other seamless payment options, such as virtual cards, is vital to enhancing security features for e-commerce platform users. Many e-commerce platform users expressed concerns about payment fraud, but only a few were aware of virtual cards and how to set limits on their cards. Therefore, there is a need to educate e-commerce platform users on the alternative secure payment options available on e-commerce platforms when shopping online in an internet café. This could reduce perceived threats and improve user confidence (self-efficacy) to successfully complete online payments during online transactions in public internet cafés.

5. **Adoption of password manager**: Given the high perceived threats to online shopping activities in internet café environments, e-commerce platform users need to adopt a password manager to prevent their accounts from being hacked. The platforms should always educate users about the importance of using password managers when shopping in unprotected environments, such as internet cafés. This could boost the self-efficacy and response efficacy of users, enabling them to make conscious efforts and decisions to adopt protective behaviours that prevent account theft and online attacks.

6. **Improving cybersecurity habits through platform-supported education:** without constant user education and information on cybersecurity practices available on e-commerce platforms, some users were unable to adopt these practices, despite the platform providing themes for online safety. Platform-supported education is vital for enhancing the self-efficacy of e-commerce platform users who lack knowledge or prior experiences, thereby reducing their perceived threats and fostering confidence in adopting cybersecurity practices during online transactions in Gqeberha's internet café environment.

Although these recommendations are primarily intended for e-commerce platform users shopping online in Gqeberha internet cafés, other platforms or internet cafés may also benefit from further investigation into these cybersecurity practices to determine how they can be applied. The researcher envisions that such investigations could enable future scholars to further dissect these practices into more detailed analyses for e-commerce platforms and internet cafés.

7.6. Limitations for this study

The researcher would like to recognise that this study has some limitations. The limitations were due to the sample size and the sampling method for the quantitative phases. The study employed a cross-sectional design rather than observing behaviours due to time constraints. Additionally, the study's locations, accessibility, and challenges in reaching some participants during the qualitative phase were considered. The data collection methods primarily relied on purposive and probability sampling, which were solely linked to specific public internet cafés in Gqeberha. These factors may introduce biases linked to location, user demographics, self-reporting bias or internet culture. This makes it difficult to generalise the findings of the study to other towns or a broader population.

7.7. Future studies

With a specific focus on e-commerce platform users, this study could be repeated in other cities of the Eastern Cape and across other South African provinces. Future

studies could broaden the study demographic and geographical coverage to include rural areas and diverse income groups outside public internet café settings, thereby exploring the influence of PMT constructs and cybersecurity practices within e-commerce.

Future studies on longitudinal or intervention-based research could be conducted to observe how PMT constructs evolved through the lens of e-commerce platform users' threat perceptions and coping mechanisms. Particularly, utilising targeted cybersecurity education to assess self-efficacy and response efficacy, and observing how changes in e-commerce platform design can reduce response costs for e-commerce platform users to apply cybersecurity practices within the context of e-commerce.

Future studies could combine PMT with Technology Adoption theories, such as the Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), or Theory of Reasoned Action (TRA), to explore the broader adoption of cybersecurity practices among e-commerce platform users and the usability factors that influence these practices within the context of e-commerce.

REFERENCES

Abdelhakim, A., Badr, R., 2021. Adopted Research Designs by Tourism and Hospitality Postgraduates in The Light of Research Onion. International Journal of Tourism and Hospitality Management 4, 98–124. https://doi.org/10.21608/ijthm.2021.206774

Ablon, L., Bogart, A., 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation. https://doi.org/10.7249/RR1751

Aboelfotoh, S.F., Hikal, N.A., 2019. A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises.

Adisa, O.T., 2023. The impact of cybercrime and cybersecurity on Nigeria's national security.

Agarwala, D., 2021. SQL injection and XSS.

Ahmad, R.A.Y.B., Tarshany, Y.M.A., Ayasrah, F.T.M., Mohamad, F.S., Saany, S.I.A., Pandey, B., 2023. The Role of Cybersecurity in E-Commerce to Achieve the Maqasid of Money, in: 2023 International Conference on Computer Science and Emerging Technologies (CSET). IEEE, pp. 1–8.

Ahmed, S.A.H., 2024. Assessing the Level of Cybersecurity Awareness and Practices of Application Users and Their Impact on Privacy Policy Consents: A Case Study in Application Downloading.

Ahmed, S.K., 2024. The pillars of trustworthiness in qualitative research. Journal of Medicine, Surgery, and Public Health 2, 100051. https://doi.org/10.1016/j.glmedi.2024.100051

Aigbefo, Q.A., Blount, Y., Marrone, M., 2022. The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology 41, 1151–1170. https://doi.org/10.1080/0144929X.2020.1856928

Al Shakosh, S., 2024. Cybersecurity awareness among Swedish young adults in usage of public Wi-Fi networks.

Al-Ababneh, M.M., 2020. Linking Ontology, Epistemology And Research Methodology. Science & Philosophy 8. https://doi.org/10.23756/sp.v8i1.500

Alawida, M., Omolara, A.E., Abiodun, O.I., Al-Rajab, M., 2022. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Computer and Information Sciences.

Alexei, Arina, Alexei, Anatolie, 2023. The Difference Between Cyber Security Vs Information Security. JES 29, 72–83. https://doi.org/10.52326/jes.utm.2022.29(4).08

Alharahsheh, H.H., Pius, A., 2020. A Review of key paradigms: positivism VS interpretivism. GAJHSS.

Ali, M.M., Mohd Zaharon, N.F., 2024. Phishing—A Cyber Fraud: The Types, Implications and Governance. International Journal of Educational Reform 33, 101–121. https://doi.org/10.1177/10567879221082966

Aliyu, M., 2019. Cyber Security Threats and Practices in Internet Café: An Assessment of Northwestern States in Nigeria.

Allemang, B., Sitter, K., Dimitropoulos, G., 2022. Pragmatism as a paradigm for patient-oriented research. Health Expectations 25, 38–47. https://doi.org/10.1111/hex.13384

Allen, M.S., Robson, D.A., Iliescu, D., 2023. Face Validity: A Critical but Ignored Component of Scale Construction in Psychological Assessment. European Journal of Psychological Assessment 39, 153–156. https://doi.org/10.1027/1015-5759/a000777

Almansoori, A., Al-Emran, M., Shaalan, K., 2023. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. Applied Sciences 13, 5700. https://doi.org/10.3390/app13095700

Alontaga, J., 2018. Internet Shop Users: Computer Practices and Its Relationship to E-Learning Readiness. Education Sciences 8, 46. https://doi.org/10.3390/educsci8020046

Alsmadi, D., Maqousi, A., Abuhussein, T., 2024. Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. Kybernetes 53, 451–466.

Alturki, R., 2021. Research Onion for Smart IoT-Enabled Mobile Applications. Scientific Programming 2021, 1–9. https://doi.org/10.1155/2021/4270998

Andrade, C., 2020. Sample Size and Its Importance in Research. Indian Journal of Psychological Medicine 42, 102–103. https://doi.org/10.4103/IJPSYM.IJPSYM_504_19

Andreianu, G., 2023. Protecting Your E-Commerce Business. Analysis on Cyber Security Threats, in: Proceedings of the International Conference on Cybersecurity and Cybercrime-2023. Asociatia Romana pentru Asigurarea Securitatii Informatiei, pp. 127–134.

Angelova, N.V., 2024. Digital Well-Being and Cybersecurity or Good Practices for Using Internet Technologies. PSYCT 17, 304–318. https://doi.org/10.37708/psyct.v17i2.930

Asenahabi, B.M., 2019. Basics of research design: A guide to selecting appropriate research design. International Journal of Contemporary Applied Researches 6, 76–89.

Aseri, A., 2021. Security Issues For Online Shoppers. International Journal of Scientific & Technology Research Volume 10, Issue 03, March 2021. Issn 2277-8616.

Asiamah, N., Mensah, H., Oteng-Abayie, E.F., 2017. General, Target, and Accessible Population: Demystifying the Concepts for Effective Sampling. TQR. https://doi.org/10.46743/2160-3715/2017.2674

Atadoga, A., Farayola, O.A., Ayinla, B.S., Amoo, O.O., Abrahams, T.O., Osasona, F., 2024. A COMPARATIVE REVIEW OF DATA ENCRYPTION METHODS IN THE USA AND EUROPE. Comput. sci. IT res. j. 5, 447–460. https://doi.org/10.51594/csitrj.v5i2.815

Avalos, B.L., Van Ouytsel, J., Walrave, M., 2022. Protection Motivation Theory, in: Ho, E.Y., Bylund, C.L., Van Weert, J.C.M. (Eds.), The International Encyclopedia of Health Communication. Wiley, pp. 1–5. https://doi.org/10.1002/9781119678816.iehc0774

Avinir, D., 2022. Online Shopping Security 101 | Solid Systems [WWW Document]. IT Company in South Africa - Solid Systems. URL https://www.solidsystems.co.za/blog/online-shopping-security-threats/ (accessed 1.1.24).

Awuzie, B., McDermott, P., 2017. An abductive approach to qualitative built environment research: A viable system methodological exposé. QRJ 17, 356–372. https://doi.org/10.1108/QRJ-08-2016-0048

Babaei, P., Vassileva, J., 2024. Drivers and persuasive strategies to influence user intention to learn about manipulative design, in: The 2024 ACM Conference on Fairness, Accountability, and Transparency. Presented at the FAccT '24: The 2024 ACM Conference on Fairness, Accountability, and Transparency, ACM, Rio de Janeiro, Brazil, pp. 2421–2431. https://doi.org/10.1145/3630106.3659046

Babchuk, W.A., 2019. Fundamentals of qualitative analysis in family medicine. Fam Med Com Health 7, e000040. https://doi.org/10.1136/fmch-2018-000040

Bada, M., Sasse, A.M., Nurse, J.R.C., 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

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

Baloyi, N., Kotze, P., 2017. Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations?, in: 2017 IST-Africa Week Conference (IST-Africa). Presented at the 2017 IST-Africa Week Conference (IST-Africa), IEEE, Windhoek, pp. 1–11. https://doi.org/10.23919/ISTAFRICA.2017.8102340

Banday, M.T., Qadri, J.A., 2011. Phishing - A Growing Threat to E-Commerce.

Barkworth, A., Tabassum, R., Habibi Lashkari, A., 2022. Detecting IMAP Credential Stuffing Bots Using Behavioural Biometrics, in: Proceedings of the 2022 12th International Conference on Communication and Network Security. Presented at the ICCNS 2022: 2022 the 12th International Conference on Communication and Network Security, ACM, Beijing China, pp. 7–15. https://doi.org/10.1145/3586102.3586104

Baumgartner, H., Weijters, B., 2021. Dealing with Common Method Variance in International Marketing Research. Journal of International Marketing 29, 7–22. https://doi.org/10.1177/1069031X21995871

Bekele, W.B., Ago, F.Y., 2022. Sample Size for Interview in Qualitative Research in Social Sciences: A Guide to Novice Researchers. REPAM 4, 42–50. https://doi.org/10.46303/repam.2022.3

Bekkers, L., Van 'T Hoff-de Goede, S., Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., Leukfeldt, E.R., 2023. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Computers & Security 127, 103099. https://doi.org/10.1016/j.cose.2023.103099

Beneke, J., Scheffer, M.-K., Du, W., 2010. Beyond Price – An Exploration into the Factors That Drive Young Adults to Purchase Online. IJMS 2. https://doi.org/10.5539/ijms.v2n2p212

Benson, L.G., Ndoro, T.T., 2022. An Investigation into Online Shopping Cart Abandonment in South Africa. IRMM 12, 26–30. https://doi.org/10.32479/irmm.12985

Bešić, M., 2023. Benefits and Risks of Artificial Intelligence in Cybersecurity and Phishing Attacks, in: E-Business Technologies Conference Proceedings. pp. 94–98.

Bhandari, P., 2021. A guide to ethical considerations in research [WWW Document]. Scribbr. URL https://www.scribbr.com/methodology/research-ethics/ (accessed 5.2.22).

Bhatia, N.L., Shukla, V.K., Punhani, R., Dubey, S.K., 2021. Growing aspects of cyber security in e-commerce, in: 2021 International Conference on Communication Information and Computing Technology (ICCICT). IEEE, pp. 1–6.

Bhattacherjee, A., 2012. Social science research: principles, methods, and practices, Second edition. Ed. Anol Bhattacherjee, Tampa, Florida?

BigCommerce, 2021. Ecommerce Security: Securing Against Cyber Threats 2021 [WWW Document]. BigCommerce. URL https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/ (accessed 1.1.24).

Bilal, M., Showngwe, S.C., Bashir, A., Ghadi, Y.Y., 2023. Assessing Secure OpenID-Based EAAA Protocol to Prevent MITM and Phishing Attacks in Web Apps., Computers, Materials & Continua.

Blancaflor, E., Eugenio, E.A., Joseph, A.C., Ray Rivera, J., Lauren, N.V., 2023. Vulnerability Assessment on Cross-site scripting attack in a simulated E-commerce platform using BeEF and XSStrike. International Conference on Software Technology and Engineering. https://doi.org/10.1109/ICSTE61649.2023.00008

Bloomfield, J., Fisher, M.J., 2019. Quantitative research design. Journal of the Australasian Rehabilitation Nurses Association 22, 27–30.

Blythe, J.M., Coventry, L., 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior 87, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Boban, M., 2024. CYBERSECURITY IN THE DIGITAL AGE: REGULATORY FRAMEWORK BASED ON THE IMPLEMENTATION OF THE NIS2 DIRECTIVE, in: Economic and Social Development (Book of Proceedings), 112th International Scientific Conference on Economic and Social Development. p. 592.

Boerman, S.C., Kruikemeier, S., Zuiderveen Borgesius, F.J., 2021. Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. Communication Research 48, 953–977. https://doi.org/10.1177/0093650218800915

Brandreth, D., Ophoff, J., 2020. Investigating Customer-Facing Security Features on South African E-commerce Websites, in: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Botha, R. (Eds.), Information and Cyber Security, Communications in Computer and Information Science. Springer International Publishing, Cham, pp. 144–159. https://doi.org/10.1007/978-3-030-66039-0_10

Brandt, P., Timmermans, S., 2021. Abductive Logic of Inquiry for Quantitative Research in the Digital Age. SocScience 8, 191–210. https://doi.org/10.15195/v8.a10

Braun, V., Clarke, V., 2024. Supporting best practice in reflexive thematic analysis reporting in *Palliative Medicine*: A review of published research and introduction to the *Reflexive Thematic Analysis Reporting Guidelines* (RTARG). Palliat Med 02692163241234800. https://doi.org/10.1177/02692163241234800

Braun, V., Clarke, V., 2022. Thematic analysis: a practical guide. SAGE, London; Thousand Oaks, California.

Braun, V., Clarke, V., 2021a. To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. Qualitative Research in Sport, Exercise and Health 13, 201–216. https://doi.org/10.1080/2159676X.2019.1704846

Braun, V., Clarke, V., 2021b. Can I use TA? Should I use TA? Should I *not* use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. Couns and Psychother Res 21, 37–47. https://doi.org/10.1002/capr.12360

Braun, V., Clarke, V., 2021c. One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology 18, 328–352. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., Clarke, V., 2019. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health 11, 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., Clarke, V., Hayfield, N., Davey, L., Jenkinson, E., 2022. Doing Reflexive Thematic Analysis, in: Bager-Charleson, S., McBeath, A. (Eds.), Supporting Research in Counselling and Psychotherapy. Springer International Publishing, Cham, pp. 19–38. https://doi.org/10.1007/978-3-031-13942-0_2

Braun, V., Clarke, V., Hayfield, N., Terry, G., 2019. Thematic Analysis, in: Liamputtong, P. (Ed.), Handbook of Research Methods in Health Social Sciences. Springer Singapore, Singapore, pp. 843–860. https://doi.org/10.1007/978-981-10-5251-4_103

Brederode, W., 2023. Cyber attacks on e-commerce sites increased in 2022 [WWW Document]. News24. URL https://www.news24.com/business/tech/cyber-attacks-on-e-commerce-sites-increased-in-2022-20230517 (accessed 1.1.25).

Brooks, H., Bee, P., Rogers, A., 2018. Introduction to qualitative data analysis, in: Bee, P., Brooks, H., Callaghan, P., Lovell, K. (Eds.), A Research Handbook for Patient and Public Involvement Researchers. Manchester University Press. https://doi.org/10.7765/9781526136527.00013

Burwood, K., 2024. South Africa's Growing Challenge with Online Fraud - ThreatMark [WWW Document]. ThreatMark. URL https://www.threatmark.com/south-africa-online-fraud/ (accessed 1.1.24).

Butler, R., Butler, M., 2019. Online security: Gaining insight into poor password practices among South Africans. Management Review [WWW Document]. URL https://www.stellenboschbusiness.ac.za/management-review/news/2019-06-15-online-security-gaining-insight-poor-password-practices-among-south-africans (accessed 1.1.24).

Butler, R., Butler, M., 2015. The password practices applied by South African online consumers: Perception versus reality. S. Afr. j. inf. manag. 17. https://doi.org/10.4102/sajim.v17i1.638

Cahit, K., 2015. Internal validity: A must in research designs. Educational Research and Reviews 10, 111–118.

Cain, A.A., Edwards, M.E., Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications 42, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Campbell, K., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C., Gehrke, P., Graham, L., Jack, S., 2021. Reflexive Thematic Analysis for Applied Qualitative Health Research. TQR. https://doi.org/10.46743/2160-3715/2021.5010

Castaneda, N., 2025. Analysis of user security practices in Gen AI.

Chang, H., 2021. Individual and collaborative autoethnography for social science research, in: Handbook of Autoethnography. Routledge, pp. 53–65.

Chennamaneni, A., Gupta, B., 2023. The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory. Behaviour & Information Technology 42, 2011–2029. https://doi.org/10.1080/0144929X.2022.2106307

Chowdhury, E.K., Chowdhury, R., 2017. Online shopping in bangladesh: a study on the motivational factors for ecommerce that influence shopper's affirmative

tendency towards online shopping. South Asian Journal of Marketing & Management Research 7, 20. https://doi.org/10.5958/2249-877x.2017.00019.4

Chowdhury, N.H., Adam, M.T.P., Skinner, G., 2019. The impact of time pressure on cybersecurity behaviour: a systematic literature review. Behaviour & Information Technology 38, 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769

Cimpanu, C., 2019. Dunkin' Donuts accounts compromised in second credential stuffing attack in three months [WWW Document]. ZDNet. URL https://www.zdnet.com/article/dunkin-donuts-accounts-compromised-in-second-credential-stuffing-attack-in-three-months/ (accessed 1.1.25).

Cisco, 2024. Cisco Secure Endpoint Overview [WWW Document]. Cisco. URL https://www.cisco.com/site/us/en/learn/topics/security/what-is-user-security.html#:~:text=An%20end%2Duser%27s%20role%20in (accessed 1.1.24).

Clift, B.C., Gore, J., Bekker, S., Batlle, I.C., Chudzikowski, K., Hatchard, J., 2019. An Edited Volume of the Proceedings of the 5th Annual Qualitative Research Symposium at the University of Bath.

Cook, L., Rumrill, P.D.Jr., 2005. Internal validity in rehabilitation research. WORK: A Journal of Prevention, Assessment & Rehabilitation 25, 279–283. https://doi.org/10.3233/WOR-2005-00511

Corbin, J., Strauss, A., 2008. Basics of qualitative research. 3rd edn Thousand Oaks.

Corry, M., Porter, S., McKenna, H., 2019. The redundancy of positivism as a paradigm for nursing research. Nursing Philosophy 20, e12230. https://doi.org/10.1111/nup.12230

Cowling, N., 2024. Topic: E-commerce in South Africa [WWW Document]. Statista. URL https://www.statista.com/topics/11038/e-commerce-in-south-africa/#topicOverview

Craigen, D., Diakun-Thibault, N., Purse, R., 2014. Defining Cybersecurity. Technology Innovation Management Review 4, 13–21. https://doi.org/10.22215/timreview/835

Craighead, C.W., Ketchen, D.J., Dunn, K.S., Hult, G.T.M., 2011. Addressing common method variance: guidelines for survey research on information technology,

operations, and supply chain management, IEEE transactions on engineering management. IEEE.

Creswell, J., Clark, V.L.P., 2017. Mixed methods research. The Journal of Positive Psychology 12, 305–306. https://doi.org/10.1080/17439760.2016.1262619

Creswell, J.W., 2021. A concise introduction to mixed methods research. SAGE publications.

Creswell, J.W., 2014. Research design qualitative quantitative and mixed methods approaches (p. 398).

Creswell, J.W., 2013. Research design: qualitative, quantitative, and mixed methods approaches, 4th ed. ed. SAGE Publications, Inc, Thousand Oaks.

Creswell, J.W., Creswell, J.D., 2023. Research Design_ Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications.

Creswell, J.W., Creswell, J.D., 2018. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.

Creswell, J.W., Poth, C.N., 2016. Qualitative inquiry and research design: Choosing among five approaches. Sage publications.

Cui, F., Lin, D., Qu, H., 2018. The impact of perceived security and consumer innovativeness on e-loyalty in online travel shopping. Journal of Travel & Tourism Marketing 35, 819–834. https://doi.org/10.1080/10548408.2017.1422452

Dakov, S., Malinova, A., 2021. A Survey of E-Commerce Security Threats and Solutions. Proceedings of CBU in Natural Sciences and ICT.

Daramola, O., Etim, E., 2022. Affordances of digital platforms in sub-Saharan Africa: An analytical review. The Electronic Journal of Information Systems In Developing Countries, 88. https://doi.org/10.1002/isd2.12213

Davison, A., 2023. SA consumers lax when it comes to online security [WWW Document]. IT-Online. URL https://it-online.co.za/2023/02/02/sa-consumers-lax-when-it-comes-to-online-security/ (accessed 1.1.23).

De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K., 2021. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context.

Behaviour & Information Technology 1–13. https://doi.org/10.1080/0144929x.2021.1905066

Debb, S.M., McClellan, M.K., 2021. Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. Cyberpsychology, Behavior, and Social Networking 24, 605–611. https://doi.org/10.1089/cyber.2021.0043

Desamsetti, H., 2021. Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenges. Am. j. trade policy 8, 239–246. https://doi.org/10.18034/ajtp.v8i3.666

Deshpande, M., Magerko, B., 2024. Holistic Approach to Design of Generative AI Evaluations: Insights from the Research Onion Model.

Dhobe, S.D., Tighare, K.K., Dake, S.S., 2020. Prevention of Fraud in Electronic Payment Gateway using Secret Code. International Research Journal of Engineering And Technology (Irjet).

Ding, Y., Meso, P., Xu, S., 2014. Protection Motivation Driven Security Learning.

Dodge, C.E., Fisk, N., Burruss, G.W., Moule, R.K., Jaynes, C.M., 2023. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. Criminology & Public Policy 22, 849–868. https://doi.org/10.1111/1745-9133.12641

Dong, Y., 2023. Descriptive Statistics and Its Applications. HSET 47, 16–23. https://doi.org/10.54097/hset.v47i.8159

Downing, S.M., 2006. Face validity of assessments: faith-based interpretations or evidence-based science? Med Educ 40, 7–8. https://doi.org/10.1111/j.1365-2929.2005.02361.x

EC-Council, 2024. Preventing SMiShing in South Africa| SMS phishing| EC-Council – Aware [WWW Document]. Eccouncil.org. URL https://aware.eccouncil.org/smishing-in-south-africa.html (accessed 1.1.24).

Egelman, S., Peer, E., 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS), in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. Presented at the CHI '15: CHI Conference on Human Factors in Computing Systems, ACM, Seoul Republic of Korea, pp. 2873–2882. https://doi.org/10.1145/2702123.2702249

Etzioni, A., 2019. Cyber Trust. J Bus Ethics 156, 1–13. https://doi.org/10.1007/s10551-017-3627-y

Eze, K.U., 2019. The Quagmires of the Amoebic Internet: Law and Technology to the Rescue. IRLJ 1, 1.

Faruk, M.J.H., Tasnim, M., Shahriar, H., Valero, M., Rahman, A., Wu, F., 2022. Investigating Novel Approaches to Defend Software Supply Chain Attacks, in: 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, pp. 283–288. https://doi.org/10.1109/issrew55968.2022.00081

Fife-Schaw, C., 2020. Questionnaire design. Research methods in psychology 343–374.

Finlay, L., 2021. Thematic analysis: The ‘Good’, the ‘Bad’ and the ‘Ugly’ 11.

Flick, U., 2018. Doing qualitative data collection–charting the routes. The SAGE handbook of qualitative data collection 3–16.

Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A Meta-Analysis of Research on Protection Motivation Theory. J Applied Social Psychol 30, 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fourie, B., 2023. Dis-Chem found guilty of breaching POPIA act [WWW Document]. URL https://www.iol.co.za/news/dis-chem-found-guilty-of-breaching-popia-act-7d10b884-8c4b-4dc7-b3cf-5a1a5200f196

Frauenstein, E.D., Flowerday, S., Mishi, S., Warkentin, M., 2023. Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. Information & Management 60, 103858. https://doi.org/10.1016/j.im.2023.103858

Galov, N., 2023. 17+ Sinister Social Engineering Statistics for 2023 [WWW Document]. WebTribunal. URL https://webtribunal.net/blog/social-engineering-statistics#gref (accessed 1.1.24).

Ganesh, A., Ndulue, C., Orji, R., 2022. Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory, in: Baghaei, N., Vassileva, J., Ali, R., Oyibo, K. (Eds.), Persuasive Technology, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 89–100. https://doi.org/10.1007/978-3-030-98438-0_7

Ganji, J., Kolivand, M., Hasanimoghadm, S., Hassani, M., 2017. Iranian Women's Sexual Experience after Childbirth: A Mixed Method Explanatory Sequential Study. International Journal of Health Studies.

Ghaderi, Z., Beal, L., Houanti, L., 2024. Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. Current Issues in Tourism 1–16. https://doi.org/10.1080/13683500.2024.2353327

Ghazali, N.N., Hassan, S., Ahmad, R., 2023. Fortifying Against Cyber Fraud: Instrument Development with the Protection Motivation Theory. IJACSA 14. https://doi.org/10.14569/IJACSA.2023.0141055

Giwah, A.D., Wang, L., Levy, Y., Hur, I., 2019. Empirical assessment of mobile device users' information security behavior towards data breach. Journal of Intellectual Capital 21, 215–233. https://doi.org/10.1108/jic-03-2019-0063

Gizaw, Z., Yalew, A.W., Bitew, B.D., Lee, J., Bisesi, M., 2022. Development and validation of questionnaire to assess exposure of children to enteric infections in the rural northwest Ethiopia. Sci Rep 12, 6740. https://doi.org/10.1038/s41598-022-10811-x

GoDitigal Western Cape, 2023. E-commerce in South Africa and the Western Cape [WWW Document]. Western Cape Government. URL https://www.westerncape.gov.za/site-page/e-commerce-south-africa-and-western-cape

Goertz, G., Mahoney, J., 2012. Concepts and measurement: Ontology and epistemology. Social Science Information 51, 205–216. https://doi.org/10.1177/0539018412437108

Goga, S., Paelo, A., Nyamwena, J., 2019. ONLINE RETAILING IN SOUTH AFRICA: AN OVERVIEW.

Goldkuhl, G., 2012. Pragmatism *vs* interpretivism in qualitative information systems research. European Journal of Information Systems 21, 135–146. https://doi.org/10.1057/ejis.2011.54

Graue, C., 2015. Qualitative Data Analysis. International Journal of Sales, Retailing & Marketing 4.

Greener, S., 2018. Methodological choices for research into interactive learning. Interactive Learning Environments 26, 149–150. https://doi.org/10.1080/10494820.2018.1436431

Greenfield, T., Greener, S. (Eds.), 2016. Research methods for postgraduates, Third edition. ed. John Wiley & Sons, Chichester, UK ; Hoboken, NJ.

Grobler, M., Gaire, R., Nepal, S., 2021. User, Usage and Usability: Redefining Human Centric Cyber Security. Front. Big Data 4, 583723. https://doi.org/10.3389/fdata.2021.583723

Gumasing, M.J.J., Ong, A.K.S., Sy, M.A.P.C., Prasetyo, Y.T., Persada, S.F., 2023. A machine learning ensemble approach to predicting factors affecting the intention and usage behavior towards online groceries applications in the Philippines. Heliyon 9, e20644. https://doi.org/10.1016/j.heliyon.2023.e20644

Gunawan, W., Wendy, 2019. Measuring information security and cybersecurity on private cloud computing. Journal of Theoretical and Applied Information Technology 96.

Haag, S., Siponen, M., Liu, F., 2021. Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. SIGMIS Database 52, 25–67. https://doi.org/10.1145/3462766.3462770

Habibi, P.K., 2021. Effectiveness of deductive and inductive instruction in EFL classes. Strength for Today and Bright Hope for Tomorrow 21, 82–90.

Ham, C.-D., 2017. Exploring how consumers cope with online behavioral advertising. International Journal of Advertising 36, 632–658. https://doi.org/10.1080/02650487.2016.1239878

Hamed, S., El-Deeb, S., 2020. Cash on Delivery as a Determinant of E-Commerce Growth in Emerging Markets. Journal of Global Marketing 33, 1–24. https://doi.org/10.1080/08911762.2020.1738002

Hamzah, M.I., 2024. Fear of COVID-19 disease and QR-based mobile payment adoption: a protection motivation perspective. J Financ Serv Mark 29, 946–963. https://doi.org/10.1057/s41264-023-00246-4

Haque, A., Karim, W., Kabir, S., Tarofder, A.K., 2020. Understanding Social Distancing Intention among University Students during Covid-19 Outbreak: An Application of Protection Motivation Theory.

Hariharan, J., Sheik, A.T., Maple, C., Beech, N., Atmaca, U.I., 2023. Customers' perception of cybersecurity risks in E-commerce websites, in: International Conference on AI and the Digital Economy (CADE 2023). IET, pp. 53–60.

Harrison, H., Birks, M., Franklin, R., Mills, J., 2017. Case study research: Foundations and methodological orientations, in: Forum Qualitative Sozialforschung/Forum: Qualitative Social Research.

Harshavardan, K., PadmaShani, R., 2023. Secure practices to prevent cyber attacks in e-commerce sites, in: 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS). IEEE, pp. 665–670.

Hasan, M.Z., Hussain, M.Z., Alam, I., Sarwar, N., Qureshi, A.M., Irshad, A., 2023. Impact of Cybercrime on Enterprises in Cloud Computing Environment: A Review, in: 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T). Presented at the 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), IEEE, Bahawalpur, Pakistan, pp. 1–6. https://doi.org/10.1109/ICEST56843.2023.10138873

Hasan, N., Rana, R.U., Chowdhury, S., Dola, A.J., Rony, M.K.K., 2021. Ethical considerations in research. Journal of Nursing Research, Patient Safety and Practice (JNRPSP) 1, 1–4.

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N.N., Aripin, J.A., Ali, F., 2024. Staying One Step Ahead: Exploring Protection Motivation Theory to Combat Cyber-fraud Among E-services Users. Procedia Computer Science 234, 1364–1371. https://doi.org/10.1016/j.procs.2024.04.011

Hassenzahl, M., 2018. The Thing and I: Understanding the Relationship Between User and Product. Human–Computer Interaction Series 301–313. https://doi.org/10.1007/978-3-319-68213-6_19

Haverkamp, I., Sarmah, D.K., 2024. Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. Int. J. Inf. Secur. 23, 2607–2635. https://doi.org/10.1007/s10207-024-00853-9

Heale, R., Twycross, A., 2015. Validity and reliability in quantitative studies. Evid Based Nurs 18, 66–67. https://doi.org/10.1136/eb-2015-102129

Healy, P., Perry, C., 2000. Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm | Emerald Insight [WWW Document]. URL https://www.emerald.com/insight/content/doi/10.1108/13522750010333861/full/html (accessed 11.12.24).

Hedrick, T.E., Bickman, L., Rog, D.J., 1993. Applied research design: A practical guide. Sage Publications.

Henry, G., 2023. E-commerce growth expected to continue [WWW Document]. www.rmb.co.za. URL https://www.rmb.co.za/news/ecommerce-growth-expected-to-continue

Herath, T.B.G., Khanna, P., Ahmed, M., 2022. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. JCP 2, 1–18. https://doi.org/10.3390/jcp2010001

Hiller, J., 2016. Epistemological Foundations of Objectivist and Interpretivist Research.

Hinderks, A., Mayo, F.J.D., Thomaschewski, J., Escalona, M.J., 2022. Approaches to manage the user experience process in agile software development: A systematic literature review. Information and Software Technology 106957. https://doi.org/10.1016/j.infsof.2022.106957

Hinds, J., Williams, E.J., Joinson, A.N., 2020. “It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies 143, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Hobbs, J.R., Stickel, M.E., Appelt, D.E., Martin, P., 1993. Interpretation as abduction, Artificial intelligence. Elsevier.

Hossain, M.A., Islam, S., Rahman, M.M., Arif, N.U.M., 2024. Impact of Online Payment Systems on Customer Trust and Loyalty in E-Commerce Analyzing Security and Convenience. AJSTEME 4, 1–15. https://doi.org/10.69593/ajsteme.v4i03.85

Hossain, Md.A., 2019. Security perception in the adoption of mobile payment and the moderating effect of gender. PSU Research Review ahead-of-print. https://doi.org/10.1108/prr-03-2019-0006

Hossan, D., Dato' Mansor, Z., Jaharuddin, N.S., 2023. Research Population and Sampling in Quantitative Study. IJBT 13, 209–222. https://doi.org/10.58915/ijbt.v13i3.263

Hotjar, 2022. Introduction to Ecommerce UX: A Step-By-Step Framework [WWW Document]. www.hotjar.com. URL https://www.hotjar.com/ecommerce/ux/ (accessed 1.1.24).

Houmz, A., Mezzene, M.S., Tellabt, A., Mezzour, G., Koutbi, M.E., 2016. Field study of cybercafe usage & security in Morocco, in: 2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS). Presented at the 2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS), IEEE, Marrakesh, Morocco, pp. 1–7. https://doi.org/10.1109/ACOSIS.2016.7843916

Hughes, R., Curley, K., Kotera, Y., 2024. Parents' Experiences after Their Child's Autism Diagnosis: A Reflexive Thematic Analysis. Psychiatry International 5, 370–394. https://doi.org/10.3390/psychiatryint5030026

Humaidi, N., Abdallah Alghazo, S.H., 2022. Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation in Enhancing Employees' Cybersecurity Protective Behaviour. Presented at the 10th International Symposium on Digital Forensics and Security, ISDFS 2022. https://doi.org/10.1109/ISDFS55398.2022.9800834

Humaidi, N., Alghazo, S.H.A., 2022. Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation in Enhancing Employees' Cybersecurity Protective Behaviour. 2022 10th International Symposium on Digital Forensics and Security (ISDFS). https://doi.org/10.1109/isdfs55398.2022.9800834

Hussien, F.T.A., Rahma, A.M.S., Wahab, H.B.A., 2022. Design and implement a new secure prototype structure of e-commerce system. International Journal of Electrical and Computer Engineering 12, 560–571.

Idayani, R.W., Nadlifatin, R., Subriadi, A.P., Gumasing, Ma.J.J., 2024. A Comprehensive Review on How Cyber Risk Will Affect the Use of Fintech. Procedia Computer Science 234, 1356–1363. https://doi.org/10.1016/j.procs.2024.03.134

Ilavendhan, A., Atchaya, M., 2024. Empowering Cyber Defenses: Shielding Against Man-in-the-Middle Attacks with Public Key Infrastructure (PKI), in: Singh, Y., Gonçalves, P.J.S., Singh, P.K., Kolekar, M.H. (Eds.), Proceedings of International Conference on Recent Innovations in Computing, Lecture Notes in Electrical Engineering. Springer Nature Singapore, Singapore, pp. 157–175. https://doi.org/10.1007/978-981-97-7862-1_11

Interpol, 2021. African Cyberthreat Assessment Report.

Ioannou, A., Tussyadiah, I., Marshan, A., 2021. Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. Psychology & Marketing 38, 1766–1778. https://doi.org/10.1002/mar.21529

Islam, M.A., Aldaihani, F.M.F., 2022. Justification for adopting qualitative research method, research approaches, sampling strategy, sample size, interview method, saturation, and data analysis. Journal of International Business and Management 5, 01–11.

Iso, D.I.S., 2010. 9241–210: 2010: ergonomics of human-system interaction—part 210: human-centred design for interactive systems (formerly known as 13407). Switzerland: International Standards Organization.

Jain, VIPIN, Malviya, B., Arya, S., 2021. An overview of electronic commerce (e-Commerce). Journal of Contemporary Issues in Business and Government 27, 665–670.

Jain, Vipin, Malviya, B., Arya, S., 2021. An Overview of Electronic Commerce (e-Commerce). Journal of Contemporary Issues in Business and Government 27.

Jamil, H., 2023. Factors affecting users cybersecurity practices: A study of Australian microbusinesses.

Jamil, Hassan, Zia, T., Nayeem, T., Whitty, M.T., D'Alessandro, S., 2024. Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. Information & Computer Security.

Jamil, H., Zia, T., Nayeem, T., Whitty, M.T., D'Alessandro, S., 2024. Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. Information and Computer Security. https://doi.org/10.1108/ICS-10-2023-0176

Jamra, R.K., Anggorojati, B., Kautsarina, Sensuse, D.I., Suryono, R.R., 2020. Systematic Review of Issues and Solutions for Security in E-commerce. 2020 International Conference on Electrical Engineering and Informatics (ICELTICs). https://doi.org/10.1109/iceltics50595.2020.9315437

Jansen, J., Van Schaik, P., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. International Journal of Human-Computer Studies 123, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jimma, E., 2022. College of Law and Governance School of Law LLM in Human Rights and Criminal Law (PhD Thesis). Doctoral dissertation, Jimma University.

Junjie, M., Yingxin, M., 2022. The Discussions of Positivism and Interpretivism. Glob Acad J Humanit Soc Sci 4, 10–14. https://doi.org/10.36348/gajhss.2022.v04i01.002

Kakar, A.A., Choudhury, B., Kakar, A., 2020. Why are some Internet users more prone to adopt prudent Cybersecurity practices than others?

Kakar, Z.U.H., Rasheed, R., Rashid, A., Akhter, S., 2023. Criteria for Assessing and Ensuring the Trustworthiness in Qualitative Research. IJBR 4, 150–173. https://doi.org/10.56249/ijbr.03.01.44

Kalhoro, S., Rehman, M., Ponnusamy, V., Shaikh, F.B., 2021. Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. IEEE Access 9, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

Kamau, G.N., 2022. ICT4D Research in Developing Countries: A Call for Pragmatism Approach. IJCIS 3, 51–55. https://doi.org/10.29040/ijcis.v3i2.67

Kankam, P.K., 2019. The use of paradigms in information research. Library & Information Science Research 41, 85–92. https://doi.org/10.1016/j.lisr.2019.04.003

Kariuki, P., Ofusori, L.O., Subramaniam, P.R., 2024. Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. Secur J 37, 292–321. https://doi.org/10.1057/s41284-023-00378-1

Kaspersky, 2019. How to Avoid Public WiFi Security Risks [WWW Document]. www.kaspersky.com. URL https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Kaushik, V., Walsh, C.A., 2019. Pragmatism as a research paradigm and its implications for social work research, Social Sciences. MDPI.

Kautondokwa, P., Ruhwanya, Z., Ophoff, J., 2021. Environmental Uncertainty and End-User Security Behaviour: A Study During the COVID-19 Pandemic, in: Drevin, L., Miloslavskaya, N., Leung, W.S., Von Solms, S. (Eds.), Information Security Education for Cyber Resilience, IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, pp. 111–125. https://doi.org/10.1007/978-3-030-80865-5_8

Kelley, D., 2018. Investigation of attitudes towards security behaviors. McNair Research Journal SJSU 14, 10.

Kennedy, B.L., Thornberg, R., 2018. Deduction, induction, and abduction. The SAGE handbook of qualitative data collection 49–64.

Khan, N.F., Ikram, N., Murtaza, H., Javed, M., 2023. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security 125, 103049. https://doi.org/10.1016/j.cose.2022.103049

Khan, N.F., Murtaza, H., Malik, K., Mahmood, M., Asadi, M.A., 2024. Explanatory and predictive analysis of smartphone security using protection motivation theory: a hybrid SEM-AI approach. Information Technology & People.

Khan, S.W., 2019. Cyber Security Issues and Challenges in E-Commerce. SSRN Journal. https://doi.org/10.2139/ssrn.3323741

Khasawneh, M.A., 2009. An Exploration of Consumer Response Towards Sponsored Search Advertising (ssa) from a Consumer Behaviour Perspective.

Khipu Networks, 2023. Cyber Security Awareness Month 2023: Empowering users to stay safe online [WWW Document]. ITWeb. URL https://www.itweb.co.za/article/cyber-security-awareness-month-2023-

empowering-users-to-stay-safe-online/8OKdWMDXQynMbznQ (accessed 12.31.23).

Kim, B.-J., Kim, M.-J., Lee, J., 2024. Examining the impact of work overload on cybersecurity behavior: highlighting self-efficacy in the realm of artificial intelligence. Curr Psychol 43, 17146–17162. https://doi.org/10.1007/s12144-024-05692-4

Kimmons, R., 2022. Mixed methods. Education Research 63, 631–641.

Kimura, K., Kuzuno, H., Shiraishi, Y., Morii, M., 2024. Man-in-the-Portal: Breaking SSL/TLS Silently Abusing Captive Portal, Journal of Information Processing. Information Processing Society of Japan.

Kimura, K., Shiraishi, Y., Morii, M., 2023. A New Approach to Disabling SSL/TLS: Man-in-the-Middle Attacks are still Effective, in: 2023 Eleventh International Symposium on Computing and Networking (CANDAR). IEEE, pp. 11–19.

Kirlappos, I., Sasse, M.A., Harvey, N., 2012. Why Trust Seals Don't Work: A Study of User Perceptions and Behavior, in: Katzenbeisser, S., Weippl, E., Camp, L.J., Volkamer, M., Reiter, M., Zhang, X. (Eds.), Trust and Trustworthy Computing, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 308–324. https://doi.org/10.1007/978-3-642-30921-2_18

Kiselichki, M., Kirovska, Z., Anastasovski, M., Jovevski, D., 2022. Security Aspects Of Digital Transactions E-Commerce And M-Commerce Implementations.

Kishore, K., Jaswal, V., Kulkarni, V., De, D., 2021. Practical Guidelines to Develop and Evaluate a Questionnaire. Indian Dermatology Online Journal 12, 266–275. https://doi.org/10.4103/idoj.IDOJ_674_20

Kitbuncha, W., 2017. Legal measures on authentication of electronic fund transfer.

Kleij, R.V.D., 2022. From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design. Presented at the 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022). https://doi.org/10.54941/ahfe1002209

Konstantinos, G., 2024. Thematic analysis: A practical guide: by Virginia Braun and Victoria Clarke, Los Angeles, USA, Sage Publications, 2022, 376 pp., $ 27.59 (paperback), ISBN-13: 978-1473953246. European Journal of Psychotherapy & Counselling 26, 461–464. https://doi.org/10.1080/13642537.2024.2391666

Kshetri, N., 2021. Cybersecurity Management.

Kshetri, N., 2019. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management 22, 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Kshetri, N., Kshetri, N., 2022. Economics of Supply Chain Cyberattacks. IT Professional. https://doi.org/10.1109/MITP.2022.3172877

Kumar, B., 2023. How To Improve Your Ecommerce UX (Hint: Start From Your Marketing) [WWW Document]. Shopify. URL https://www.shopify.com/blog/ecommerce-ux (accessed 1.1.24).

Kunal, Singh, P., Hirani, N., 2022. A Cohesive Relation Between Cybersecurity and Information security, in: 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT). Presented at the 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), IEEE, Bangalore, India, pp. 1–6. https://doi.org/10.1109/GCAT55367.2022.9972023

Kuppusamy, P., Samy, G.N., Maarop, N., Shanmugam, B., Perumal, S., 2022. Information Security Policy Compliance Behavior Models, Theories, and Influencing Factors: A Systematic Literature Review. Vol.

Kuraku, S., Kalla, D., Smith, N., Samaah, F., 2023. Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks.

Kuruwitaarachchi, N., Abeygunawardena, P.K.W., Rupasingha, L., Udara, S.W.I., 2019. A Systematic Review of Security in Electronic Commerce- Threats and Frameworks. GJCST 33–39. https://doi.org/10.34257/GJCSTEVOL19IS1PG33

Kuzma, J., 2011. Web vulnerability study of online pharmacy sites. Informatics for Health and Social Care 36, 20–34. https://doi.org/10.3109/17538157.2010.520418

Labuschagne, W.A., Eloff, M.M., Veerasamy, N., Mujinga, M., 2011. Design of a cyber security awareness campaign for internet Cafés users in rural areas.

Lakens, D., 2022. Sample size justification. Collabra: psychology 8, 33267.

Laudon, K.C., Traver, C.G., 2020. E-commerce 2019: Business, technology, society. Pearson.

Leavy, P., 2017. Research design.

Lee, E., Seomun, G., 2021. Structural Model of the Healthcare Information Security Behavior of Nurses Applying Protection Motivation Theory. International Journal of Environmental Research and Public Health 18, 2084. https://doi.org/10.3390/ijerph18042084

Lee, J., 2020. Statistics, Descriptive, in: International Encyclopedia of Human Geography. Elsevier, pp. 13–20. https://doi.org/10.1016/B978-0-08-102295-5.10428-7

Legg, C., Hookway, C., 2008. Pragmatism.

Lempereur, K., 2022. What is a credential stuffing attack? Examples & Mitigation [WWW Document]. DataDome. URL https://datadome.co/guides/credential/what-is-credential-stuffing/ (accessed 1.1.25).

Lesko, S., 2020. Models and scenarios of implementation of threats for internet resources. Russian Technological Journal. https://doi.org/10.32362/2500-316x-2020-8-6-9-33

Lim, J., 2021. Cybersecurity awareness by consumers still low, says IBM Security survey [WWW Document]. Tech Wire Asia. URL https://techwireasia.com/08/2021/consumer-cybersecurity-awareness-still-low-businesses-should-step-up-ibm-security-survey/ (accessed 1.1.24).

Liu, F., Pan, L., Yao, L., 2018. Evolutionary game based analysis for user privacy protection behaviors in social networks, in: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, pp. 274–279.

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J., Abbas, S., 2022. Cybersecurity threats: A never-ending challenge for e-commerce. Frontiers in Psychology 13. https://doi.org/10.3389/fpsyg.2022.927398

Luo, S., Choi, T., 2022. Ecommerce supply chains with considerations of cybersecurity: Should governments play a role? Production and operations management. https://doi.org/10.1111/poms.13666

Lynn, T., van der Werff, L., Hunt, G., Healy, P., 2016. Development of a Cloud Trust Label: A Delphi Approach. Journal of Computer Information Systems 56, 185–193. https://doi.org/10.1080/08874417.2016.1153887

MacRae, A.W., 2019. Descriptive and inferential statistics, in: Companion Encyclopedia of Psychology. Routledge, pp. 1099–1121.

Maddel, M.M., Nandavadekar, V.D., 2014. Enhancing Social Security Through Cyber Security for Cyber Cafe: Implication for Pune City. International Journal of Information Technology & Computer Sciences Perspectives 3, 1255.

Madupati, B., 2022. Cybersecurity in Day-to-Day Life : A Technical Perspective. J Mathe & Comp Appl 1–6. https://doi.org/10.47363/JMCA/2022(1)E114

Mafuya, A., 2022. Examining the Experiences of Black Internet café Owners on the Use of Smartphones in the Townships: A Case Study on Small Businesses in Katlehong, East Rand (Master's Thesis). University of Johannesburg (South Africa).

Magunje, C., Chigona, W., 2024. Educators' Cybersecurity Vulnerabilities in Marginalised Schools in South Africa, in: Gerber, A. (Ed.), South African Computer Science and Information Systems Research Trends, Communications in Computer and Information Science. Springer Nature Switzerland, Cham, pp. 347–360. https://doi.org/10.1007/978-3-031-64881-6_20

Makhitha, K., Ngobeni, K., 2024. The Influence of Perceived Risk Factors on Emerging-Market Consumers' Attitude Towards Shopping for Clothes Online. Studies in Media and Communication.

Makhitha, K., Ngobeni, K.M., 2021. The influence of demographic factors on perceived risks affecting attitude towards online shopping.

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., Zeineddine, H., 2019. An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. IEEE Access 7, 93010–93022. https://doi.org/10.1109/ACCESS.2019.2927266

Malapane, T.A., 2019. A Risk Analysis of E-Commerce: A Case of South African Online Shopping Space. Systems and Information Engineering Design Symposium. https://doi.org/10.1109/SIEDS.2019.8735643

Malapane, T.A., Ndlovu, N., 2024. Towards a Policy Framework for E-Commerce Risk Management: A Case of S outh African Online Shopping. Systems and Information Engineering Design Symposium.

Malhotra, N.K., Schaller, T.K., Patil, A., 2017. Common Method Variance in Advertising Research: When to Be Concerned and How to Control for It. Journal of Advertising 46, 193–212. https://doi.org/10.1080/00913367.2016.1252287

Mamat, S., Mahmud, W.A.W., Azlan, A.A., 2023. Security Threats to Privacy Data of Malaysian Youths: Online Transaction and Communication.

Maphosa, V., 2023. An overview of cybersecurity in Zimbabwe's financial services sector. F1000Res 12, 1251. https://doi.org/10.12688/f1000research.132823.1

Mardiana, S., 2020. Modifying Research Onion for Information Systems Research. Solid State Technology, 1202-1210.

Marikyan, D., Papagiannidis, S., 2023. Protection Motivation Theory. https://research-information.bris.ac.uk/ws/portalfiles/portal/376433746/Marikyan_and_Papagiannidis_2023_protection_motivation_theory_Review.pdf

Marikyan, D., Papagiannidis, S., Rana, O.F., Ranjan, R., 2022. Blockchain adoption: A study of cognitive factors underpinning decision making. Computers in Human Behavior 131, 107207. https://doi.org/10.1016/j.chb.2022.107207

Marshall, B., Cardon, P., Poddar, A., Fontenot, R., 2013. Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. Journal of Computer Information Systems 54, 11–22. https://doi.org/10.1080/08874417.2013.11645667

Martinez, J., Javier, M.D., 2021. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. International Journal of Safety and Security Engineering. https://doi.org/10.18280/ijsse.110505

Mashiane, T., Kritzinger, E., 2021. Identifying behavioral constructs in relation to user cybersecurity behavior. Eurasian Journal of Social Sciences 9, 98–122. https://doi.org/10.15604/ejss.2021.09.02.004

Mason, P., Augustyn, M.M., Seakhoa-King, A., 2021. Mixed methods research in tourism: a systematic sequential approach. Folia Turistica 56, 1–26.

Mat Dawi, N., Hwang, H.J., Abdul Jalil, N., Maresova, P., Namazi, H., 2024. Consumer Motivation to Purchase Online During COVID-19 Pandemic: Extending Protection Motivation Theory. Sage Open 14, 21582440241238613. https://doi.org/10.1177/21582440241238613

Matlala, N.P., 2023. Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa. IJBA 3, 1425–1442. https://doi.org/10.55927/ijba.v3i4.5515

Maxwell, J., Chmiel, M., 2015. Qualitative Research Design. https://doi.org/10.1093/obo/9780199756810-0126

Mazikana, A.T., 2023. The Good Part of Using a Questionnaire: Advantages and Disadvantages. SSRN Journal. https://doi.org/10.2139/ssrn.4386399

Mehraj, H., Jayadevappa, D., Haleem, S.L.A., Parveen, R., Madduri, A., Ayyagari, M.R., Dhabliya, D., 2021. Protection motivation theory using multi-factor authentication for providing security over social networking sites. Pattern Recognition Letters 152, 218–224. https://doi.org/10.1016/j.patrec.2021.10.002

Meier, Y., Schäwel, J., Kyewski, E., C. Krämer, N., 2020. Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions, in: International Conference on Social Media and Society. Presented at the SMSociety'20: International Conference on Social Media and Society, ACM, Toronto, ON, Canada, pp. 21–29. https://doi.org/10.1145/3400806.3400810

Meirte, J., Hellemans, N., Anthonissen, M., Denteneer, L., Maertens, K., Moortgat, P., Van Daele, U., 2020. Benefits and disadvantages of electronic patient-reported outcome measures: systematic review. JMIR perioperative medicine 3, e15588.

Misra, R., Mahajan, R., Singh, N., Khorana, S., Rana, N.P., 2022. Factors impacting behavioural intentions to adopt the electronic marketplace: findings from small businesses in India. Electron Markets 32, 1639–1660. https://doi.org/10.1007/s12525-022-00578-4

Mitra, D., Kulkarni, P., Pathak, P., Natrai, N.A., 2022. Importance of Coping with Cyber Security Challenges in E Commerce Business. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC). https://doi.org/10.1109/iihc55949.2022.10059851

Mofokeng, T.E., 2021. The impact of online shopping attributes on customer satisfaction and loyalty: Moderating effects of e-commerce experience. Cogent Business & Management 8. https://doi.org/10.1080/23311975.2021.1968206

Mohajan, H.K., 2020. Quantitative Research: A Successful Investigation in Natural and Social Sciences. JEDEP 9. https://doi.org/10.26458/jedep.v9i4.679

Moonstone, 2024. Impersonation fraud skyrockets by 337%, targeting financial sector – Moonstone Information Refinery [WWW Document]. Moonstone.co.za. URL https://www.moonstone.co.za/impersonation-fraud-skyrockets-by-337-targeting-financial-sector/

Morgan, D.L., 2014. Pragmatism as a Paradigm for Social Research. Qualitative Inquiry 20, 1045–1053. https://doi.org/10.1177/1077800413513733

Mosteanu, R., Narcisa, Galea, K., 2020. Artificial Intelligence and Cyber Security – Face To Face With Cyber Attack – A Maltese Case of Risk Management Approach 9.

Mou, J., Pusan National University, Republic of Korea; Cohen, J., University of the Witwatersrand, South Africa; Bhattacherjee, A., University of South Florida, USA; Kim, J., Pusan National University, Republic of Korea, 2022. A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modelling Approach in Search Advertising. JAIS 23, 196–236. https://doi.org/10.17705/1jais.00723

Mousavi, R., Chen, R., Kim, D.J., Chen, K., 2020. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems 135, 113323. https://doi.org/10.1016/j.dss.2020.113323

Moustafa, A.A., Bello, A., Maurushat, A., 2021. The Role of User Behaviour in Improving Cyber Security Management. Front. Psychol. 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Mouton, J., 1996. Understanding social research. Van Schaik Publishers.

Mtambeka, P., Mtegha, C.Q., Chigona, W., Tuyeni, T.T., 2023. Factors Affecting how University Students Comply with Cybersecurity Measures: A Case of South Africa. Presented at the Proceedings of NEMISA Digital Skills Conference

2023: Scaling Data Skills For Multidisciplinary Impact, pp. 1--16. https://doi.org/10.29007/bkw1

Mthuli, S.A., Ruffin, F., Singh, N., 2022. 'Define, Explain, Justify, Apply' (DEJA): An analytic tool for guiding qualitative research sample size. International Journal of Social Research Methodology 25, 809–821. https://doi.org/10.1080/13645579.2021.1941646

Munyendo, C.W., Acar, Y., Aviv, A.J., 2023. " In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya, in: 2023 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 570–587.

Nasr, MH, Farrag, M., Nasr, M, 2020. E-payment systems risks, opportunities, and challenges for improved results in e-business. International Journal of Intelligent Computing and Information Sciences, 20(1), pp.16-27. IJICIS 20, Nasr, M.H., Farrag, M.H. and Nasr, M., 2020.

Ncubukezit, T., 2022. Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. International Conference on Cyber Warfare and Security 17, 395–403. https://doi.org/10.34190/iccws.17.1.51

Nedbank, 2023. How to protect yourself from ransomware | Nedbank [WWW Document]. Nedbank.co.za. URL https://personal.nedbank.co.za/learn/blog/how-to-protect-yourself-from-ransomware.html (accessed 1.1.25).

Nello-Deakin, S., Vallvé, C.S., Akinci, Z.S., 2024. Who's afraid of pedestrianisation? Residents' perceptions and preferences on street transformation, Habitat International. Elsevier.

Netshirando, V., Munyoka, W., Kadyamatimba, A., 2021. Determinants of digital commerce repeat-purchase behaviour in South Africa: A rural citizen perspective. African Journal of Science, Technology, Innovation and Development 13, 701–712. https://doi.org/10.1080/20421338.2020.1797268

Newhouse, W., Weeks, S., Mulugeta, B., Sandlin, K., 2019. Multifactor authentication for e-commerce. National Institute of Standards and Technology, US Department of Commerce ….

News24, 2020. Hackers on the dark web love South Africa - here's why we suffer 577 attacks per hour [WWW Document]. News24. URL https://www.news24.com/news24/bi-archive/sa-third-highest-number-of-cybercrime-victims-2020-6 (accessed 1.1.23).

Nha, V.T.T., 2021. Understanding validity and reliability from qualitative and quantitative research traditions. JFS 37. https://doi.org/10.25073/2525-2445/vnufs.4672

Nkadimeng, V., 2019. Internet access – Survey reveals South African connectivity statistics – Moonstone Information Refinery [WWW Document]. Moonstone. URL https://www.moonstone.co.za/internet-access-survey-reveals-south-african-connectivity-statistics/#:~:text=Access%20to%20the%20Internet%20using (accessed 12.31.22).

Noble, H., Smith, J., 2015. Issues of validity and reliability in qualitative research. Evidence-based nursing 18, 34–35.

Noble, H., Smith, J., 2014. Qualitative data analysis: a practical example. Evid Based Nurs 17, 2–3. https://doi.org/10.1136/eb-2013-101603

Norman, D., Nielsen, J., 2016. The definition of user experience (UX). Nielsen Norman Group Publication 1, 2–1.

Nouri, A.I., Abdi, A.M., Hassali, M.A., 2018. Synopsis of Research Methodologies: A Brief Guide for Pharmacists. JPRI 24, 1–16. https://doi.org/10.9734/JPRI/2018/42207

Nyoni, P., Velempini, M., Mavetera, N., 2024. Privacy Perceptions on Personal Data and Data Breaches in South Africa. The African Journal of Information Systems 16, 1.

Ofori-Sasu, D., N'guessan, E.J., Nanziri, L.E., 2024. E-Commerce and Digital Trade in Africa, in: The Palgrave Handbook of International Trade and Development in Africa. Springer International Publishing, Cham, pp. 419–439. https://doi.org/10.1007/978-3-031-65715-3_22

Oh, S.J., Xiao, S., Park, B.I., Roh, T., 2023. Coping or threat? Unraveling the mechanisms enabling user acceptance of blockchain technologies. Inf Technol Manag. https://doi.org/10.1007/s10799-023-00409-8

Ojo, S., 2021. A Case of Internet Insecurity on SMEs in Nigeria: A Cybercafé Entrepreneur Experience. SAGE Publications: SAGE Business Cases Originals, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom. https://doi.org/10.4135/9781529763959

Oki, O.A., Chinaza, U., Jose, M.L., 2021. Factors Influencing the Adoption of Online Retail Shopping amongst the Internet Users in Buffalo City South Africa. https://doi.org/10.5281/ZENODO.4734074

Omar, N.A., Nazri, M.A., Ali, M.H., Alam, S.S., 2021. The panic buying behavior of consumers during the COVID-19 pandemic: Examining the influences of uncertainty, perceptions of severity, perceptions of scarcity, and anxiety. Journal of Retailing and Consumer Services 62, 102600.

Omorog, C.D., Medina, R.P., 2020. Internet Security Awareness of Filipinos: A Survey Paper. IJCSR 1, 14–26. https://doi.org/10.25147/ijcsr.2017.001.1.18

Ophoff, J., Lakay, M., 2019. Mitigating the Ransomware Threat: A Protection Motivation Theory Approach, in: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (Eds.), Information Security, Communications in Computer and Information Science. Springer International Publishing, Cham, pp. 163–175. https://doi.org/10.1007/978-3-030-11407-7_12

O'Shea, D., 2019. Digital card-not-present fraud to hit $130B by 2023 [WWW Document]. Retail Dive. URL https://www.retaildive.com/news/digital-card-not-present-fraud-to-hit-130-billion-by-2023/545171/ (accessed 1.1.23).

Osita, G.C., Okoronkwo, M.C., Esther, U.N., Vanessa, N.C., 2022. Application of Emerging Technologies in Mitigation of e-Commerce Security Challenges. CCU J. Sci 2, 2734–3766.

Otokunefor, H.O., Kari, H.K., 2008. Issues, Controversies, and Problems of Cybercafés Located in a University Campus, in: Security and Software for Cybercafés. IGI Global, pp. 62–83.

Paavola, S., 2015. Deweyan approaches to abduction. Action, Belief and Inquiry-Pragmatist Perspectives on Science, Society and Religion. Helsinki: Nordic Pragmatism Network 230–49.

Palatty, N.J., 2023. How Many Cyber Attacks Per Day: The Latest Stats and Impacts in 2023 - Astra Security Blog [WWW Document]. ASTRA. URL

https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/ (accessed 1.1.24).

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., Hoagwood, K., 2015. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Adm Policy Ment Health 42, 533–544. https://doi.org/10.1007/s10488-013-0528-y

Papagiannidis, S., Alamanos, E., Bourlakis, M., Dennis, C., 2023. The Pandemic Consumer Response: A Stockpiling Perspective and Shopping Channel Preferences. British Journal of Management 34, 664–691. https://doi.org/10.1111/1467-8551.12616

Parker, H.J., 2020. An Online Information Security Awareness Model: The Disclosure of Personal Data.

Parker, H.J., Flowerday, S., 2021. Understanding the disclosure of personal data online. Information and Computer Security. https://doi.org/10.1108/ICS-10-2020-0168

Parvez, V., 2023. A Study on Perspective of Global E-commerce in Emerging Market 11.

Patten, M., 2016. Questionnaire research: A practical guide. routledge.

Paun, C., Ivascu, C., Olteteanu, A., Dantis, D., 2024. The Main Drivers of E-Commerce Adoption: A Global Panel Data Analysis. JTAER 19, 2198–2217. https://doi.org/10.3390/jtaer19030107

Pentz, C.D., du Preez, R., Swiegers, L., 2020. To bu(Y) or not to bu(Y): Perceived risk barriers to online shopping a mong South African generation Y consumers. Cogent Business & Management 7, 1827813. https://doi.org/10.1080/23311975.2020.1827813

Peripherals, M., 2023. Phishing, smishing, the security is missing! [WWW Document]. ITWeb. URL https://www.itweb.co.za/article/phishing-smishing-the-security-is-missing/O2rQGMAEDxDMd1ea (accessed 1.1.24).

Petrosyan, A., 2024. Credential stuffing attack share worldwide by vertical 2018 l Statistic [WWW Document]. Statista. URL https://www.statista.com/statistics/885318/login-attempts-globally-credential-stuffing-attacks-by-industry/ (accessed 1.1.25).

Phamthi, V.A., Nagy, Á., Ngo, T.M., 2024. The influence of perceived risk on purchase intention in e-commerce—Systematic review and research agenda. Int J Consumer Studies 48, e13067. https://doi.org/10.1111/ijcs.13067

Phomkamin, J., Pumpuang, C., Potijak, P., Sangngam, S., Ketprasit, I., Mujtaba, B., 2021. Engagement Strategies for E-commerce Businesses in the Modern Online World.

Piedmont, R.L., 2023. Construct Validity, in: Maggino, F. (Ed.), Encyclopedia of Quality of Life and Well-Being Research. Springer International Publishing, Cham, pp. 1332–1332. https://doi.org/10.1007/978-3-031-17299-1_539

Pobee, F., 2021. Preliminary insight into electronic commerce adoption in a developing country: evidence from Ghana. IJEB 16, 377. https://doi.org/10.1504/IJEB.2021.118497

Ponto, J., 2015. Understanding and Evaluating Survey Research. JADPRO 6. https://doi.org/10.6004/jadpro.2015.6.2.9

Prasad, R., Rohokale, V., 2020. Cyber Security: The Lifeline of Information and Communication Technology, Springer Series in Wireless Technology. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-31703-4

Prasetyo, Rahman, Wahab, S.N., 2022. Predicting E-commerce Consumers' Loyalty Through the Lens of Protection Motivation Theory, in: 2022 International Conference on Data Analytics for Business and Industry (ICDABI). IEEE, Sakhir, Bahrain, pp. 418–422. https://doi.org/10.1109/ICDABI56818.2022.10041643

Prasetyo, R., Wahab, S.N., 2022. Predicting E-commerce Consumers' Loyalty Through the Lens of Protection Motivation Theory. Presented at the 2022 International Conference on Data Analytics for Business and Industry, ICDABI 2022, pp. 418–422. https://doi.org/10.1109/ICDABI56818.2022.10041643

Price, O., Lovell, K., 2018. Quantitative research design.

Puchert, D., 2024. How to spot a card-skimmer at an ATM or restaurant [WWW Document]. URL https://mybroadband.co.za/news/security/545421-how-to-spot-a-card-skimmer-at-an-atm-or-restaurant.html (accessed 12.31.23).

Pulla, V., Carter, E., 2018. Employing interpretivism in social work research. International Journal of Social Work and Human Services Practice 6, 9–14.

Qabajeh, I., Thabtah, F., Chiclana, F., 2018. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Computer Science Review 29, 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003

Rahimi, S., Khatooni, M., 2024. Saturation in qualitative research: An evolutionary concept analysis. International Journal of Nursing Studies Advances 6, 100174. https://doi.org/10.1016/j.ijnsa.2024.100174

Rahman, Md.A., Amjad, M., Ahmed, B., Siddik, Md.S., 2020. Analyzing Web Application Vulnerabilities: An Empirical Study on E-Commerce Sector in Bangladesh, in: Proceedings of the International Conference on Computing Advancements. Presented at the ICCA 2020: International Conference on Computing Advancements, ACM, Dhaka, Bangladesh, pp. 1–6. https://doi.org/10.1145/3377049.3377107

Rahman, Md.M., Tabash, M.I., Salamzadeh, A., Abduli, S., Rahaman, Md.S., 2022. Sampling Techniques (Probability) for Quantitative Social Science Researchers: A Conceptual Guidelines with Examples. SEEU Review 17, 42–51. https://doi.org/10.2478/seeur-2022-0023

Rai, R., Rohilla, A., Rai, A., 2024. Understanding Cybersecurity Threats in E-Commerce, in: Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning. IGI Global, pp. 501–522.

Raj Sreenath, S.S., Hewitt, B., Sreenath, S., 2024. Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. Behaviour & Information Technology 1–16. https://doi.org/10.1080/0144929X.2024.2314255

Ramsay, J.D., Cozine, K., Comiskey, J., 2020. Theoretical foundations of homeland security: strategies, operations, and structures. Routledge.

Ramsern, A., Govender, K., 2023. E-Commerce Challenges of SMMEs In South Africa During the Covid-19 Pandemic. Journal of Positive Psychology & Wellbeing 2023 7, 1282–1308.

Rao, U., 2023. Overview of Cyber Security. IJARSCT 47–51. https://doi.org/10.48175/IJARSCT-9470

Read, K., Van Der Schyff, K., 2020. Modelling the intended use of Facebook privacy settings. SA Journal of Information Management 22. https://doi.org/10.4102/sajim.v22i1.1238

Remenyi, D., 2022. Case study research: The quick guide series. UJ Press.

Resmo, 2024. Social Engineering Statistics to Know in 2023 | Resmo [WWW Document]. www.resmo.com. URL https://www.resmo.com/blog/social-engineering-statistics (accessed 1.1.24).

Rhodes University, 2024. RU-HREC Standard Operating Procedures Index [WWW Document]. Ru.ac.za. URL https://www.ru.ac.za/researchgateway/ethics/standardoperatingprocedures/ (accessed 1.1.25).

Ribadu, M.B., Rahman, W.N.W.Ab., 2019. An integrated approach towards Sharia compliance E-commerce trust. Applied Computing and Informatics 15, 1–6. https://doi.org/10.1016/j.aci.2017.09.002

Rice, S., Winter, S.R., Doherty, S., Milner, M., 2017. Advantages and disadvantages of using internet-based survey methods in aviation-related research. Journal of Aviation Technology and Engineering 7, 5.

Richard, A.F., 2023. Cyber Smart: Your Guide to Online Security and Responsibility.

Roberts, G., Rahman, S., 2021. Does Digital Native Status Impact End-User Antivirus Usage? International Journal of Computer Networks and Communications 13, 121–142. https://doi.org/10.5121/ijcnc.2021.13207

Roberts, Gerrianne, Rahman, S.S., 2021. Does digital native status impact end-user antivirus usage? International Journal of Computer Networks & Communications (IJCNC) 13. https://doi.org/10.5121/ijcnc.2021.13207

Rodríguez-Ardura, I., Meseguer-Artola, A., 2020. How to prevent, detect and control common method variance in electronic commerce research, Journal of theoretical and applied electronic commerce research. SciELO Chile.

Roestenburg, W.J.H., Strydom, H., Fouché, C.B., De Vos, A.S., 2021. Research at grass roots : for the social sciences and human services professions. Van Schaik Publishers.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychology: A source book 153–176.

Rogers, R.W., 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology 91, 93–114. https://doi.org/10.1080/00223980.1975.9915803

Roller, M.R., 2020. The In-depth Interview Method.

Roopa, S., Rani, M., 2012. Questionnaire Designing for a Survey. JIOS 46, 273–277. https://doi.org/10.5005/jp-journals-10021-1104

Rosário, A.T., 2023. Security in Digital Marketing: Challenges and Opportunities. Confronting Security and Privacy Challenges in Digital Marketing 206–233.

Rouge, P., Yeung, C., Salsburg, D., Calandrino, J.A., 2020. Checkout checkup: Misuse of payment data from web skimming.

Rowland, E., Conolly, A., 2024. A worked example of contextualising and using reflexive thematic analysis in nursing research. Nurse Researcher. https://doi.org/10.7748/nr.2024.e1924

Ruan, W., Kang, S., Song, H., 2020. Applying protection motivation theory to understand international tourists' behavioural intentions under the threat of air pollution: A case of Beijing, China. Current Issues in Tourism 23, 2027–2041. https://doi.org/10.1080/13683500.2020.1743242

Rus, A.-C., El-Hajj, M., Sarmah, D.K., 2024. NAISS: A reverse proxy approach to mitigate MageCart's e-skimmers in e-commerce. Computers & Security 140, 103797. https://doi.org/10.1016/j.cose.2024.103797

Rus, C., Sarmah, D., El-Hajj, M., 2023. Defeating MageCart Attacks in a NAISS Way:, in: Proceedings of the 20th International Conference on Security and Cryptography. Presented at the 20th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, Rome, Italy, pp. 691–697. https://doi.org/10.5220/0012079300003555

SA Experience, 2024. Port Elizabeth [WWW Document]. South Africa Experience. URL https://www.southafrica-experience.com/destinations/cities/port-elizabeth (accessed 12.31.23).

Sabric, 2023. Annual Crime Statistics Executive Summary Qualification of Information Contact Crime Digital Crime Application Fraud Card Fraud.

Sadık, O., 2019. A discussion of the concepts of validity and reliability in qualitative and quantitative research.

Saeed, S., 2023. A Customer-Centric View of E-Commerce Security and Privacy. Applied Sciences 13, 1020. https://doi.org/10.3390/app13021020

Sahoo, S.R., Gupta, B.B., 2019. Classification of various attacks and their defence mechanism in online social networks: a survey. Enterprise Information Systems 13, 832–864. https://doi.org/10.1080/17517575.2019.1605542

Sajikumar, S., Ajithkumar, N., Vijayan, G., 2024. Exploring the Interplay of Privacy Concerns, Mobile Cybersecurity Awareness, and Protective Motivation Behavior. International Journal of Religion 5, 612–619.

Sam, T.J., liezel, cilliers, Willie, C., 2019. “The African Digital Citizen’s Awareness of Online Information Privacy”.

Saunders, M., Lewis, P., Thornhill, A., 2023. Research methods for business students, Ninth edition. ed. Pearson, Harlow.

Saunders, Mark.N.K., Lewis, P., Thornhill, A., 2019. Research methods for business students, Eighth Edition. ed. Pearson, New York.

Schneider, M., Rahman, S., 2021. Protection Motivation Theory Factors That Influence Undergraduates to Adopt Smartphone Security Measures 9.

Schwendtner, T., Amsl, S., Teller, C., Wood, S., 2024. Shopping behaviour of elderly consumers: change and stability during times of crisis. International Journal of Retail and Distribution Management 52, 1–15. https://doi.org/10.1108/IJRDM-01-2023-0029

Semrush, 2024. Top Retail Websites in South Africa - March 2024 Most Visited & Popular Rankings [WWW Document]. Semrush. URL https://www.semrush.com/website/top/south-africa/e-commerce-and-retail/ (accessed 1.1.24).

Shabe, T., Kritzinger, E., Loock, M., 2017. Scorecard Approach for Cyber-Security Awareness. SETE@ICWL. https://doi.org/10.1007/978-3-319-71084-6_16

Shah, I.A., Jhanjhi+, N.Z., Brohi, S.N., 2024. Secure model for credit card fraud detection using ML approaches, in: 8th IET Smart Cities Symposium (SCS 2024). IET, pp. 709–715.

Shah, P., Agarwal, A., 2020. Cybersecurity behaviour of smartphone users in India: an empirical ana lysis. ICS 28, 293–318. https://doi.org/10.1108/ics-04-2019-0041

Shaikh, J.R., Babar, S.D., Iliev, G., 2017. E-commerce Development with Respect to its Security Issues and Solutions: A Literature Review.

Shakela, V., Jazri, H., 2019. Assessment of spear phishing user experience and awareness: an evaluation framework model of spear phishing exposure level (spel) in the namibian financial industry, in: 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). IEEE, pp. 1–5.

Sharma, G., 2017. Pros and cons of different sampling techniques. International journal of applied research 3, 749–752.

Sharma, L.R., Bidari, S., Bidari, D., Neupane, S., Sapkota, R., 2023. Exploring the mixed methods research design: types, purposes, strengths, challenges, and criticisms. Glob Acad J Linguist Lit 5.

Sharma, M., 2017. Safe by Design – An Overview of UX Security [WWW Document]. Toptal Design Blog. URL https://www.toptal.com/designers/product-design/ux-security (accessed 1.1.24).

Sharma, S.K., Kanchan, T., Krishan, K., 2018. Descriptive Statistics, in: López Varela, S.L. (Ed.), The Encyclopedia of Archaeological Sciences. Wiley, pp. 1–8. https://doi.org/10.1002/9781119188230.saseas0165

Shava, F.B., Van Greunen, D., 2013. Factors affecting user experience with security features: A case study of an academic institution in Namibia, in: 2013 Information Security for South Africa. Presented at the 2013 Information Security for South Africa, IEEE, Johannesburg, South Africa, pp. 1–8. https://doi.org/10.1109/ISSA.2013.6641061

Shenton, A.K., 2004. Strategies for ensuring trustworthiness in qualitative research projects. EFI 22, 63–75. https://doi.org/10.3233/EFI-2004-22201

Shiri, V., Xiong, M., Cheng, J., Guo, J.L.C., 2024. Motivating Users to Attend to Privacy: A Theory-Driven Design Study. https://doi.org/10.1145/3643834.3661544

Shook, J.R., 2023. Pragmatism. MIT Press.

Singh, N., Benmamoun, M., Meyr, E., Arikan, R.H., 2021. Verifying rigor: analyzing qualitative research in international marketing, International marketing review. Emerald Publishing Limited.

Singhal, K., Nandini Singhal, Mohit Jain, Kartikey Singh, Rashmi Pandey, 2023. Silencing the Scammers: Effective Strategies in Credit Card Fraud Detection. IJSRCSEIT 82–86. https://doi.org/10.32628/CSEIT239062

Skjelvik, A., Vestad, A., 2023. Digital safety alarms – Exploring the understandings of the cybersecurity practice in Norwegian municipalities, in: European Interdisciplinary Cybersecurity Conference. Presented at the EICC 2023: European Interdisciplinary Cybersecurity Conference, ACM, Stavanger Norway, pp. 129–133. https://doi.org/10.1145/3590777.3590798

Soava, G., Mehedintu, A., Sterpu, M., 2022. Analysis and Forecast of the Use of E-Commerce in Enterprises of the European Union States. Sustainability 14, 8943. https://doi.org/10.3390/su14148943

Sommestad, T., Karlzén, H., Hallberg, J., 2015. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy 9, 26–46. https://doi.org/10.4018/ijisp.2015010102

Spanning, 2022. Cybersecurity Awareness: Definition, Importance & More [WWW Document]. Spanning. URL https://spanning.com/blog/cybersecurity-awareness/

Stake, R.E., 2013. Multiple case study analysis. Guilford Press.

Stapor, K., 2020. Descriptive and Inferential Statistics, in: Introduction to Probabilistic and Statistical Methods with Examples in R, Intelligent Systems Reference Library. Springer International Publishing, Cham, pp. 63–131. https://doi.org/10.1007/978-3-030-45799-0_2

Stone, C., 2019. A Defense and Definition of Construct Validity in Psychology. Philos. of Sci. 86, 1250–1261. https://doi.org/10.1086/705567

Strycharz, J., Van Noort, G., Smit, E., Helberger, N., 2019. Protective behavior against personalized ads: Motivation to turn personalization off. Cyberpsychology 13. https://doi.org/10.5817/CP2019-2-1

Strzelecki, A., Rizun, M., 2022. Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. Sustainability 14, 5866. https://doi.org/10.3390/su14105866

Subramani, K., Melicher, W., Starov, O., Vadrevu, P., Perdisci, R., 2022. PhishInPatterns: measuring elicited user interactions at scale on phishing websites, in: Proceedings of the 22nd ACM Internet Measurement Conference. Presented at the IMC '22: ACM Internet Measurement Conference, ACM, Nice France, pp. 589–604. https://doi.org/10.1145/3517745.3561467

Sulaiman, N.S., Fauzi, M.A., Hussain, S., Wider, W., 2022. Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information 13, 413. https://doi.org/10.3390/info13090413

Sunet, E., Zenzo, M., 2022. Investigating Cyber Security Awareness (CSA) Amongst Managers in Small and Medium Enterprises (SMEs), in: Lecture Notes in Networks and Systems. Springer International Publishing, Cham, pp. 180–191. https://doi.org/10.1007/978-3-030-85799-8_16

Szumski, O., 2018. Cybersecurity best practices among Polish students. Procedia Computer Science 126, 1271–1280. https://doi.org/10.1016/j.procs.2018.08.070

Taherdoost, H., 2022a. Cybersecurity vs. Information Security. Procedia Computer Science 215, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

Taherdoost, H., 2022b. Designing a Questionnaire for a Research Paper: A Comprehensive Guide to Design and Develop an Effective Questionnaire. AJMS 11, 8–16. https://doi.org/10.51983/ajms-2022.11.1.3087

Taherdoost, H., 2016a. Sampling methods in research methodology; how to choose a sampling technique for research. How to choose a sampling technique for research (April 10, 2016).

Taherdoost, H., 2016b. Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. How to test the validation of a questionnaire/survey in a research (August 10, 2016).

Tawalbeh, L.A., Muheidat, F., 2023. Factors that Motivate Defense Against Social Engineering Attacks Across Organizations. Procedia Computer Science 224, 75–82. https://doi.org/10.1016/j.procs.2023.09.013

Tehseen, S., Ramayah, T., Sajilan, S., 2017. Testing and controlling for common method variance: A review of available methods, Journal of management sciences.

Tenny, S., Brannan, J.M., Brannan, G.D., 2017. Qualitative study.

Teofilus, T., Wananda, V., Hongdiyanto, C., Sutrisno, T.F.C.W., 2020. A Study of Indonesian Online Marketplace: Information Processing Theory Paradigm. Journal of Distribution Science 18, 75–87. https://doi.org/10.15722/JDS.18.8.202008.75

Terlizzi, M.A., Brandimarte, L., Brown, S.A., Sanchez, O.P., 2019. Privacy concerns and protection motivation theory in the context of mobile banking. European Conference on Information Systems.

Thwaites Bee, D., Murdoch-Eaton, D., 2016. Questionnaire design: the good, the bad and the pitfalls. Arch Dis Child Educ Pract Ed 101, 210–212. https://doi.org/10.1136/archdischild-2015-309450

Tian, X., 2024. Unraveling the dynamics of password manager adoption: a deeper dive into critical factors. Information & Computer Security.

Timmins, F., 2015. Surveys and questionnaires in nursing research. Nursing Standard 29, 42–50. https://doi.org/10.7748/ns.29.42.42.e8904

Torten, R., Reaiche, C., Boyle, S., 2018. The impact of security awarness on information technology professionals' behavior. Computers & Security 79, 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Toyon, M.A.S., 2021. Explanatory sequential design of mixed methods research: Phases and challenges. IJRBS 10, 253–260. https://doi.org/10.20525/ijrbs.v10i5.1262

Trafimow, D., 2022. Construct validity. International Journal of Aviation Research 14.

Tran, D.V., Nguyen, P.V., Le, L.P., Nguyen, S.T.N., 2024. From awareness to behaviour: understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis.

TransUnion, 2024. Digital Fraud Attempts Coming From South Africa the Highest in Telecommunications [WWW Document]. Digital Fraud Attempts Coming From South Africa the Highest in Telecommunications. URL https://newsroom.transunion.co.za/digital-fraud-attempts-where-the-consumer-was-in-south-africa-the-highest-in-telecommunications-financial-services-and-communities/

Tsai, H.S., Jiang, M., Alhabash, S., Larose, R., Rifon, N.J., Cotten, S.R., 2016a. Understanding online safety behaviors: A protection motivation theory perspective. Computers and Security 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016b. Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tsai, H.-Y.S., Jiang, M., Alhabash, S., Larose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: A protection motivation theory perspective. Computers and Security 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tsoai, N., Chipunza, C., 2022. Relationship between personality of owner-managers and performance of internet cafes in Free State, South Africa. Southern African Journal of Entrepreneurship and Small Business Management 14, 1–12.

Tutar, G., Küçükoğlu, H., Özdemir, A., Alkan, Ö., Ipekten, O.B., 2024. An Investigation of Gender Differences in E-Commerce Shopping Frequency During COVID-19: Evidence From Türkiye. Sage Open 14, 21582440241287630. https://doi.org/10.1177/21582440241287630

Unger, R., Chandler, C., 2012. A project guide to UX design : for user experience designers in the field or in the making. New Riders.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., Briggs, P., 2019. Using protection motivation theory in the design of nudges to improve online security behavior.

International Journal of Human-Computer Studies 123, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van Der Schyff, K., Foster, G., Renaud, K., Flowerday, S., 2023. Online privacy fatigue: a scoping review and research agenda. Future Internet 15, 164. https://doi.org/ 10.3390/fi15050164

Vanishree, 2012. Customer Perception towards Online Shopping.

Varachia, M., 2022. Adoption of cybersecurity practices for SMMEs.

Varma, G., Chauhan, R., Singh, D., 2023. Towards cyber awareness among smart device users: an interactive, educational display of IoT device vendors compromise history. Multimed Tools Appl 83, 52795–52818. https://doi.org/10.1007/s11042-023-17520-1

Vasupula, N., Munnangi, V., Daggubati, S., 2022. Modern Privacy Risks and Protection Strategies in Data Analytics, in: Reddy, V.S., Prasad, V.K., Wang, J., Reddy, K.T.V. (Eds.), Soft Computing and Signal Processing, Advances in Intelligent Systems and Computing. Springer Singapore, Singapore, pp. 81–89. https://doi.org/10.1007/978-981-16-1249-7_9

Vega, J., Shevchyk, D., Cheng, Y., 2022. A literature survey of phishing and its countermeasures, in: Second Annual Computer Science Conference for CSU Undergraduates.

Veiga, A.D., Ochola, E.O., Mujinga, M., Mwim, E., 2022. Investigating Data Privacy Evaluation Criteria and Requirements for e- Commerce Websites. ARTIIS.

Verkijika, S.F., 2019. An Evaluation of the Password Practices on Leading e-Commerce Websites in South Africa, in: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (Eds.), Information Security, Communications in Computer and Information Science. Springer International Publishing, Cham, pp. 104–114. https://doi.org/10.1007/978-3-030-11407-7_8

Verusboc, 2022. Cybersecurity Awareness | Verus Bank of Commerce [WWW Document]. Verusboc.com. URL https://www.verusboc.com/resources/cybersecurity-awareness- (accessed 1.1.24).

Vestad, A., 2022. Personality Traits and Security Motivation, in: Blobel, B., Yang, B., Giacomini, M. (Eds.), Studies in Health Technology and Informatics. IOS Press. https://doi.org/10.3233/SHTI220980

Viji, D., Dixit, V., Jha, V., 2022. Phishing Website Detection and Classification, in: Manogaran, G., Shanthini, A., Vadivu, G. (Eds.), Proceedings of International Conference on Deep Learning, Computing and Intelligence, Advances in Intelligent Systems and Computing. Springer Nature Singapore, Singapore, pp. 401–411. https://doi.org/10.1007/978-981-16-5652-1_35

Visinescu, L.L., Azogu, O., Ryan, S.D., Wu, Y. “Andy”, Kim, D.J., 2016. Better Safe than Sorry: A Study of Investigating Individuals’ Protection of Privacy in the Use of Storage as a Cloud Computing Service. International Journal of Human–Computer Interaction 32, 885–900. https://doi.org/10.1080/10447318.2016.1204838

Vogt, W.P., Gardner, D.C., Haeffele, L.M., 2012. When to use what research design. Guilford Press.

Von Solms, B., Von Solms, R., 2018. Cybersecurity and information security – what goes where? ICS 26, 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Vosta, L.N., Jalilvand, M.R., 2023. Electronic trust-building for hotel websites: a social exchange theory perspective. Journal of Islamic Marketing 14, 2689–2714.

Vrhovec, S., Mihelič, A., 2021. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Computers & Security 106, 102309. https://doi.org/10.1016/j.cose.2021.102309

Wahab, F., Khan, I., Kamontip, Hussain, T., Amir, A., 2023. An investigation of cyber attack impact on consumers’ intention to purchase online. Decision Analytics Journal 8, 100297. https://doi.org/10.1016/j.dajour.2023.100297

Wall, A., Simmering, M., Fuller, C., Waterwall, B., 2022. Manipulating common method variance via experimental conditions, Electronic Journal of Business Research Methods.

Walsham, G., 1995. The Emergence of Interpretivism in IS Research. Information Systems Research 6, 376–394. https://doi.org/10.1287/isre.6.4.376

Wang, M., Kunasekaran, P., Rasoolimanesh, S.M., 2022. What influences people's willingness to receive the COVID-19 vaccine for international travel? Current Issues in Tourism 25, 192–197. https://doi.org/10.1080/13683500.2021.1929874

Wang, Yazhu Maggie, 2023. Decreasing the Problematic Use of an Information System: A Conceptual Replication in the Context of Digital Streaming Services. TRR 9, 1–30. https://doi.org/10.17705/1atrr.00077

Wang, Y.M., 2023. Decreasing the Problematic Use of an Information System: A Conceptual Replication in the Context of Digital Streaming Services. AIS Transactions on Replication Research 9, 1–30. https://doi.org/10.17705/1atrr.00077

Wannenburg, M.C., Nieman, A., Steyn, B., Wannenburg, D.G., 2023. South Africans' susceptibility to phishing attacks. Southern African Journal of Accountability and Auditing Research 25, 53–72. https://doi.org/10.54483/sajaar.2023.25.1.4

Wasti, S.P., Simkhada, P., Van Teijlingen, E., Sathian, B., Banerjee, I., 2022. The Growing Importance of Mixed-Methods Research in Health. Nepal J Epidemiology 12, 1175–1178. https://doi.org/10.3126/nje.v12i1.43633

Wijaya, S.W., Polina, A.M., 2014. Internet Access At Public Access Venues In A Developing Countries: Lessons from Yogyakarta, Indonesia. The Journal of Community Informatics 10.

Willie, M.M., 2024. Population and Target Population in Research Methodology. GRSSE 4, 75–79. https://doi.org/10.52970/grsse.v4i1.405

Wright, K.B., 2005. Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services, Journal of Computer-Mediated Communication. Oxford University Press Oxford, UK.

Wu, H.-C., Chen, S.X., Xu, H., 2024. Exploring the drivers of COVID-19 protective behaviors among Singaporean tourists to Indonesia using travel bubbles. Curr Psychol 43, 13972–13985. https://doi.org/10.1007/s12144-022-03629-3

Xinyuan, W., 2021. On the Feasibility of Detecting Software Supply Chain Attacks. IEEE Military Communications Conference. https://doi.org/10.1109/MILCOM52596.2021.9652901

Yang, N., Singh, T., Johnston, A., 2020. A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self Determination Theory. AIS Transactions on Replication Research 6, 10.

Yasar, K., 2022. What Is a Man-in-the-Middle Attack (MitM)? - Definition from IoTAgenda [WWW Document]. TechTarget. URL https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM (accessed 1.1.25).

Yeng, P.K., Yang, B., Fauzi, M.A., Nimbe, P., 2023. A framework for exploring incentive methods towards reducing phishing susceptibility in Healthcare: Based on a review and in-the-wild field study approach. 2023 Intelligent Methods, Systems, and Applications (IMSA) 228–234.

Yin, R.K., 2018. Case study research and applications. Sage Thousand Oaks, CA.

Yin, R.K., 2014. Case study research: Design and methods, 5th ed. Sage.

Young, M., Varpio, L., Uijtdehaage, S., Paradis, E., 2020. The Spectrum of Inductive and Deductive Research Approaches Using Quantitative and Qualitative Data. Academic Medicine 95, 1122–1122. https://doi.org/10.1097/ACM.0000000000003101

Youssef, H.A.H., Hossam, A.T.A., 2023. Privacy Issues in AI and Cloud Computing in E-commerce Setting: A Review. International Journal of Responsible Artificial Intelligence 13, 37–46.

Yuniar, A., Fibrianto, A., 2021. Consumer's Privacy Perception in Online Shopping Behavior using E-Commerce Platform, in: Proceedings of the 1st ICA Regional Conference, ICA 2019, October 16-17, 2019, Bali, Indonesia. Presented at the Proceedings of the 1st ICA Regional Conference, ICA 2019, October 16-17 2019, Bali, Indonesia, EAI, Bali, Indonesia. https://doi.org/10.4108/eai.16-10-2019.2304352

Zawaideh, F.H., Abu-Ulbeh, W., Mjlae, S.A., El-Ebiary, Y.A.B., Al Moaiad, Y., Das, S., 2023. Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce, in: 2023 International Conference on Computer Science and Emerging Technologies (CSET). IEEE, pp. 1–7.

Zende, S.S., 2022. Digitalization in India Prospect and Challenges. INJETECH.

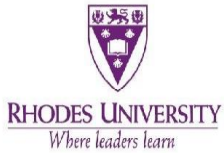
Zhang, D., Lim, J., Zhou, L., Dahl, A.A., 2021. Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study (Preprint). https://doi.org/10.2196/preprints.31633

Zhang, P., Oest, A., Cho, H., Sun, Z., Johnson, R.C., Wardman, B., Sarker, S., Kapravelos, A., Bao, T., Wang, R., 2021. Crawlphish: Large-scale analysis of client-side cloaking techniques in phishing, in: 2021 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 1109–1124.

Zhao, Y., Ni, Q., Zhou, R., 2018. What factors influence the mobile health service adoption? A meta-analysis and the moderating role of age. International Journal of Information Management 43, 342–350. https://doi.org/10.1016/j.ijinfomgt.2017.08.006

APPENDICES

Appendix 1: Ethical clearance



Rhodes University Human Research Ethics Committee
Room 8 Truro House, Makhanda, 6139, South Africa
PO Box 94, Makhanda, 6140, South Africa
t: +27 (0) 46 603 7314
e: ethics-committee@ru.ac.za
https://www.ru.ac.za/researchgateway/ethics/
NHREC Registration number: RC-241114-045

21 February 2025

Mr Segun Musa Obisesan
Computer Science & Information Systems
Rhodes University

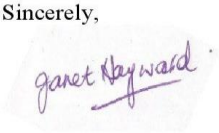
Dear Mr Obisesan,

Re: Using the Protection Motivation Theory to understand the impact of User Cybersecurity Practices on the utilisation of E-commerce platforms by online shoppers: A Scoping Review.

The Rhodes University Human Research Ethics Committee (RU-HREC) has reviewed your request for ethics waiver. Your research involves analysis of material that is available in the public domain and does not involve interaction with human participants. As such it does not require research ethics approval, and your request for ethics waiver has been approved.

Ethics Waiver Number: RUHREC-2025-0002

Sincerely,



Dr Janet Hayward
Chair of Rhodes University Human Research Ethics Committee

Appendix 2: Letters of permission to conduct research

KAYMECH

Address: 18 Parliament Street, Central, Port Elizabeth 6001

Phone: +27 717 329 299
Email: kmechcafe@gmail.com

Date: 13 March 2025

Mr Segun M. Obisesan (Master Student)
Department of Information Systems
Rhodes University
Drosty Road
Grahamstown, 6139

Subject: Letter of Permission to Conduct Research at Kaymech Internet Café

Dear Mr. Obisesan,

Following your request dated **04 March 2025**, we acknowledge receipt of your application to conduct research at our **Internet Café**. We hereby grant you permission to conduct your study titled:

"Using the Protection Motivation Theory to Evaluate the Impact of Cybersecurity Practices on User Experiences with E-commerce Platforms in Gqeberha, Eastern Cape Province."

The permission is granted under the following conditions:

1. The research activities, including the administration of self-administered questionnaires and semi-structured interviews, should be conducted as agreed between these months **(12 April to 12 July 2025)**. Any extension will require the approval of the business owner.
2. The researcher must ensure that all data collected from internet café users remain confidential and are used strictly for academic purposes.
3. The study should be conducted in a manner that does not interfere with the normal operations of the café or inconvenience our customers.
4. All research activities should adhere to ethical guidelines as outlined in the ethical clearance certificate issued by Rhodes University.
5. Upon completion of the study, you may provide a summary of key findings and recommendations to Keymech Internet Café that could help our customer regarding cybersecurity practices.

Should you require any further clarification, please feel free to contact us to 071 732 9299.

We wish you success in your research.

Yours sincerely,

Olaitan Oyedemi
Owner, Kaymech Internet Café
+27 717 329 299

STUDIO4 PHOTOGRAPHY

Address: 453 Govan Mbeki Avenue, North End, Port Elizabeth 6001
Phone: +27 835 057 446
Email: studio4photo@gmail.com

14 March 2025

To:
Segun M. Obisesan
Master's Student
Department of Information Systems
Rhodes University
Drosty Road, Grahamstown, 6139

Subject: Permission letter to Conduct Research at Studio4 Photography

Dear Mr. Obisesan,

With reference to your request dated 04 March 2025, seeking permission to conduct research at our Studio4 Photography, we hereby grant you permission to collect data for your study ***Using the Protection Motivation Theory to Evaluate the Impact of Cybersecurity Practices on User Experiences with E-commerce Platforms in Gqeberha, Eastern Cape Province***, which we believe it could be of help to our clients.

We acknowledge the purpose and objectives of your research, particularly in assessing cybersecurity practices and their influence on user experiences within our business environment.

As part of this approval, please note the following conditions that must be adhered to:

1. All information collected from our clients must remain strictly confidential and used solely for academic research purposes.
2. The research activities (i.e., distribution of self-administered questionnaires and semi-structured interviews) should not interfere with the normal operations of the Studio4 Photopraphy.
3. The approved data collection period is from **12 April to 12 July 2025.** If there is a need for extension, you will need to seek the approval of the business owner.
4. You must adhere to the ethical standards outlined in the clearance certificate issued by Rhodes University.

Should you require further assistance or have any inquiries during your research, please feel free to contact me as indicated in the letter head above.

We wish you success in your research.

Yours Sincerely,

Monsezi Malalanse
Owner, Studio4 Photography

SK DESIGN SERVICES

For: Graphics - Internet - Printing

Date: 14 March 2025

To:
Segun Musa Obisesan,
Master Student
Department of Information Systems
Rhodes University
Drosty Road, Grahamstown

RE: Permission to Conduct Research at SK Design Services

Dear Mr. Obisesan,

I acknowledge receipt of your request to conduct research at SK Design Services as part of your study titled: *"Using the Protection Motivation Theory to Evaluate the Impact of Cybersecurity Practices on User Experiences with E-commerce Platforms in Gqeberha, Eastern Cape Province."*

After reviewing your request, I am pleased to grant permission for data collection at the premises under the following conditions:

- You may distribute self-administered questionnaires and conduct interviews either in person or over the phone, ensuring minimal disruption to our business operations.
- The researcher should conduct his study within the stipulated period: **from April to July, 2025 (i.e., 3 Months)** and should you require any further extension, approval should be obtained from me.
- All data collected must be anonymized, and no personal or sensitive information about our clients may be shared or stored improperly.
- The researcher must adhere to the ethical standards outlined in your university's ethical clearance certificate.

I trust that you will uphold the highest ethical standards while conducting your research. Should you require any additional assistance or clarification, please do not hesitate to contact me.

I wish you success in your study.

Regards

Stephen Kwame Asamoah
Owner
SK Design Services

081 469 4994
374a Govan Mbeki Street, North En
Gqeberha
skdesignservices@gmail.com

Appendix 3: Language Editing Certificate

Certificate of Editing

This is to certify that the dissertation

USING PROTECTION MOTIVATION THEORY TO EVALUATE THE IMPACT OF CYBERSECURITY PRACTICES ON USER EXPERIENCE WITH E-COMMERCE PLATFORMS AMONG INTERNET CAFÉ USERS IN GQEBERHA

by

SEGUN OBISESAN

has been proofread and edited for English language usage.

Date: 20 AUGUST 2025

LHugo

Lianne Hugo

Language Practitioner
B.A. (HMS)
PGCE

Appendix 4: Turnitin Digital Receipt

turnitin

Digital Receipt

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

The first page of your submissions is displayed below.

Submission author:	segun obisesan
Assignment title:	Plagiarism Checkers Part 1 (Moodle TT)
Submission title:	My Master's Thesis
File name:	65424_segun_obisesan_My_Masters_Thesis_553663_17560924...
File size:	5.84M
Page count:	244
Word count:	72,664
Character count:	423,586
Submission date:	27-Aug-2025 10:14AM (UTC+0200)
Submission ID:	2727242251

USING PROTECTION MOTIVATION THEORY TO EVALUATE THE IMPACT OF CYBERSECURITY PRACTICES ON USER EXPERIENCE WITH E-COMMERCE PLATFORMS AMONG INTERNET CAFÉ USERS IN GQEBERHA

By

Segun Musa Obisesan

Thesis submitted in fulfilment of the requirements for the award of the Degree of

Master of Commerce

in

Information Systems

Faculty of Commerce

Of

Rhodes University

Supervisor: Dr Moses Moyo

Date of Submission: September 2025

Appendix 5: Recent Turnitin Similarity Report

Turnitin Originality Report

Processed on: 27-Aug-2025 10:17 SAST
ID: 2727242251
Word Count: 72664
Submitted: 3

My Master's Thesis By segun obisesan

Similarity Index	Similarity by Source	
14%	Internet Sources:	7%
	Publications:	12%
	Student Papers:	2%

< 1% match ()
Wentzel, Alicia Veronica. "User interface design guidelines for digital television virtual remote controls", Faculty of Commerce, Information Systems, 2016

< 1% match ()
TAU, VICTORIA, GUMBO, SIBUKELE et al. "NEMISA Digital Skills Conference (Colloquium) 2023", National Electronic Media Institute of South Africa (NEMISA) and University of South Africa (UNISA), 2023

< 1% match ()
"School management teams' experiences in implementing a school feeding programme in Nigeria public primary schools", University of Pretoria, 2023

< 1% match (Internet from 12-Dec-2022)
https://ktk.pte.hu/sites/ktk.pte.hu/files/uploads/to/Pobee%20Frederick%20Okpoti_Disszert%C3%A1ci%C3%B3.pdf

< 1% match (Internet from 06-Jul-2024)
http://stmlportal.net/index.php/resource-at-stml/download/send/47-stml-go-green-2024/213-volume-1-proceeding-go-green-24

< 1% match (Internet from 06-Jul-2024)
http://stmlportal.net/index.php/resource-at-stml/download/send/47-stml-go-green-2024/214-volume-2-proceeding-go-green-24

< 1% match (Internet from 17-May-2024)
https://etd.cput.ac.za/bitstream/20.500.11838/2958/1/jideani_paul_209089067.pdf

< 1% match (Internet from 11-Jul-2024)
https://etd.cput.ac.za/bitstream/20.500.11838/4076/1/Nkandi_Zandiswa_204126827.pdf

< 1% match (Internet from 06-Oct-2022)
http://vital.seals.ac.za:8080/vital/access/services/Download/vital:44982/SOURCE1

Appendix 6: Informed consent for the quantitative phase of the Questionnaires

Dear Respondents

I am Segun M. Obisesan, a student pursuing a Master of Commerce (Information Systems) degree in the Information Systems Department at Rhodes University. My degree is by thesis and requires me to conduct empirical research in which I have to collect data from respondents. The title of my thesis is: *Using the protection motivation theory to evaluate the impact of cybersecurity practices on user experiences with e-commerce platforms in Gqeberha, Eastern Cape province.*

I am asking you to participate in this study by completing this questionnaire. There are no correct answers, therefore, use your best knowledge and first impression. Please do not write your name on this questionnaire, just sign the informed consent form before completing this questionnaire. Please note that there are NO benefits for your participation in this study and that your participation is voluntary. You can withdraw from participation any time even after completing the questionnaire without providing any explanation to the researcher. There are NO risks associated with this study as your responses with be treated with utmost confidence.

Informed consent declaration
This research has been approved by the Rhodes University Ethics Committee on this following basis that:

- I am over eighteen (18) year of age;
- I understand the purpose of the research study and my involvement in it;
- I understand that I can withdraw from the research project at any stage without asking for permission or providing any explanation to that effect;
- I understand that while information gained during this research study may be published, It will not be identified and the responses you provide will remain confidential;
- I understand that I will receive no payment for participating in this research study;
- I understand that my participation in this research study is one on a voluntary basis;

Should you require to enquire about this research you can reach my supervisor Dr Moyo at moses.moyo@ru.ac.za or 078 554 9610/078 868 4485? Your help is much highly valued.

Thank you
Segun M Obisesan

_____

I have read and understood the informed consent declaration for this research as explained above that I would NOT be paid in any form for my participation in the questionnaires and I hereby willingly consent to participate as aforesaid in the research study.

Please click the box ☐

THIS QUESTIONNAIRES CONTAINS SECTIONS

SECTION A: DEMOGRAPHIC DATA
PLEASE TICK OR CROSS THE APPROPRIATE BOXES TO INDICATE THAT YOU HAVE COMPLETED THIS SECTION.

1. **Sex:**
   - ☐ Female
   - ☐ Male

2. **Age Group:**
   - ☐ **≥** 18 years
   - ☐ 18 – 19 years
   - ☐ 20 – 30 years
   - ☐ 31 – 40 years
   - ☐ 41 – 50 years
   - ☐ Above 50

3. **Highest educational qualification:**
   - ☐ Matric
   - ☐ Diploma
   - ☐ Bachelor's Degree
   - ☐ Honour's Degree
   - ☐ Master's Degree
   - ☐ Doctorate

4. **Do you shop online in an internet café?**
   - ☐ Yes
   - ☐ No

If No, (please do not continue answering the questionnaire)

If Yes, continue answering the rest of the questionnaire

5. **How long have you been shopping online in an internet café?**
   - ☐ Less than 1 year
   - ☐ 1 – 3 years
   - ☐ 4 - 6 years
   - ☐ 7 – 10 years
   - ☐ More than 10 years

6. **How often do you use the internet café specifically for online shopping?**
   - ☐ Rarely (less than once a month)
   - ☐ Occasionally (once a month)
   - ☐ Frequently (a few times a month)
   - ☐ Very frequently (weekly or more)

7. **How many different online shopping platforms do you typically use?**
   - ☐ 1 platform
   - ☐ 2–3 platforms
   - ☐ 4–5 platforms
   - ☐ More than 5 platforms

8. **How would you rate your awareness of cybersecurity risks when shopping online**?
   - ☐ Excellent
   - ☐ Good

☐ Average
☐ Poor

9. **How would you rate your understanding of cybersecurity risks when shopping online?**
   ☐ Excellent
   ☐ Good
   ☐ Average
   ☐ Poor
10. **How would you rate your awareness of best security practices when shopping online?**
   ☐ Excellent
   ☐ Good
   ☐ Average
   ☐ Poor
11. **How would you rate your understanding of best security practices when shopping online?**
   ☐ Excellent
   ☐ Good
   ☐ Average
   ☐ Poor

SECTION B: PERCEPTIONS OF CYBERSECURITY THREATS AND RISKS WHEN SHOPPING ONLINE IN AN INTERNET CAFÉ

12. **The following statements are intended to measure your perceived cybersecurity threats and risks when shopping online. Rate each of the statement using the Likert Scale shown**

Cybersecurity risks	**Strongly Agree =5**	**Agree =4**	**Not Sure =3**	**Disagree =2**	**Strongly Disagree =1**
12.1. **I am concerned about my personal and financial information being stolen while shopping online.**	☐	☐	☐	☐	☐
12.2. **I believe cybercriminals frequently target online shopping platforms to steal customer data.**	☐	☐	☐	☐	☐
12.3. **I always worry about falling victim to phishing scams or fake shopping websites when using internet cafe facilities.**	☐	☐	☐	☐	☐
12.4. I **feel that online shopping platforms do not provide sufficient protection against cybersecurity threats.**	☐	☐	☐	☐	☐
12.5. I **am concerned that malware or spyware could compromise my accounts on the e-commerce platforms I use for online shopping.**	☐	☐	☐	☐	☐
12.6. **I believe shopping on e-commerce platforms in an internet café greatly increases cybersecurity risks.**	☐	☐	☐	☐	☐
12.7. **I believe phishing attempts such as fake emails or websites asking for personal information are a major threat when shopping online.**	☐	☐	☐	☐	☐

12.8. **I am concerned about being redirected to fraudulent or suspicious websites while making a purchase.**	☐	☐	☐	☐	☐
12.9. **I believe online shoppers are at risk of unauthorized transactions or suspicious activities on their bank or payment accounts.**	☐	☐	☐	☐	☐
12.10. **I am worried about receiving fake order confirmation emails or scam messages after shopping online.**	☐	☐	☐	☐	☐

SECTION C: AWARENESS OF BASIC CYBERSECURITY PRACTICES AND MEASURES WHEN SHOPPING ONLINE IN AN INTERNET CAFÉ

13. These statements solicit your awareness of basic cybersecurity practices needed for safe use of ecommerce platforms. Rate each on the scale shown

Cybersecurity practices	Strongly Agree =5	Agree =4	Neutral =3	Disagree =2	Strongly Disagree =1
13.1. I am aware that creating unique, complex passwords for each e-commerce account enhances security.	☐	☐	☐	☐	☐
13.2. I understand that using password managers can help securely store and generate strong passwords.	☐	☐	☐	☐	☐
13.3. I am aware that shopping on secure websites (HTTPS) reduces cybersecurity risks.	☐	☐	☐	☐	☐
13.4. I understand the risks of clicking on links in unsolicited emails or texts claiming to be from e-commerce platforms.	☐	☐	☐	☐	☐
13.5. I am aware that using reputable third-party payment processors (e.g., PayPal, Google Pay, Apple Pay) adds an extra layer of security.	☐	☐	☐	☐	☐
13.6. I am aware that regularly reviewing bank statements can help detect unauthorized charges.	☐	☐	☐	☐	☐

14. How often do you actively use the following cybersecurity measures for safe online shopping?

Cybersecurity practices/measures	Always = 5	Often = 4	Sometimes = 3	Rarely = 2	Never = 1
14.1. Creating strong and unique passwords for my shopping accounts.	☐	☐	☐	☐	☐
14.2. Enabling two-factor authentication on e-commerce platforms.	☐	☐	☐	☐	☐
14.3. Avoiding shopping on public Wi-Fi without using security measures	☐	☐	☐	☐	☐
14.4. Verifying the authenticity of e-commerce platforms before making a purchase.	☐	☐	☐	☐	☐
14.5. Using well-known e-commerce platforms for security reasons.	☐	☐	☐	☐	☐

SECTION D: PERCEIVED CYBERSECURITY PRACTICES EFFECTIVENESS

15. To what extent do you agree or disagree with the following statements about the effectiveness of cybersecurity practices and your experience when shopping on e-commerce platforms in an internet cafe?

Statement	Strongly agree = 5	Agree = 4	Neutral = 3	Disagree = 2	Strongly disagree = 1
15.1. I believe that cybersecurity practices such as strong passwords, two-factor authentication effectively reduce my risk of cybersecurity risks while shopping online.	☐	☐	☐	☐	☐
15.2. I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	☐	☐	☐	☐	☐
15.3. I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	☐	☐	☐	☐	☐
15.4. My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments	☐	☐	☐	☐	☐
15.5. I regularly check for cybersecurity updates or tips to improve my online shopping security.	☐	☐	☐	☐	☐
15.6. I avoid shopping on websites that seem untrustworthy	☐	☐	☐	☐	☐
15.7. I find it difficult to apply security measures on e-commerce platforms	☐	☐	☐	☐	☐
15.8. I limit my online shopping activities due to concerns about cybersecurity threats in an unsecured websites when using internet café	☐	☐	☐	☐	☐
15.9. Even when I know a website is secure, my concerns about cyber threats make me reconsider purchasing from an ecommerce platform when shopping online	☐	☐	☐	☐	☐

Any additional information that you think will be essential to this study could be provided:

_____

Thank you for your time dedicated to completing this questionnaire.
End of Questionnaire

Appendix 7: Informed consent for the qualitative phase of the semi-structure interview

Dear Participants

I am Segun M. Obisesan, a student pursing a Master of Commerce (Information Systems) in the Department of Information Systems at Rhodes University. My degree is by thesis which requires me to conduct an empirical research in which I have to collect data from participants. The title of my thesis is: *Using the protection motivation theory to evaluate the impact of cybersecurity practices on user experiences with e-commerce platforms in Gqeberha, Eastern Cape Province.*

This semi-structured interview is designed to solicit information about your evaluation on the impact of cybersecurity practices on user experiences within e-commerce platforms in Gqeberha, Eastern Cape. The reason for your participants is to gather your perceptions, awareness and understanding of cybersecurity threats and how basic cybersecurity measures have impacted your online shopping experiences within e-commerce platforms. I am asking you to participate in the face-to-face interview. The interview will take 15 to 30 minutes which will be conducted at your own convenient time. I would like to seek your approval for audio recording the interview conversations. You are free to provide any information that can be of help to this study during the interview and information provide will remain confidential and there is NO any risk that involved with your participation in the interview as stated in the informed consent declaration guided by Rhodes University Ethics Committee. You are free to refrain from answering questions when you feel so.

Informed consent declaration

This research has been approved by the Rhodes University Ethics Committee on this following basis that:

- I am over eighteen (18) year of age;
- I understand the purpose of the research study and my involvement in it;
- I understand that I can withdraw from the research project at any stage without asking for permission or providing any explanation to that effect;
- I understand that while information gained during this research study may be published, I will not be identified and the results I provide will remain confidential;
- I understand that I will received no payment for participating in this research study;
- I understand that my participation in this research study is done on a voluntary basis
- I agree to the researcher's request to use the voice recording of my comments and opinions during the interview only for this purpose to ensure the accurate recording of opinions/reply;
- I have the right to request a copy of the interview transcriptions to confirm that my opinions are accurately recorded;
- I understand that I have the right to request from the researcher to provide me on how my information will be stored securely and clarify precisely on the confidentiality and anonymity of my data in terms of Protection Information Act (No. 4 of 2013).

Should you require to enquire about his research you can reach my supervisor Dr Moyo at moses.moyo@ru.az.ca or 078 554 9610 /078 868 4485?

Thank you

Segun M Obisesan

_____

I have read and understood the informed declaration as explained above that I would NOT be paid in any form for my participation in this interview. I hereby willingly consent to participate as aforesaid in the research study.

Please click the box ☐

THE INTERVIEW GUIDE CONSISTS OF TWO SECTIONS

SECTION A

Welcoming and greeting of the interviewee

Explaining to the interviewee the reason for this study asking them to sign the consent forms

The researcher confirms that the informed consent for this study has been explained to the interviewee

Ensuring that an interviewee/participant is feel safe and settled

The researcher will ask for their permission to record the session

Many platforms do you shop from and your most preferably platforms

SECTION B

Research question 1	1. Tell me about your experience in using online shopping 2. What types of cybersecurity risks do you think of when you using online shopping platforms? 3. How vulnerable do you feel when entering your personal or payment information on these platforms and how serious are the consequence if there is a security breach?
Research question 2	4. What cybersecurity practices or features do you look for when shopping on an e-commerce platform to ensure your safety? 5. Have you ever encountered a security issue while shopping online? If so, how did you handle it? 6. How effective do you consider cybersecurity measures in protecting your information?
Research question 3	7. How difficult or easy is it for you to follow cybersecurity practices, such as a strong password or enabling multi-factor authentication, when shopping on e-commerce platforms? 8. How has these security practices impact your overall shopping experience?
Research question 4	9. What improvement or suggestions would you like to see or share when it comes cybersecurity practices on the e-commerce platforms to improve your shopping experience?

END OF THE INTERVIEW
THANK YOU FOR PARTICIPATION

Appendix 8: Participant Infomed Consent Declaration

(To be signed by research participant/s)

Project Title: Using the Protection Motivation Theory to Evaluate the Impact of Cybersecurity Practices on User Experiences with E-commerce Platforms in Gqeberha, Eastern Cape Province

I am Segun M Obisesan, a student pursing a Master of Commerce (Information Systems) from the Department of Information Systems, Rhodes University has requested my permission to participate in the above-mentioned research project.

The nature and the purpose of the research project and of this informed consent declaration have been explained to me in a language that I understand.

I am aware that:

1. The purpose of the research project is to use the PMT to assess the impact of cybersecurity practices on user experiences with e-commerce platforms in Gqeberha.
2. Rhodes University has given ethical clearance to this research project ***(2025-8291-9526)*** and I have seen/may request to see the clearance certificate by contacting the Ethics Coordinator (ethics-committee@ru.ac.za).
3. By participating in this research project I will be contributing towards improving cybersecurity practices and users experiences in online shopping platforms. The findings may help e-commerce platforms design effective and user-friendly security measures that can enhance online shopping experiences. It may offer valuable information on recommendation perceived cybersecurity practices and promoting safer online shopping for e-commerce users.In addition, policymakers may use the findings to develop regulations and guidelines that strengthen cybersecurity practices for users.
4. I will participate in the project by interview. This semi-structured interview is designed to solicit information about your evaluation on the impact of cybersecurity practices on user experiences within e-commerce platforms in Gqeberha, Eastern Cape. The reason for your participants is to gather your perceptions, awareness and understanding of cybersecurity threats and how basic cybersecurity measures have impacted your online shopping experiences within e-commerce platforms.
5. My participation is entirely voluntary and should I at any stage wish to withdraw from participating further, I may do so without any negative consequences.
6. I will not be compensated for participating in the research, but my out-of-pocket expenses will be reimbursed.
7. There is NO any risk that involved with your participation in the interview. You are free to refrain from answering questions when you feel so. You are free to provide any information that can be of help to this study during the interview and information provide will remain confidential. The interview will take 15 to 30 minutes which will be conducted at your own convenient time. I would like to seek your approval for audio recording the interview conversations.
8. The Researcher intends to publish the research results in the form of academic journal or conference paper and institutional report. However, confidentiality and anonymity of records will be maintained, and my name and identity will not be revealed to anyone who has not been involved in the conducting of the research, ***unless I indicate to the***

contrary/recognize that as a public figure my identity will inevitably be/become known, in which case I agree to accept the loss of anonymity.

9. In terms of the Protection of Personal Information Act (No. 4 of 2013) it remains my right to request the Researcher to provide me with a detailed explanation of exactly how confidentiality and anonymity of the data I provide will be achieved. I may also request to know exactly how my personal information will be stored securely, for how long it will be stored.
10. Data collected from me for this research project will not be used for any further study. I consent to data collected from me for this research project being used by the Researcher in a follow up study.
11. In terms of the POPI Act, I possess the right to receive feedback about this research. This will take the form of email or printed papers provided and forwarded to me unless ***I elect not to receive this feedback.***
12. Any further questions that I might have regarding the nature of the research and/or my participation in it will be answered by the researcher Segun Obisesan at q24O7469@campus.ru.ac.za or 074 354 8687 and my supervisor Dr Moyo at moses.moyo@ru.az.ca or 078 554 9610 /078 868 448
13. By signing this informed consent declaration, I am not waiving any legal claims, rights, or remedies. A copy of this informed consent declaration will be given to me, and the original will be kept on record by the Researcher.
14. I ***agree*** to the Researcher's use of voice recording of my comments and opinions during interviews, the purpose of which is to ensure the accurate recording of my views/responses. Furthermore, I have the right to request a copy of the interview transcriptions to confirm that my opinions are accurately recorded

I, ..., have read the above information / confirm that the above information has been explained to me in a language that I understand and I am aware of this document's contents. I have asked all questions that I wished to ask, and these have been answered to my satisfaction. I fully understand what is expected of me during the research.

I have not been pressurised in any way and I voluntarily agree to participate in the above-mentioned project.

.....	.....	.....
Participants signature	**Witness**	**Date**

Appendix 9: Ethical wavier for the article

RHODES UNIVERSITY
Where leaders learn

Rhodes University Human Research Ethics Committee
Room 8 & 24 Truro House, St Peters Campus
Makhanda,6139
t: +27 (0) 46 603 7314 & 8073
e: ethics-committee@ru.ac.za
https://www.ru.ac.za/researchgateway/ethics
NHREC Registration number:RC-241114-045

17 March 2025

Mr Segun Musa Obisesan

Email: g24O7469@campus.ru.ac.za

Review Reference: 2025-8291-9526

Dear Mr Obisesan,

Title: USING THE PROTECTION MOTIVATION THEORY TO EVALUATE THE IMPACT OF CYBERSECURITY PRACTICES ON USER EXPERIENCES WITH E-COMMERCE PLATFORMS IN GQEBERHA, EASTERN CAPE PROVINCE.

Researcher: Mr Segun Musa Obisesan

Supervisor(s): Dr Moses Moyo

This letter confirms that the above research proposal has been reviewed and **APPROVED** by the Rhodes University Human Research Ethics Committee (RU-HREC). Your Approval number is: 2025-8291-9526

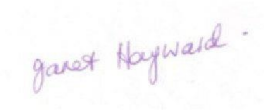
Approval has been granted for 1 year. An annual progress report will be required in order to renew approval for an additional period. You will receive an email notifying you when the annual report is due.

Please apply for a protocol amendment should any substantive change(s) be made, for whatever reason, during the research process. This includes changes in investigators. Email your request to ethics-committee@ru.ac.za.

Please submit a brief report to the ethics committee on the completion of the research. The purpose of this report is to indicate whether the research was conducted successfully, if any aspects could not be completed, or if any problems arose that the ethical standards committee should be aware of.

If a thesis or dissertation arising from this research is submitted to the library's electronic theses and dissertations (ETD) repository, please notify the committee of the date of submission and/or any reference or cataloguing number allocated.

Sincerely,



Dr Janet Hayward

Chair: Rhodes University Human Research Ethics Committee (RU-HREC)

Appendix 10: Tables referenced in chapter 5

Table AP1: Chi-square tests on demographic data on the e-commerce platform users for cybersecurity risks and cybersecurity practices

Variables		Chi-Square Tests	df	Asymptotic Significance (2-sided)
Gender	Awareness of best security practices when shopping online	2.716[a]	3	.438
	Understanding of best security practices when shopping online	2.454[a]	3	.484
	Awareness of cybersecurity risks when shopping online	2.734[a]	3	.434
	Understanding of cybersecurity risks when shopping online	.245[a]	3	.970
Age	Awareness of cybersecurity risks when shopping online	12.974[a]	12	.371
	Understanding of cybersecurity risks when shopping online	15.562[a]	12	.212
	Awareness of best security practices when shopping online	12.679[a]	12	.393
	Understanding of best security practices when shopping online	18.246[a]	12	.108
Education	Awareness of cybersecurity risks when shopping online	3.963[a]	12	.984
	Understanding of cybersecurity risks when shopping online	6.464[a]	12	.891
	Awareness of best security practices when shopping online	4.658[a]	12	.968
	Understanding of best security practices when shopping online	7.665[a]	12	.811
Online Shopping Experience	Awareness of cybersecurity risks when shopping online	13.042[a]	12	.366
	Understanding of cybersecurity risks when shopping online	10.671[a]	12	.557
	Awareness of best security practices when shopping online	16.633[a]	12	.164
	Understanding of best security practices when shopping online	12.518[a]	12	.405
Shopping Frequency	Awareness of cybersecurity risks when shopping online	18.150[a]	9	.033
	Understanding of cybersecurity risks when shopping online	11.253[a]	9	.259
	Awareness of best security practices when shopping online	14.730[a]	9	.099
	Understanding of best security practices when shopping online	4.813[a]	9	.850

Table AP2: Spearman Correlation for knowledge and understanding of best security practices and adoption of cybersecurity practices

Variables	R	n	p-value	comment	%
Awareness of best security practices when shopping online					
Awareness of best security practices when shopping & Understanding of best security practices when shopping online	0.770**	90	0,000	Strongly associated	100,00%
Awareness of best security practices when shopping online & I feel that online shopping platforms do not provide sufficient protection against cybersecurity threats	0.227*	90	0,031	weak correlation	96,90%
Awareness of best security practices when shopping online & creating strong and unique passwords for my shopping accounts	0.280**	90	0,008	Weak correlation	99,24%
Awareness of best security practices when shopping online & I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	0.282**	90	0,007	Weak correlation	99,28%
Awareness of best security practices when shopping online & I regularly check for cybersecurity updates or tips to improve my online shopping security	0.305**	90	0,003	Weak correlation	99,65%
Understanding of best security practices when shopping online					
Understanding of best security practices when shopping online & I feel that online shopping platforms do not provide sufficient protection against cybersecurity threats	0.240*	90	0,023	weak correlation	97,75%

Understanding of best security practices when shopping online & I am worried about receiving fake order confirmation emails or scam messages after shopping online	0.233*	90	0,027	weak correlation	97,27%
Understanding of best security practices when shopping online & creating strong and unique passwords for my shopping accounts	0.261*	90	0,013	Weak correlation	98,70%
Understanding of best security practices when shopping online & verifying the authenticity of e-commerce platforms before making a purchase	0.227*	90	0,031	Weak correlation	96,87%
Understanding of best security practices when shopping online & I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	0.372**	90	0,01	Weak correlation	99,00%
Understanding of best security practices when shopping online & I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	0.239*	90	0,023	Weak correlation	97,65%
Understanding of best security practices when shopping online & I regularly check for cybersecurity updates or tips to improve my online shopping security	0.282**	90	0,007	Weak correlation	99,30%
Understanding of best security practices when shopping online & I avoid shopping on websites that seem untrustworthy	0.209*	90	0,048	Weak correlation	95,18%

**. Correlation is significant at the 0.01 level (2-tailed). *. Correlation is significant at the 0.05 level (2-tailed).

Table AP3: Spearman correlation for awareness and understanding of cybersecurity risks and adoption of cybersecurity practices

Variables	r	n	p-value	comment	%
Awareness of cybersecurity risk when shopping online					
Awareness of cybersecurity risks when shopping online & understanding of cybersecurity risks when shopping online	0.712**	90	0,000	Strongly associated	100,00%
Awareness of cybersecurity risks when shopping online & I feel that online shopping platforms do not provide sufficient protection against cybersecurity threats	0.209*	90	0,049	weak correlation	95,15%
Awareness of cybersecurity risks when shopping online & enabling two-factor authentication on e-commerce platforms	0.304**	90	0,004	weak correlation	99,64%
Awareness of cybersecurity risks when shopping online & I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	0.227*	90	0,031	weak correlation	96,86%
Awareness of cybersecurity risks when shopping online & I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	0.221*	90	0,037	weak correlation	96,34%
Understanding of cybersecurity risks when shopping online					
Understanding of cybersecurity risks when shopping online & I am aware that shopping on secure websites (HTTPS) reduces cybersecurity risks	.240*	90	0,023	Weak correlation	97,74%
Understanding of cybersecurity risks when shopping online & creating strong and unique passwords for my shopping accounts	.339**	90	0,001	Weak correlation	99,89%
Understanding of cybersecurity risks when shopping online & enabling two-factor authentication on e-commerce platforms	.331**	90	0,001	Weak correlation	99,86%
Understanding of cybersecurity risks when shopping online & I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web	.226*	90	0,032	Weak correlation	96,80%
Understanding of cybersecurity risks when shopping online & I regularly check for cybersecurity updates or tips to improve my online shopping security	.256*	90	0,015	Weak correlation	98,52%

**. Correlation is significant at the 0.01 level (2-tailed). *. Correlation is significant at the 0.05 level (2-tailed).

Table AP4: Chi-square test about age and shopping frequency for e-commerce platform users

Age and Shopping Frequency for e-commerce platform users							
			Very frequently	**Frequently**	**Occasionally**	**Rarely**	**Total**
Age	**50+**	Count	1	1	1	3	6
		Expected Count	1.0	1.1	1.1	2.9	6.0
		% within Age	16.7%	16.7%	16.7%	50.0%	100.0%
		% within Shopping Frequency	6.7%	6.3%	6.3%	7.0%	6.7%
		% of Total	1.1%	1.1%	1.1%	3.3%	6.7%
	41-50	Count	3	2	2	5	12
		Expected Count	2.0	2.1	2.1	5.7	12.0
		% within Age	25.0%	16.7%	16.7%	41.7%	100.0%
		% within Shopping Frequency	20.0%	12.5%	12.5%	11.6%	13.3%
		% of Total	3.3%	2.2%	2.2%	5.6%	13.3%
	31-40	Count	7	6	6	11	30
		Expected Count	5.0	5.3	5.3	14.3	30.0
		% within Age	23.3%	20.0%	20.0%	36.7%	100.0%
		% within Shopping Frequency	46.7%	37.5%	37.5%	25.6%	33.3%
		% of Total	7.8%	6.7%	6.7%	12.2%	33.3%
	20-30	Count	4	7	6	23	40
		Expected Count	6.7	7.1	7.1	19.1	40.0
		% within Age	10.0%	17.5%	15.0%	57.5%	100.0%
		% within Shopping Frequency	26.7%	43.8%	37.5%	53.5%	44.4%
		% of Total	4.4%	7.8%	6.7%	25.6%	44.4%
	18-19	Count	0	0	1	1	2
		Expected Count	.3	.4	.4	1.0	2.0
		% within Age	0.0%	0.0%	50.0%	50.0%	100.0%
		% within Shopping Frequency	0.0%	0.0%	6.3%	2.3%	2.2%
		% of Total	0.0%	0.0%	1.1%	1.1%	2.2%
Total		Count	15	16	16	43	90
		Expected Count	15.0	16.0	16.0	43.0	90.0
		% within Age	16.7%	17.8%	17.8%	47.8%	100.0%
		% within Shopping Frequency	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	16.7%	17.8%	17.8%	47.8%	100.0%

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.259[a]	12	.902
Likelihood Ratio	6.610	12	.882
Linear-by-Linear Association	1.757	1	.185
N of Valid Cases	90		
a. 11 cells (55.0%) have expected count less than 5. The minimum expected count is .33.			

Table AP5: Chi-square test about gender and shopping frequency for e-commerce platform users

Gender and Shopping Frequency for e-commerce platform users							
			Very frequently	**Frequently**	**Occasionally**	**Rarely**	**Total**
Gender	**Male**	**Count**	13	7	6	23	49
		Expected Count	8.2	8.7	8.7	23.4	49.0
		% within Sex	26.5%	14.3%	12.2%	46.9%	100.0%
		% within Shopping Frequency	86.7%	43.8%	37.5%	53.5%	54.4%
		% of Total	14.4%	7.8%	6.7%	25.6%	54.4%
	Female	**Count**	2	9	10	20	41
		Expected Count	6.8	7.3	7.3	19.6	41.0
		% within Sex	4.9%	22.0%	24.4%	48.8%	100.0%
		% within Shopping Frequency	13.3%	56.3%	62.5%	46.5%	45.6%
		% of Total	2.2%	10.0%	11.1%	22.2%	45.6%
Total		**Count**	15	16	16	43	90
		Expected Count	15.0	16.0	16.0	43.0	90.0
		% within Sex	16.7%	17.8%	17.8%	47.8%	100.0%
		% within Shopping Frequency	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	16.7%	17.8%	17.8%	47.8%	100.0%

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.885[a]	3	.031
Likelihood Ratio	9.773	3	.021
Linear-by-Linear Association	2.347	1	.125
N of Valid Cases	90		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.83.			

Table AP6: Spearman correlation between e-commerce platform users' perceived cyber threats and the effectiveness of cybersecurity practices

Variables	**r**	**n**	**p-value**	**comments**
I believe that cybersecurity practices such as strong passwords, two-factor authentication effectively reduce my risk of cybersecurity risks while shopping online & I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	.260*	90	0,013	Weak correlation
I believe that cybersecurity practices such as strong passwords, two-factor authentication effectively reduce my risk of cybersecurity risks while shopping online & I regularly check for cybersecurity updates or tips to improve my online shopping security	.226*	90	0,032	Weak correlation
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web & I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security	.471**	90	0,000	Moderate correlation
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web & My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments	.217*	90	0,039	Weak correlation
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web & I regularly check for cybersecurity updates or tips to improve my online shopping security	.378**	90	0,000	Moderate correlation

Variables	r	n	p-value	comments
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web & I avoid shopping on websites that seem untrustworthy	.225*	90	0,033	Weak correlation
I check for security indicators such as padlock icon and SSL certificate before making a purchase on an ecommerce platform on the web & I limit my online shopping activities due to concerns about cybersecurity threats in an unsecured websites when using internet café	.240*	90	0,023	Weak correlation
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security & I believe that cybersecurity practices such as strong passwords, two-factor authentication effectively reduce my risk of cybersecurity risks while shopping online	.260*	90	0,013	Weak correlation
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security & My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments	.246*	90	0,020	Weak correlation
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security & I regularly check for cybersecurity updates or tips to improve my online shopping security	.479**	90	0,000	Moderate correlation
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security & I limit my online shopping activities due to concerns about cybersecurity threats in an unsecured websites when using internet café	.305**	90	0,003	Moderate correlation
I regularly update my passwords, and enable two-factor authentication for online shopping accounts to enhance security & Even when I know a website is secure, my concerns about cyber threats make me reconsider purchasing from an ecommerce platform when shopping online	.330**	90	0,001	Moderate correlation
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments & I regularly check for cybersecurity updates or tips to improve my online shopping security	.452**	90	0,000	Moderate correlation
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments & I avoid shopping on websites that seem untrustworthy	.379**	90	0,000	Moderate correlation
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments & I find it difficult to apply security measures on e-commerce platforms	.293**	90	0,005	Weak correlation
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments & I limit my online shopping activities due to concerns about cybersecurity threats in an unsecured websites when using internet café	.273**	90	0,009	Weak correlation
My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments & Even when I know a website is secure, my concerns about cyber threats make me reconsider purchasing from an ecommerce platform when shopping	.435**	90	0,000	Moderate correlation
I regularly check for cybersecurity updates or tips to improve my online shopping security & My fear of cybersecurity threats (e.g. phishing, fraud, data breaches) influence my decision to use extra security measures when shopping online or making online payments	.452**	90	0,000	Moderate correlation
I regularly check for cybersecurity updates or tips to improve my online shopping security & I find it difficult to apply security measures on e-commerce platforms	.219*	90	0,038	Weak correlation
I regularly check for cybersecurity updates or tips to improve my online shopping security & Even when I know a website is secure, my concerns about cyber threats make me reconsider purchasing from an ecommerce platform when shopping online	.358**	90	0,001	Moderate correlation

**. Correlation is significant at the 0.01 (2-tailed).*. Correlation is significant at the 0.05 level (2-tailed).