

https://dspace.org/

Exploring the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa

Lebogo, Grace Tsholofelo

2023
https://hdl.handle.net/10539/37215

Downloaded from a DSpace repository. https://dspace.org/

Exploring the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa

Grace Tsholofelo Lebogo

Supervisor Name: Dr Kiru Pillay

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

Johannesburg, 2021

ABSTRACT

This study explored the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa. Given the rise of cybercrime worldwide, consumers are cautious of using e-commerce platforms. This research aimed to understand the extent to which cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms, and how cybersecurity awareness programmes influence e-commerce consumer confidence. A quantitative method was followed to obtain the results where a structured survey was distributed on social media platforms, WhatsApp messaging platform, and via email, by requesting respondents to answer questions on the following variables: Cybersecurity awareness programmes, Consumer confidence: Motivation, and Consumer confidence: Security and Privacy. There was a total of 297 responses collected for this study, of which only 250 (84%) met the inclusion criteria. The results indicate that consumers are influenced by cybersecurity awareness programmes to shop more on these platforms and this is done by communicating with consumers by displaying messages on the platforms and sending messages to e-commerce consumers to increase their cybersecurity awareness levels and confidence.

KEY WORDS

Cybersecurity awareness programmes, consumer confidence, e-commerce platforms, security and privacy

DECLARATION

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

Name: Grace Tsholofelo Lebogo Signature: Gtlebogo

Signed at Centurion

On the 31st day of October 2022

DEDICATION

I thank God for reaching this point when faced with so many obstacles. This research report is dedicated to my mother who has been my pillar of strength. You have mentored me through my difficult academic journey and have sacrificed a lot to ensure that I press on even when I felt that I could not continue. I am eternally grateful that God chose you as my mother. To my two beautiful children, and husband you have endured the most during this journey. I also wish to acknowledge you and appreciate all the encouragement and sacrifices you have made to ensure that I succeed. To my supervisor, Dr Kiru Pillay, this journey has been a daunting one, especially because it was virtual and I could not meet you in person. Thank you for your special contribution. This research report would never have been possible without your guidance and support. Thank you for the patience and time you have afforded me. To my good friends Nonkosi and Dineo, your encouragement and constant phone calls to let me know that everything will work out carried me through. To my employer, the Road Accident Fund, thank you for the sponsorship. “I am because of you.” To all the respondents and those that ensured that they sent my survey out, thank you. This report was possible because of you.

Table of Contents

CHAPTER 1. INTRODUCTION 11

1.1 CONTEXT OF THE STUDY 11
1.2 BACKGROUND OF THE STUDY 11
1.3 RESEARCH PROBLEM 14
1.4 RESEARCH QUESTIONS 15
1.5 SIGNIFICANCE OF THE STUDY 15
1.6 DELIMITATION OF THE STUDY 17
1.7 ASSSUMPTIONS 18

CHAPTER 2. LITERATURE REVIEW 19

2.1 INTRODUCTION 19
2.2 DEFINITIONS 19
2.2.1 E-COMMERCE 19
2.2.2 TRUST, CONFIDENCE AND AWARENESS 20
2.3 THEORETICAL FOUNDATION OF THE STUDY 22
2.3.1 AWARENESS PROGRAMMES 25
2.3.2 MOTIVATION 27
2.3.3 ISSUES OF PRIVACY 28
2.3.4 CONCEPTUAL FRAMEWORK 29
2.3.5 DEFINITION OF HYPOTHESES 30
2.4 CONCLUSION OF LITERATURE REVIEW 31

CHAPTER 3. RESEARCH METHODOLOGY 32

3.1 RESEARCH APPROACH 32
3.2 RESEARCH DESIGN 32
3.3 POPULATION AND SAMPLING 33
3.3.1 POPULATION 33
3.3.2 SAMPLING 34
3.4 DATA COLLECTION METHODS 35
3.4.1 PILOT STUDY 35
3.5 RESEARCH INSTRUMENT 37
3.6 DATA ANALYSIS 38
3.7 VALIDITY AND RELIABILITY 39
3.7.1 VALIDITY 39
3.7.2 EXTERNAL VALIDITY 39
3.7.3 RELIABILITY 40
3.8 LIMITATIONS 41
3.9 ETHICAL CONSIDERATIONS 41

CHAPTER 4. PRESENTATION OF RESULTS 43

4.1 INTRODUCTION 43
4.2 THE SAMPLE 44
4.2.1 RELIABILITY STATISTICS 44
4.3 FACTOR ANALYSIS 45
4.4 SECTION ANALYSIS 45
4.4.1 RESULTS PERTAINING TO HYPOTHESIS 1 45
4.4.2 RESULTS PERTAINING TO HYPOTHESIS 2 48
4.4.3 CONSUMER CONFIDENCE: MOTIVATION 48
4.4.4 CONSUMER CONFIDENCE: SECURITY & PRIVACY 51
4.5 CROSS-TABULATIONS 53
4.6 CORRELATIONS 63
4.7 STRUCTURAL EQUATION MODEL 64
4.8 RESULT (DEFAULT MODEL) 65
4.9 CONCLUSION 69

CHAPTER 5. DISCUSSION OF RESULTS 71

5.1 INTRODUCTION 71
5.2 INCLUSION CRITERIA 72
5.3 DISCUSSION PERTAINING TO H1 72
5.4 DISCUSSION PERTAINING TO H2 76
5.4.1 CONSUMER CONFIDENCE: SECURITY & PRIVACY 80
5.5 CONCLUSION 82

CHAPTER 6. Conclusions & Recommendations 84

6.1 INTRODUCTION 84
6.2 DEDUCTIONS 84
6.2.1 CONCLUSIONS REGARDING HYPOTHESIS 1 85
6.2.2 CONCLUSIONS REGARDING HYPOTHESIS 2 86
6.3 RESEARCH QUESTIONS 88
6.4 RECOMMENDATIONS 91
6.5 SUGGESTIONS FOR FURTHER RESEARCH 93
6.6 CONCLUSION 93

APPENDIX A: RESEARCH INSTRUMENT 102

APPENDIX B: CORRELATIONS 110

APPENDIX C: CROSSTABULATIONS 114

APPENDIX D: RELIABILITIES 274

APPENDIX E: ETHICS CERTIFICATE 287

LIST OF TABLES

Table 1: Definition of Terms 17

Table 2: Cronbach Alpha Scores..... 44

Table 3: KMO and Bartlett's Test 45

Table 4: Scale items for cybersecurity awareness programmes questions from respondents (%) 47

Table 5: Scale items for consumer confidence: Motivation questions from respondents (%) 50

Table 6: Scale items for consumer confidence: Security & privacy questions from respondents (%) 52

Table 7: P-Value Analysis 1 54

Table 8: P-Value Analysis 2 55

Table 9: P-Value Analysis 3 57

Table 10: P-Value Analysis 4 58

Table 11: P-Value Analysis 5 59

Table 12: P-Value Analysis 6 60

Table 13: P-Value Analysis 7 61

Table 14: Relationship analysis between variables 62

Table 15: Regression Weights (Group number 1 – Default Model) 65

Table 16: Standardised Regression Weights (Group number 1 – Default model) 66

Table 17: CMIN 66

Table 18: Baseline Comparisons..... 67

Table 19: RMSEA..... 67

Table 20: Covariance's (Group number – Default Model) 68

Table 21: Correlations (Group number 1 – Default Model)..... 68

Table 22: H1 correlations 75

Table 23: H2 correlations 79

LIST OF FIGURES

Figure 1: FNB Cybersecurity Awareness Programme**Error! Bookmark not defined.**

Figure 2: Conceptual Model 29

Figure 3: cybersecurity awareness programmes responses bar chart 48

Figure 4: consumer confidence: Motivation bar chart..... 51

Figure 5: consumer confidence: Security & privacy Bar Chart 53

Figure 7: SEM DIAGRAM..... 64

LIST OF ACRONYMS

BRICS – Brazil, Russia, India, China & South Africa (economic grouping of emerging economies)

COVID 19 – Coronavirus Disease

CSA – Cybersecurity Awareness

EFA - Exploratory factor analysis

FNB – First National Bank

PMT – Protection Motivation Theory

P-Value – Probability value

PII - Personal identifiable information

RMSEA - Root Mean Square Error of Approximation

SPSS- Statistical package for social sciences

SEM – Structural equation model

TPB – Theory of planned behaviour

SEM – Structural equation model

CHAPTER 1. INTRODUCTION

1.1 CONTEXT OF THE STUDY

This research paper focuses on exploring the role of cybersecurity awareness programmes in building consumer confidence in South Africa when transacting on e-commerce platforms. Cybersecurity awareness programmes in the context of this study refers to programmes that are specifically designed to educate and inform users on the dangers of, and appropriate behaviours and practices to adopt when transacting on e-commerce platforms.

PURPOSE OF THE STUDY

The purpose of this study is to explore whether cybersecurity awareness programmes build consumer confidence in the use of e-commerce platforms in South Africa.

1.2 BACKGROUND OF THE STUDY

Many organisations have an online presence, which enables the provision of goods and services to consumers. E-commerce is one of the means by which organisations provide goods and services to their clients and has become the new normal for many consumers. According to Gupta (2014), e-commerce is the creation of value through transactions between organisations and between organisations and their customers through electronic communication channels and the use of digital information. Dan (2014) defines e-commerce as buying and selling of services as well as goods using telecommunication devices or mobile devices with internet access to conclude transactions up to the receiving of goods and services.

Privacy and security while using e-commerce websites are key issues, which must be addressed. Bandara et al. (2020) State that with the surge of data breaches, which are continually being reported and continued difficulty in privacy management, consumers have become very distrustful.

Janakiraman et al. (2018) State that consumers place their trust in ecommerce websites when using their platforms and expect cybersecurity to be the responsibility of the e-commerce platform owners. It is imperative for consumers to trust the websites of the organisations that provide goods and services to them. Security and trust are among the factors that are limitations for e-commerce, especially where financial transactions are concerned, and both are essential factors that influence consumers' intentions to make purchases (Abbad et al., 2011; Yaseen et al., 2017). Other factors, such as privacy, are also affected by the consumer's trust in e-commerce. Another study by Corbitt et al. (2003) found that the higher the degree of trust a person has in e-commerce the more likely they are to participate in e-commerce by making purchases. Corbitt et al. (2003) Further state that the trustworthiness of the technology used to support e-commerce transactions plays an important role in the trust levels of consumers. The more they rely on the services that are provided by an online platform, the more trust they have.

Therefore, e-commerce websites must ensure their customer's information security and privacy to gain their trust (Girsang et al., 2020). However, in the context of e-commerce platforms, they have had many challenges including identity theft resulting from the failure to protect confidential information, cyber distortion, social engineering and malware attacks but have become more stable in the recent past (Khan, 2019). Cybercrime is the major obstacle that e-

commerce organisations need to combat. According to a study done by Gupta and Agarwal (2017), South Africa is among the BRICS (the geo-political grouping consisting of Brazil, Russia, India, China and South Africa) countries with the highest cybersecurity incidents. This may be attributed to a lack of awareness of cyber threats. South Africans are participating in e-commerce with limited to no knowledge of the eminent threats that exist when transacting therefore making them prone to cybercrimes including, as mentioned previously, identity theft, cyber distortion, social engineering and malware attacks.

Awareness equally plays a major role from a consumer perspective and should subsequently be given the necessary attention. Cybersecurity awareness programmes have a vital role to play in educating users on the dangers of using the internet and instilling good practices. Cybersecurity is not just about technology, but also about building the necessary awareness with individuals in cyberspace.

According to Mcanyana et al. (2020), there is a lack of awareness of cyber threats in South Africa, which has also been attributed to the low levels of technical know-how by South African users who have limited to no experience of cybersecurity as opposed to users in other parts of the world.

The rationale for this study is to explore whether cybersecurity awareness programmes build consumer confidence in the use of e-commerce platforms in South Africa.

1.3 RESEARCH PROBLEM

Cyber-attacks that target consumers of e-commerce platforms, e.g. identity theft, cyber distortion, social engineering and malware attacks are detrimental to the sustainability of this type of trade and to the South African economy as a whole. Furthermore, issues of privacy have become a major concern for consumers, with many being wary of disclosing their personal identifiable information (PII) due to the fear that it may be used falsely. Therefore, many are subsequently not willing to participate in activities which require them to disclose their PII (Van Bavel et al., 2019). Malapane (2019) states that the decision-making process of consumers is affected by trust issues that emanate online.

Human beings remain the weakest link where cybersecurity is concerned with a study by Deloitte (2015) noting a growing number of breaches against consumers. Consumer awareness of security measures, which offer protection when transacting on e-commerce platforms, is necessary in order to build trust and confidence when transacting on these platforms. Consumer trust is still one of the many factors, which prevent consumers from participating in e-commerce. Yaseen et al. (2017). Therefore the need for cybersecurity awareness programs is necessary to build consumer trust in order to mitigate the threats which come with using e-commerce platforms in order to equip consumers with the necessary know-how when using e-commerce platforms, with Yaseen et al. (2017) arguing in favour of educational programmes on how to safely use e-commerce platforms. This study explores whether cybersecurity awareness programmes build consumer confidence in the use of e-commerce platforms in South Africa.

1.4 RESEARCH QUESTIONS

The primary research question posed is: To what extent does cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms?

Emanating from the main research question, the following sub-question emerged:

1. *How do cybersecurity awareness programs aimed at consumers influence their confidence to make purchases on e-commerce platforms?*

1.5 SIGNIFICANCE OF THE STUDY

The number of internet users in South Africa is increasing by the day. Faced by the COVID-19 pandemic, consumer adoption of e-commerce subsequently surged. Organisations have also moved their focus to providing their services to clients digitally due to the convenience of facilitating financial transactions and shopping for goods and services online (Munjal, 2016). Consumers, now more than ever, are relying on online platforms to make purchases and access services. However, not all of them are aware of the dangers associated with using these platforms. Consumers should be confident when participating in e-commerce in order for them to keep on wanting to use these platforms. Cybersecurity awareness programmes play a pivotal role in influencing the behaviour and decisions of users on the internet, which includes consumers of e-commerce platforms (Hueca et al., 2020).

Bada et al. (2019) State that awareness programmes are about how consumers behave online, in line with their perceived level of risk. (Muhirwe and White, 2016)

state that the goal of awareness is to change behaviour, which in relation to this study is key to understanding whether awareness programmes build consumer confidence from a behavioural point of view. Pratt et al. (2010) indicate that when consumers spend more time shopping online it becomes a routine, which makes them prone to cybercrimes such as the interception of data, illegal interference with data or software programmes, illegal access to data, etc. (Government, 2021)

This study focuses on exploring whether cybersecurity awareness programmes build consumer confidence when using e-commerce platforms. This study will assist business owners of e-commerce platforms to understand what is required in order to increase consumer confidence through cybersecurity awareness programmes in response to the surge in cyber-attacks, which may have dire consequences for their business enterprises. Additionally the following practical application may be made from this study:

a) Provide a view of consumer confidence instilled by cybersecurity awareness programmes; and
b) This research will provide insights into what makes consumers feel more confident when transacting on e-commerce platforms.

1.6 DELIMITATION OF THE STUDY

This study is delimited to South African e-commerce consumers in the Gauteng Province. This was done due to the researcher mainly having access to an audience in the Gauteng Province within the allocated time frame of the research project. Cybersecurity awareness programmes from an e-commerce platform point of view is the focus of this study.

This study excludes platform owners. Cybersecurity awareness programmes for employees and other parties are excluded from this study.

Table 1: Definition of Terms

Term	**Definition**
Cyber-attack	Unwanted actions, which do not adhere to security protocols, which in turn compromise the confidentiality, integrity and availability of resources over a network. (Singh and Silakari, 2009)
Cyberspace	The combination of networks, hardware, software, data and other ICT tools, which enable a variety of activities that were traditional in in an online format. (Ning et al., 2018)
Cybersecurity	A well-organised collection of resources, infrastructure and processes combined to protect systems, which interact with cyberspace from unwanted activities. (Craigen et al., 2014)
Cyber security awareness	Key processes, control measures and technological measures aimed at the protection of an organisation's information systems and data assets (Mashiane et al., 2019)

e-commerce consumer	A consumer of goods and or services over a network
e-commerce	The buying and selling of goods via transactions facilitated and concluded on the internet using telecommunications tools (Dan, 2014)
e-commerce platform	A trading platform which operates over a network using information communication technology resources (Bakar et al., 2013)

1.7 ASSSUMPTIONS

The following assumptions underpin this study:

- Cybersecurity awareness programmes train consumers on how to protect themselves on e-commerce platforms;
- Some level of education is required for e-commerce consumers to understand cybersecurity awareness programmes;
- To participate in e-commerce, participants must have a source of income or receive funds from somewhere;
- Confidence is a state of mind instilled in e-commerce consumers via cybersecurity awareness programmes;
- Cybersecurity awareness is the responsibility of the e-commerce consumer;
- Respondents will answer all questions posed in the survey; and
- Respondents will complete the survey.

CHAPTER 2. LITERATURE REVIEW

2.1 INTRODUCTION

The purpose of this chapter is to provide a literature review by firstly providing definitions relevant to the study for understanding of key concepts referred to in this paper. The second part of this chapter will look at the theoretical framework underpinning this study, motivation, cybersecurity awareness programmes, consumer confidence, and security and privacy.

2.2 DEFINITIONS

2.2.1 E-COMMERCE

Dan (2014) defines e-commerce as the buying and selling of goods via transactions facilitated and concluded on the internet using telecommunications tools. Kwilinski et al. (2019) define e-commerce as the application and use of technology over a network for economic activity participation, which provides a significant competitive advantage to the user due to the popularity of conducting business in an electronic manner. Gupta (2014), while maintaining a similar definition as Dan (2014), defines e-commerce as the buying and selling of goods and services using an electronic medium, and clearly differentiates between types of e-commerce, namely. business to business (b2b), business to consumer (b2c), consumer to consumer (c2c), business to government (b2g) and mobile commerce. For the purpose of this study, e-commerce is defined as the use of any technology-enabled device, which is connected to the internet for the purchase of goods and services.

2.2.2 TRUST, CONFIDENCE AND AWARENESS

Cybersecurity awareness is the conscious awareness that an individual has about cyber threats which, from a point of knowledgeability, becomes the first line of defence in mitigating the possible exposure to looming threats in cyberspace (Dlamini and Modise, 2013). With the advancement of e-commerce and the risks that come with this medium, it becomes imperative for consumers to be alert while shopping online. Thus, the awareness of e-commerce consumers is imperative.

Khan et al. (2016) State that although awareness is important, one of the challenges of e-commerce (besides security) is the actual awareness of e-commerce in developing countries for people living in rural areas. While this is a key challenge, the introduction of security awareness programmes could be extended to these communities to ensure better preparedness once e-commerce becomes adopted. Hueca et al. (2020) State that a cybersecurity awareness programme informs users of what is expected from them. Smith (2004) states that in order to restore consumer confidence, e-commerce platforms must take the necessary steps to combat cybercrime to reduce the impact it has on business and its consumers. Consumers constantly run the risk of having their confidential information compromised by participating in e-commerce. A lack of awareness of threats that are eminent in cyberspace makes users ignorant of the threats that are present, thus making them easy targets (Kortjan and Von Solms, 2014). Zwilling et al. (2020) define cybersecurity awareness by characterizing it as three different levels of awareness behaviours, i.e. low awareness, medium awareness and high awareness. Low awareness is typically being completely negligent in terms of threats, even when provided with alerts of possible dangers

on networked devices. Medium awareness is defined as not using networked technology devices appropriately, and high awareness as having the knowledge and technical abilities to use technology-enabled devices on a network and having knowledge about cyber threats and the necessary precautions to take in order to stay safe. To understand the level of awareness of e-commerce consumers, the definitions by Zwilling et al. (2020) will be adopted for the purpose of this study.

Consumer confidence is the trust that a consumer has when using a platform to the extent that they feel that their data is safe and they will experience no negative effects from using the particular e-commerce platform. Falahat et al. (2019) state that trust plays a significant role in influencing consumer behaviour when transacting on e-commerce platforms and is used by consumers trying to reduce their levels of uncertainty when transacting in this manner. Their intention to purchase goods on e-commerce platforms and ensuring that their data is secure will be positively or negatively influenced by their confidence. Corbitt et al. (2003) State that trust is an important prerequisite that informs consumers' purchase decisions in e-commerce. According to these authors, successful e-commerce websites are those that ensure that they elicit the consumer's trust through constant communication and marketing, while subsequently ensuring that they lower any existing perceptions of associated risk. South African consumers are no exception to this, e-commerce platform owners must gain their trust in order to ensure their safety and continual participation, however the deployment of cybersecurity awareness programs on e-commerce platform has a bearing on their trust and confidence.

Cybersecurity awareness programmes may play a part in influencing the consumers' confidence as they transact on e-commerce platforms based on what the programme covers. When consumers are of the view that the e-commerce platform takes their safety and privacy seriously, especially where PII is concerned, their confidence is said to increase according to a study by (Lu, 2009). For the purpose of this study, consumer confidence is derived from the trust that a consumer has when engaging on an e-commerce platform.

2.3 THEORETICAL FOUNDATION OF THE STUDY

This study adopted the protection motivation theory (PMT), which was developed by Rogers (1975) to predict and formalise the understanding of fear appraisals in health behaviour, and specifically the probability of threat occurrence and the effectiveness of coping mechanisms adopted. This theory is also about the cognitive process used by individuals based on what influences they have been exposed to, to behave in a certain manner. Van Bavel et al. (2019) state that individuals, when faced with a threat, use a coping appraisal to understand whether reacting in a certain manner by means of taking an appropriate action will assist them to mitigate the effects of the threat, or not. In the context of this study, cybersecurity awareness programmes are used to educate e-commerce consumers on the behaviours that are required for them to safeguard their data while transacting on e-commerce platforms. Due to cybersecurity awareness programmes being aimed at assisting with changing the consumer's behaviour when transacting on these platforms, Van Bavel et al. (2019) found that where the PMT was applied, users who had received a coping message behaved more securely online. When consumers plan to purchase goods and or services on particular platforms, their PII is requested which poses both a security and privacy

threat. Therefore, the exposure of cybersecurity awareness programmes to consumers could be used as a mechanism of influence to behave in a particular manner whereas some could argue that it is dependent on how and when the user is exposed to these programmes.

This study also adopted the theory of planned behaviour (TPB) developed by Ajezen (1991), which was refined in 1987 and focuses on the intention to perform certain behaviours in human beings.

Both of these theories focus on the factors which motivate behaviour, the likelihood of the behaviour taking place, and what motivates the consumer to behave in a particular manner. An important aspect of human behaviour is the manner in which the person regulates him- or herself. Cybersecurity awareness programmes are used to educate e-commerce consumers on the behaviours required for them to safeguard their data while transacting on e-commerce platforms. This study proposes the following hypothesis:

- Cybersecurity awareness programmes positively influence consumer confidence when transacting on e-commerce platforms; and
- Cybersecurity programmes motivate e-commerce consumers to transact cautiously in order to enhance their security and privacy, which both increase consumer confidence.

Cybersecurity awareness programmes motivate the behavioural intention of an individual and is the combination of their perceived behavioural control and the intention thereof.

Bakar et al. (2013) state that consumer behaviour should be of a responsible and secure nature, which demonstrates that they are knowledgeable about their role

while participating in e-commerce. For the purpose of this study, when consumers transact on e-commerce platforms with responsibility when having been made aware of the threat landscape via awareness programmes, confidence is demonstrated. Gundu et al. (2019) State that awareness programmes may be used to improve security knowledge, which may be used by consumers.

Chandarman and Van Niekerk (2017) have also used the TPB in their study, which focused on students' cybersecurity, and again by Gurung et al. (2008) where the privacy perceptions of e-commerce consumers, as well as their awareness levels were studied to predict behavioural intention using a set of defined variables. In the context of this study the Theory of planned behaviour is adopted because security awareness programs are about changing consumer behaviour when transacting online. Consumers are influenced to behave in a much safer manner due to the exposure to cybersecurity awareness programmes therefore influencing informed behaviour when transacting online. The PMT was used to understand the cognitive process that users employ when engaging in online channels where their PII is required. As part of this study an experiment proved that users who had received a coping message behaved more securely online than those who did not (van Bavel et al., 2019).

The theories underpinning this study are focused on the motivation to behave in a certain manner. Burns and Roberts (2013) Further state that the TPB focuses on intention, which includes the motivation to act in a particular manner, while the PMT focuses on what influences the behaviour. This applies to consumers of e-commerce platforms where their intention is to make a purchase on a particular

platform and there is a need to behave securely. The exposure to cybersecurity awareness programmes plays a role in empowering consumers with the confidence required for them to behave in a manner that ensures their security and privacy as far as their PII is concerned. The TPB is behavioural in nature and the awareness programmes are aimed at changing consumer behaviour to ensure that they take the necessary precautionary measures to protect themselves when transacting on e-commerce platforms (Madden et al., 1992). Both the independent variable of cybersecurity awareness programmes (motivation and security & privacy) and the dependent variable of consumer confidence are addressed in this study to explore and understand how cybersecurity awareness programmes influence the consumers' confidence when transacting on e-commerce platforms.

2.3.1 Awareness programmes

Cybersecurity awareness programmes have been studied by multiple scholars and have been referred to interchangeably as security awareness training. A cybersecurity awareness programme is defined as a programme designed to educate users of a specific computing platform and/or application on the safe usage thereof and to provide them with safety guidelines on responsible computing and safeguarding of information assets (Hueca et al., 2020). Hueca et al. (2020) Further state that awareness programmes are about influencing user behaviour through relevant information about cyber risks. Given the increasing risks that are associated with transacting online, it is vital for e-commerce platform owners to take the necessary measures, which ensure that their clientele is well aware of the treat landscape and the mitigation strategies that they may use to

protect themselves. This indicates that cybersecurity awareness does is not the sole responsibility of the e-commerce platform owners but of consumers as well. Zwilling et al. (2020) Refer to awareness programmes as increasing knowledge about cybersecurity by means of training programmes.

A study done by Kritzinger and von Solms (2010) states that home users use the internet for many activities, including e-commerce, without the required knowledge to protect themselves from cyber threats and thus exposing themselves because of this limited knowledge. They conclude that cybersecurity awareness programmes should be targeted at everyone in society, as awareness and education influence a change in behaviour (Kritzinger and von Solms, 2010). During e-commerce transactions when knowledge is absent or limited it becomes much easier to trick consumers. This in turn affects consumers' spending habits which could be detrimental to e-commerce (Matbouli and Gao, 2012).

Hueca et al. (2020) State that an awareness programme must include the following aspects: security policies, which the organisation follows, highlighting security risks that exist for the organisation for both their internal and external interfaces, information about what the user is responsible for, and finally the processes put in place to constantly monitor the awareness programme. For the purpose of this study, the outline by Hueca et al. (2020) is partially adopted, with the exception of security policies followed by the organisation, as this study is concerned with whether the education provided by these programmes builds consumer confidence when transacting on e-commerce platforms.

The lack of awareness of the benefits of e-commerce is detrimental to this type of trade and could prevent it from growing, especially in developing countries

such as South Africa, therefore making training and workshops all the more important for consumers (Yaseen et al., 2017).

Delivery of awareness programmes to the audience must have the desired impact in order to influence behavioural change. Zhang-Kennedy and Chiasson (2021) It becomes a fruitless exercise when the awareness programmes are not designed on such a way that they catch the attention of the user at the right time in order to achieve the desired impact. When multimedia is used to create awareness, the engagement and motivation to use this content increases.

2.3.2 Motivation

In terms of cybersecurity awareness programmes, Hueca et al. (2020) highlighted that it is about behaviour which motivates the user to act in a specific manner. The presence of information regarding what users are responsible for when using platforms could very well serve as motivation for them to interact with the platform in a responsible and informed manner. This in turn allows consumers to act in a particular manner which favours protecting themselves from cybercrime. Shah and Agarwal (2020) state that target behaviour is motivated by behaviour intent where a change in behaviour is pertinent for effective awareness programmes. Awareness programmes motivate consumers in various ways, such as local South African First National Bank which sends out constant email communications to their clients which inform them of the different types of cyber attacks which they need to be on the lookout for such as phishing. These messages are constant on all their platforms and inform the user of the necessary precautions they can take in order to protect themselves. These communications may be seen as awareness programmes, as they make consumers aware of

cybercrimes that may be initiated against them and what actions they need to take to ensure their safety and protection against them.

2.3.3 ISSUES OF PRIVACY

The access to consumer data by unauthorised parties is considered an invasion of their privacy (Muneer et al., 2018). There is a potential loss of personal consumer data concern when consumers are participating in e-commerce due to their low level of awareness. Falahat et al. (2019) State that e-commerce growth may be slowed down when consumers have no confidence that their privacy and information are safe. From a South African lens, it is imperative to educate the nation as uptake of e-commerce grows to ensure that consumers are appraised of how privacy is protected by e-commerce platforms from which they make purchases.

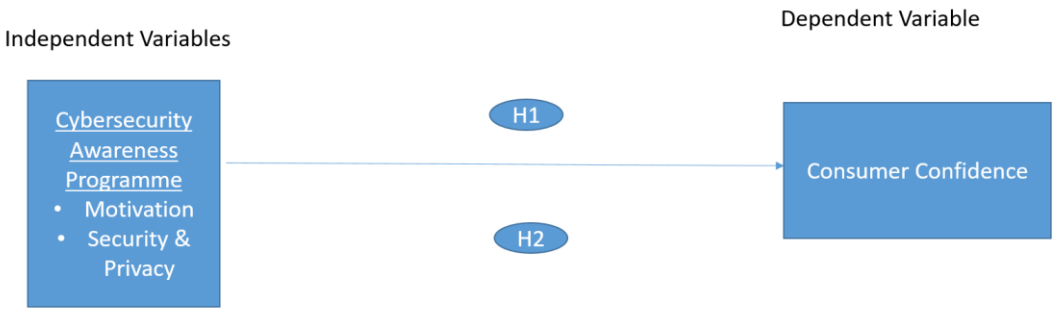
(Lu, 2009) states that the manner in which consumers perceive the organisation which is trading and how it ensures protection and privacy of PII, results in consumer confidence being impacted, therefore if the perception is that the protection and privacy of PII is a priority then the consumers' confidence becomes higher. The risk of compromised privacy plays a major role in how consumers perceive an e-commerce platform (Gurung et al., 2008). Consumers become wary when participating in e-commerce due to perceived security risks, thereby negatively influencing their intention to purchase (Gurung et al., 2008). This perceived risk subsequently has a negative impact on the e-commerce platform and may have dire consequences, especially when the organisation is only digitally based. A study done by Bakar et al. (2013) in Malaysia found that consumers were not sure of whether or not e-commerce merchants were

protecting their personal data when making purchases. Therefore, this lack of awareness placed them at risk of being victims of cybercrime. Organisations must ensure that they clearly demonstrate to their customers that they take privacy and security seriously on their e-commerce platforms by ensuring that they legitimately communicate the privacy and security measures they have taken to ensure their customers are safe on their platforms (Smith, 2004). When cybercrime is more prominent than the measures which are put in place to ensure cyber secure behaviour, this results in a fall in consumer confidence (Smith, 2004).

2.3.4 Conceptual framework

The below figure is a proposed conceptual framework (hypotheses) which is aimed at demonstrating how cybersecurity awareness programmes can build consumer confidence. This conceptual framework is aimed at demonstrating that H (2) is dependent on the existence of H (1). Therefore, consumer confidence when transacting on e-commerce platforms is low to non-existent because consumers have not been exposed to the relevant cybersecurity awareness programs, which serve as motivation to act and make informed decisions about protecting their personal Identifiable information (PII), and being informed of how their privacy and security is ensured by the e-commerce platform they transact on. These decisions are an important factor in the transacting decisions of consumers and subsequently for e-commerce platform owners.

Figure 1: Conceptual Model



Lebogo (2021)

2.3.5 Definition of hypotheses

The following hypotheses have been developed in relation to this study.

H1: Cybersecurity awareness programmes positively influence consumer confidence when transacting on e-commerce platforms.

H2: Cybersecurity awareness programmes motivate e-commerce consumers to transact cautiously in order to enhance their security and privacy, which in turn will increase consumer confidence.

The two hypotheses have been formulated, since this study aims to determine whether the exposure to cybersecurity awareness programmes has an influence on consumer confidence when transacting on e-commerce platforms, or not. Furthermore, this study seeks to understand cybersecurity awareness as a construct and the manner in which it relates to the confidence of the consumer (if at all) when transacting online.

2.4 Conclusion of Literature Review

Cybersecurity awareness programmes play an important role in ensuring that consumers are aware of the dangers of cybercrime, as e-commerce is an important aspect of the economy that must be treated with the utmost care. E-commerce plays an important role in the South African economy as it has ensured that South Africa (as a developing country) participates in digital business. There are frameworks and policies that have been developed in South Africa to promote a culture of cybersecurity for all users. Consumer confidence, specifically for e-commerce users, is strongly influenced by consumer behaviour based on the knowledge they have when participating in e-commerce and the trust they have in retailers guaranteeing their security is a priority. E-commerce consumers too have a responsibility to be aware of their behaviours in order to reduce the effects of cybercrime. The literature review findings have resulted in limited literature specific to this study. Many studies have focused on trust, attitudes, behaviours, normative beliefs, etc., but there is a lack of literature linked to direct associations between consumer confidence and cybersecurity awareness programmes.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 RESEARCH APPROACH

According to Creswell and Creswell (2017), a research approach is a detailed plan of how the research study will be conducted including how the data will be collected, interpreted and analysed based on the research problem. For the purpose of this study, a quantitative method where the researcher collected and obtained data through a structured survey was adopted. This method was utilised as a means to address the research questions of this study and the relationships between the identified variables to understand how the cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms.

Variables are referred to as the specific attributes which will be measured within the study (Creswell and Creswell, 2017). The quantitative methodology allows the researcher to measure variables numerically. The positivist worldview is appropriate for this study as it assessed and reduced the problem into smaller portions and variables in order to determine influence, and/or outcomes (Creswell and Creswell, 2017).

3.2 RESEARCH DESIGN

Research design is the outline of how data, which is meaningful and adequately answers the research questions, will be collected (Schindler, 2019). This study utilised a survey to collect data. Therefore, this correlational study does not focus

on one variable but many variables and not necessarily one causal relationship. Hence, a cross-sectional design is appropriate when collecting data for more than one variable (Aggarwal and Ranganathan, 2019). Creswell and Creswell (2017) state that survey research allows the researcher to enumerate the description of the variables for later statistical analysis. This is deemed appropriate as this study seeked to explore whether cybersecurity awareness programmes build the confidence of the e-commerce consumer using multiple variables. The ability to enumerate the results of the variables as measured by the study enabled this study to assess whether or not awareness programmes build consumer confidence from the sample selected. The advantage of using this type of design for this study meant that it may be administered online, which was not costly to distribute.

3.3 POPULATION AND SAMPLING

3.3.1 Population

The population of a study is the appropriate subjects from which the researcher is able to derive answers to the research questions being posed. (Schindler (2019). The population used for this study was e-commerce consumers in the Gauteng Province of South Africa. According to Davis (2019), South Africa has an estimated 18.43 million e-commerce users. Participants met the following criteria in order to be considered for this study from a consumer point of view:

- They must have internet access;
- They must have a device from which they can access the internet; and
- They must confirm that they participate in e-commerce.

This study excluded any demographic information, as e-commerce transactions are undertaken by anyone from any background with a device that has internet access and connection.

3.3.2 Sampling

A sample is defined as a subset of the population that will be utilised for the study (Cooper and Schindler, 2014). Sampling design refers to how the researcher will select the population characteristics of the selected participants (Creswell and Creswell, 2017). Sampling is a technique which utilises probability or non-probability based on what the researcher's objectives will require (Creswell and Creswell, 2017). There are various types of sampling, i.e. probability and non-probability sampling. (Etikan and Bala, 2017) distinguish between the different types as quota sampling, which is when the researcher accesses a population using a quota sample consisting of the characteristics found in the main population until the required number is obtained. Accidental sampling is similar to quota sampling, but not guided by particular characteristics. Purposive sampling is a sample chosen with the judgment of the researcher looking at the factors that will ensure that the researcher will be able to collect relevant data, etc. Probability sampling is randomised, therefore allowing all objects an equal chance at participating in the study (Etikan and Bala, 2017).

The randomised sampling method was used for this study to ensure that there was equal probability of participants to be selected for the study. The sample were individuals who utilise e-commerce platforms in South Africa within the Gauteng Province. This was deemed the most appropriate method in order to

collect relevant data with the purpose of ensuring that the research problem is adequately addressed.

3.4 DATA COLLECTION METHODS

A link to the survey was placed on social media sites namely Facebook, Twitter and LinkedIn. The survey was also distributed via email and WhatsApp. The survey was developed on qualtrics. Qualtrics is an online- based survey tool, which allows data to be collected and analysed with ease, i.e. compiling of the survey on a web-based platform and selecting how the survey may be completed, e.g. via web, mobile, tablet, etc. For convenience, the survey was made mobile friendly, i.e. participants could complete the survey using mobile phones and other internet-connected devices to ensure that the best possible reach was achieved.

3.4.1 Pilot study

An initial pilot study was run to ensure that the participants were actually able to participate on their preferred medium without any issues of being able to access and participate, as well as to ensure that the survey was understandable and to obtain the relevant feedback. The researcher obtained feedback on the questions and amended them accordingly in order to ensure that it is easy to understand and complete when sent out officially to all participants. The following amendments were made to the questions based on the pilot:

- On the Consumer Confidence: Motivation section the following question was omitted: “I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me

via email." This question was deemed similar to the following question: "I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness," which is contained in the Cybersecurity Awareness section. The respondents felt that the question was a duplication of the same question.

- Under the Consumer Confidence: Security & Privacy section the following question was omitted: "I'm made aware of how my privacy is protected when transacting on e-commerce platforms." This particular question was viewed as irrelevant as it was deemed as encompassed in the following question: "Cybersecurity awareness programmes inform me about how to ensure that my data is secure online."
- Under the Cybersecurity Awareness section, the following amendments were made. The following question was enhanced from, "Cybersecurity awareness programmes are effective" to "Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime." The following statement was added: "Cybersecurity awareness programmes are important for me."
- A definition, which explains to the reader what a cybersecurity awareness programme in the context of this study, was added to provide a clearer explanation to respondents.
- A definition of what e-commerce is in the context of this study was added.

3.5 RESEARCH INSTRUMENT

The research instrument addressed the sub-research questions as stated in Chapter 1 and the detailed instrument is provided in Appendix B.

A structured survey was partitioned as per the defined variables with fixed questions. A total number of 14 questions were asked in the research instrument. These questions emerged from existing literature, which was used as a baseline for this study. This survey was distributed to participants who were screened to ensure that they were e-commerce consumers prior to participating in the study. The survey was used to collect data, which was used for statistical analysis, and to assess and correlate the variables in order to determine whether cybersecurity programmes build consumer confidence when transacting on e-commerce platforms. The instrument firstly introduced the participant to the topic by providing a brief background of the study, as well as its purpose. The survey requested consent from the user to participate in the study voluntarily and provided them with a confidentiality clause. An overall number of 250 valid responses was received which is deemed statistically significant for this study.

The survey was sub-divided into sections as per the defined variables, i.e. cybersecurity awareness programme and consumer confidence with relevant questions under each variable.

Different scales were used for the different sections to ensure that participants easily understand what is expected from them. The Likert scale refers to a summated rating scale where participants were afforded the opportunity to express their views on whether they agree or disagree with statements being posed in the instrument (Schindler, 2019). A true or false scale was also used in

order to obtain answers to the Privacy set of questions. For the purpose of this study, section 16 and 19 contained Likert-scaled questions and section 18 the true or false scale. The instrument is attached in Appendix A.

3.6 DATA ANALYSIS

Due to the enumeration of variables used in this study, statistical analysis using the SPSS software package was used to analyse the data once collected. Descriptive analysis will be used to numerically and systematically organise, as well as analyse, the data collected for this study (Fisher and Marshall, 2009). In analysing the data, the researcher:

(i) Assessed the number of surveys sent out versus the number of returned surveys and reported on the number of spoiled surveys;

(ii) Checked for response bias, i.e. the level at which non-respondents would have influenced the results had they actually responded;

(iii) Aggregated the scoring range, mean and standard deviation for each variable and the level of variation from the average score on each variable. A 60% confidence level will be calculated from the mean and standard deviation (Cooper and Schindler, 2014).This is done to test reliability of the data;

(iv) The researcher drew conclusions based on the results of the data analysis in terms of the questions answered and proven hypotheses and determined if any patterns were found and the meaning thereof (Creswell and Creswell, 2017); and

(v) The researcher also referred to past literature to ensure that the results are in line and consistent with existing literature.

3.7 VALIDITY AND RELIABILITY

3.7.1 Validity

Validity in research measures the extent to which an instrument measures exactly what it was intended to measure, while reliability is the degree to which an instrument will have the ability to produce the same outcome when replicated (Taber, 2018). In the case of this study the researcher must be able to meaningfully infer and make conclusions based on derived scores (Creswell and Creswell, 2017).

3.7.2 External Validity

Consumers exhibit various behaviours while transacting on e-commerce platforms. By studying the sample selected for a study, the researcher may make certain inferences and generalise at a particular point in time. For the purpose of this study, the researcher did not generalise the results of the study, as the sample had have unique responses, which cannot be applied to the general population of e-commerce consumers.

Creswell and Creswell (2017) State that internal validity pertains to the accuracy of inferences that the researcher is able to draw based on the data. In this study, the accuracy of the effect of the independent variables on the dependent variable, therefore the hypothesised outcomes, was addressed, whereby the researcher ensured that the survey was constructed in a logical manner and that all questions linked to the objectives of the study. The sample group will mature as changes in legislature and the advancement of awareness programmes may

trigger changes in behaviour, e.g. the implementation of the Protection of Personal Information Act in South Africa as of 1 July 2021. This was be taken into consideration to ensure that the responses are valid. The scales that were be applied in this study have been tested in various academic studies, e.g. a study conducted on consumer privacy perceptions on e-commerce done by (Gurung et al., 2008).

3.7.3 Reliability

Reliability in this study was be determined using the internal consistency method. Internal consistency refers to the extent to which the instrument is able to consistently measure what it is meant, e.g. a behaviour in a user (Sürücü and MASLAKÇI, 2020). Generally the behaviour patterns will differ from person to person and depending on when the instrument is administered, people experiences and knowledge bases will also vary (Taber, 2018). With this study the researcher aimed to take a snapshot in time; therefore, even if the same participants were to be engaged in a different time their responses will be fundamentally different as their experience with cybersecurity awareness programmes may change over time. In order to measure the internal consistency the Cronbach alpha coefficient was applied. The Cronbach alpha coefficient tests internal consistency by determining the alpha coefficient by evaluating the extent to which a set of attributes sufficiently measures a single dimension construct (Sürücü and MASLAKÇI, 2020). The instrument was be deemed acceptable and reliable when a coefficient of 0.60 or over is achieved.

3.8 LIMITATIONS

This research has the following limitations:

This research study may have an exhaustive list of independent variables, which may be deemed appropriate to measure whether confidence is built by cybersecurity awareness programmes on e-commerce platforms. However, for the purpose of this study and to test the hypotheses developed the selected variables were used.

3.9 ETHICAL CONSIDERATIONS

This research study adhered to, but it was not limited to the following ethical considerations in order to avoid issues of bias, privacy, respect, the right to choose, etc.

To ensure that the research was be conducted in an ethical manner, the following processes were be adhered to:

(i) Provision of formal consent: All participants were be requested to provide consent in order to participate in the study;

(ii) Respect for privacy and anonymity: the researcher did not associate any responses with any particular respondents' names;

(iii) Harm: The researcher did not through this research pose any harm to any participant and maintained the option of voluntary participation and opting out at any point when the participant, for whatever reason, did not feel the need to proceed with the research instrument;

(iv) Transparency: the researcher was be transparent about the objectives of the research upfront;

(v) Non–discrimination: the researcher did not discriminate against anyone, but allowed the correct type of participants to take part in the study; and

(vi) Adhered to Wits University specific ethical rules and regulations

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

The purpose of this chapter is to present the results by providing a description of the data analysis. The data was analysed using SPSS version 27.0. The data was collected by distributing a survey to respondents, on social media platforms i.e. Facebook, Twitter & LinkedIn, and distributed via email and WhatsApp. The survey was subsequently completed by 250 participants (n= 250) who indicated that they do participate in e-commerce by making purchases online.

The participants who met the criteria for inclusion did not answer all the questions posed; therefore, the percentages are reflective of the total number of respondents answering the individual questions. The survey was compiled using qualtrics. Data was collected to explore whether cybersecurity awareness programmes build consumer confidence in the use of e-commerce platforms in South Africa.

The results presented the descriptive statistics in the form of graphs, cross-tabulations and other figures for the quantitative data collected. Inferential techniques include the use of correlations and chi square test values, which are interpreted using the p-values. The traditional approach to reporting a result requires a statement of statistical significance. A p-value was generated from a test statistic. A significant result is indicated with "$p < 0.05$" (5%). The results are presented as follows: a synopsis of the sample, the research instrument and its amendments, factor analysis, reliability statistics, section analysis, cross-tabulations, correlations, structural equation model and conclusion.

4.2 The sample

Respondent consent: 99% (294 out of 297 responses) of respondents provided consent to this study with the exception of 1% (3 out of 297 responses) who did not consent to taking part in the study. There was 297 responses collected for this study. Out of these only 250 (84%) met the inclusion criteria and were subsequently used for the data analysis. 47 (16%) participants did not complete the survey.

4.2.1 Reliability statistics

The two most important aspects of precision are reliability and validity. Reliability is computed by taking several measurements on the same subjects. A reliability coefficient of 0.60 or higher is considered as “acceptable” for a newly developed construct.

The table below reflects the Cronbach’s alpha score for all the items that constituted the survey to test the internal consistency. This is represented as per the sections of the survey.

Table 2: Cronbach Alpha Scores

	Section	Number of Items	Cronbach's Alpha
Q16	Consumer Confidence: Motivation	5	0.747
Q18	Consumer Confidence: Security & Privacy	3	0.635
Q19	Cybersecurity Awareness Programmes	6	0.772

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

4.3 Factor analysis

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

Table 3: KMO and Bartlett's Test

nr	Section	Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	Bartlett's Test of Sphericity		
			Approx. Chi-Square	df	Sig.
Q16	Consumer Confidence: Motivation	0.686	412.049	10	0.000
Q18	Consumer Confidence: Security & Privacy	0.621	102.443	3	0.000
Q19	Cybersecurity Awareness Programmes	0.814	368.960	15	0.000

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

4.4 Section analysis

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

4.4.1 Results pertaining to hypothesis 1

Cybersecurity awareness programmes positively influence consumer confidence when transacting on e-commerce platforms

Table 99 summarises the scoring patterns for question 19 which used a 5 point likert scale to rate responses where 1 = Strongly disagree, 2 = Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly agree. The questions in this section were used to measure respondent awareness of cybersecurity programmes when participating in e-commerce.

The table below summarises the scoring patterns. High scores indicate that cybersecurity awareness programmes are positively influencing consumers when transacting on e-commerce platforms. The average overall level of agreement for Q19.1 to Q19.5 is 75% whereby a significant increase in Q19.6 is noted, which has an overall level of agreement of 84%. These questions are related to how consumers of e-commerce websites use the learnings of these programmes and the encouragement they receive from these programmes to shop online due to their presence. These programmes encourage secure transacting and vigilance online. They also relate to what cybersecurity awareness programmes communicate to the consumers and their effectiveness, while question 19.6 requested respondents to indicate their view about the importance of these programmes. Lower scores indicate that consumer confidence in transacting on e-commerce platforms is negatively influenced by the presence of these programmes. Question 19.2, “I would shop more online if there were awareness programmes available to increase my knowledge”, had a response rate of 98.8% (n=247), of which 71.2 % of respondents agreed and 12.1% disagreed. Therefore, the majority of the respondents to this particular question indicated that they would shop online with awareness programmes being available, which is a positive indicator for e-commerce platform business. This indication also sends a message to platform business owners to take the implementation of

cybersecurity awareness programmes seriously, as it has an impact on their sales.

Table 4: Scale items for cybersecurity awareness programmes questions from respondents (%)

		Strongly Disagree		Disagree		Not sure		Agree		Strongly Agree		Chi Square p-value
		Count	Row N %	Count	Row N %	Count	Row N %	Count	Row N %	Count	Row N %	
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime	Q19.1	1	0.4%	18	7.3%	33	13.4%	122	49.4%	73	29.6%	< 0.001
I would shop more online if there were awareness programmes available to increase my knowledge	Q19.2	5	2.0%	25	10.1%	41	16.6%	85	34.4%	91	36.8%	< 0.001
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Q19.3	3	1.2%	31	12.6%	29	11.7%	133	53.8%	51	20.6%	< 0.001
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	Q19.4	5	2.0%	33	13.4%	27	10.9%	123	49.8%	59	23.9%	< 0.001
I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness	Q19.5	1	0.4%	37	15.0%	17	6.9%	128	51.8%	64	25.9%	< 0.001
Cybersecurity awareness programmes are important for me	Q19.6	1	0.4%	7	2.8%	20	8.1%	103	41.7%	116	47.0%	< 0.001

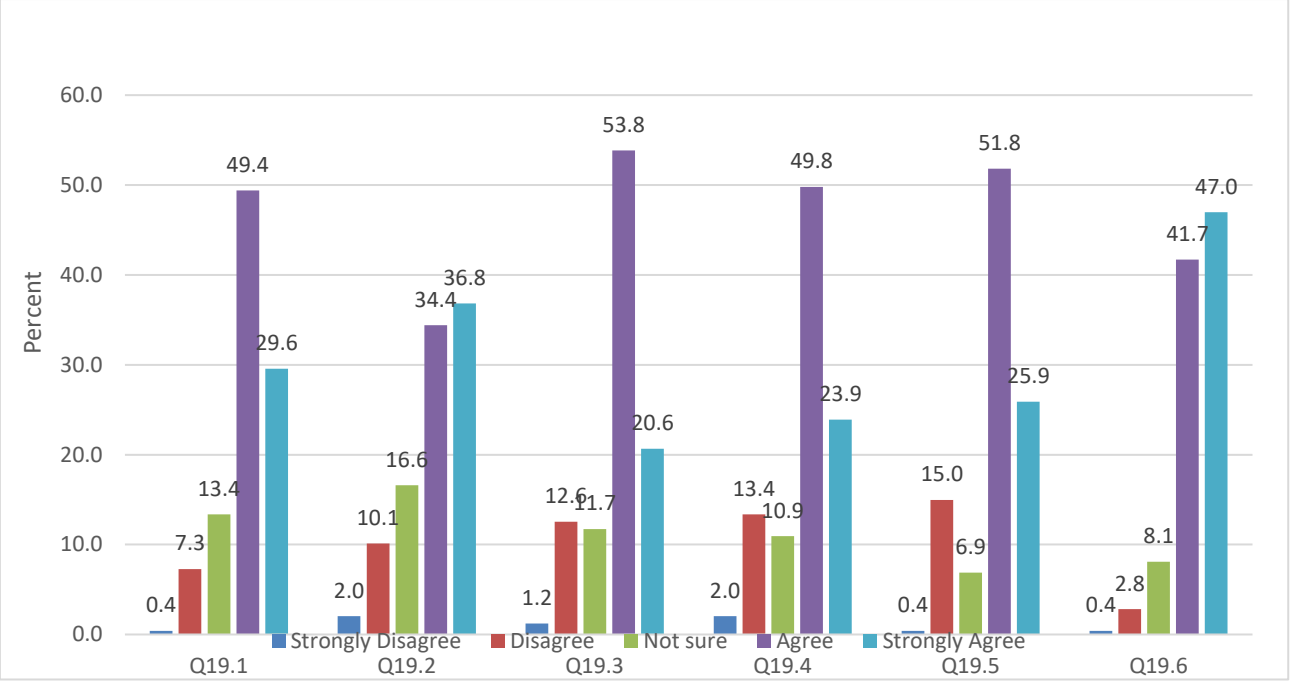


Figure 2: cybersecurity awareness programmes responses bar chart

4.4.2 Results pertaining to hypothesis 2

Cybersecurity awareness programmes motivate e-commerce consumers to transact cautiously in order to enhance their security and privacy, which both increase consumer confidence.

4.4.3 Consumer confidence: Motivation

The table below summarises the scoring patterns for question 16, which used a 5-point likert scale to rate responses where 1 = Strongly disagree, 2 = Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly agree. One response per question was permitted for each respondent. The questions were used to measure consumer confidence in relation to whether the messages they saw motivated them to transact responsibly and thus measure their understanding of what these

messages are meant for and if they at all influence their behaviour when participating on e-commerce platforms.

High scores indicate that consumers are aware of the cybersecurity awareness messages and are thus motivated to transact in a responsible manner, while lower scores indicate that the cybersecurity awareness messages are inneffective and do not motivate behavioural changes in consumers when transacting on e-commerce platforms. As such, consumers will not be motivated to transact on e-commerce platforms at all, or transact irresponsibly due to the lack of adequate knowledge on safe cybersecurity practices and behaviours.

The following patterns are observed:

- All statements show (significantly) higher levels of agreement, whilst other levels of agreement are lower (but still greater than levels of disagreement).
- There are no statements with higher levels of disagreement, i.e. no statements higer than 10% for disagreement and stongly disagreeing respectively.
- The significance of the differences is tested and shown in the table below.
- Factor analysis indicates that all of the statements perfectly aligned along a single component, implying the statements perfectly measured consumer confidence – motivation.
- It is noted that the range of overall agreement is between 75% and 84%. This is a high level of agreement across the dimension being measured, implying that the awareness programmes are providing some level of confidence to consumers, however, with a special focus on Q16.3 and

16.4 where the confidence in relation to motivation is tabulated at item 16.3 and 16.4 . The responses for these two questions were reported to be 50% and 53.6% respectively in agreement, while 5.2% and 6 % disagreed, respectively.

Table 5: Scale items for consumer confidence: Motivation questions from respondents (%)

		Strongly Disagree		Disagree		Not sure		Agree		Strongly Agree		Chi Square p-value
		Count	Row N %	Count	Row N %	Count	Row N %	Count	Row N %	Count	Row N %	
The security awareness messages I see on e-commerce platforms inform my actions	Q16.1	6	2.4%	24	9.6%	32	12.8%	123	49.2%	65	26.0%	< 0.001
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms	Q16.2	3	1.2%	23	9.2%	25	10.0%	133	53.2%	66	26.4%	< 0.001
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Q16.3	2	0.8%	13	5.2%	32	12.8%	125	50.0%	78	31.2%	< 0.001
With awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce platforms	Q16.4	1	0.4%	15	6.0%	24	9.6%	134	53.6%	76	30.4%	< 0.001
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Q16.5	5	2.0%	30	12.0%	26	10.4%	106	42.4%	83	33.2%	< 0.001

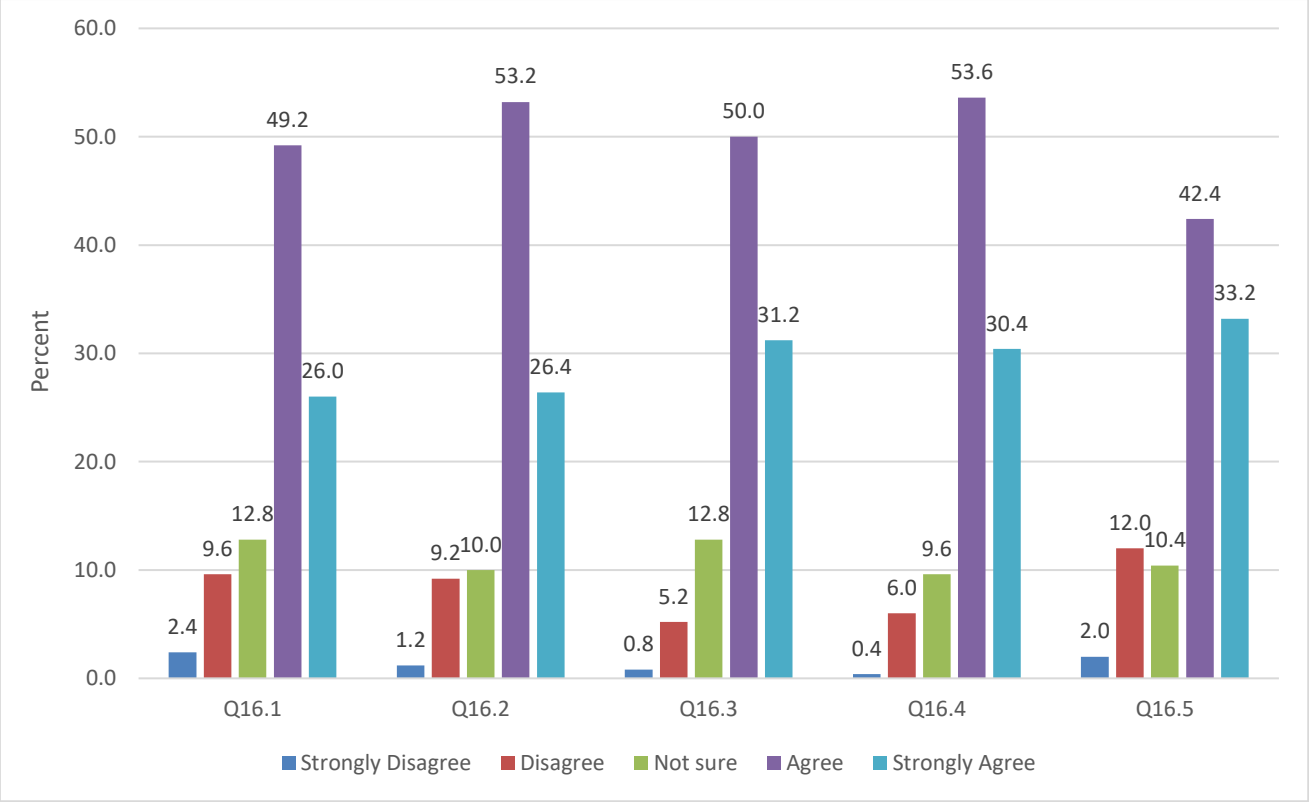


Figure 3: consumer confidence: Motivation bar chart

4.4.4 Consumer confidence: Security & privacy

This section requested respondents to respond with a true or false response to indicate their agreement or disagreement with the statements posed in the survey. Respondents were limited to a true or false response where only one response per question was permitted. The questions were used to measure consumer confidence in relation to security and privacy in order to build an understanding of whether consumers feel confident that cybersecurity awareness programmes are effective in building their confidence when transacting by ensuring that they are aware of how their privacy is protected and the role they play in ensuring privacy and security of their data.The table below summarises the scoring patterns.

There are significantly higher and similar levels of respondents who indicated that they agreed (True) with the statements. This implies that a higher number of respondents agree that they are aware of how their security and privacy are protected and what their responsibility is towards security and privacy. The two key items on security and privacy being item 18.1 and 18.2 both had a response rate of 100% each. The below table provides an overall feedback on the scores obtained for each item. The noticeable high scores of all items in this section indicate that participants are aware of security and privacy of their data on e-commerce platforms.

Table 6: Scale items for consumer confidence: Security & privacy questions from respondents (%)

		False		True		Chi Square p-value
		Count	Row N %	Count	Row N %	
I'm made aware of how my privacy is protected when transacting on e-commerce platforms	Q18.1	47	18.8%	203	81.2%	< 0.001
Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	Q18.2	34	13.6%	216	86.4%	< 0.001
Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	Q18.3	41	16.4%	209	83.6%	< 0.001

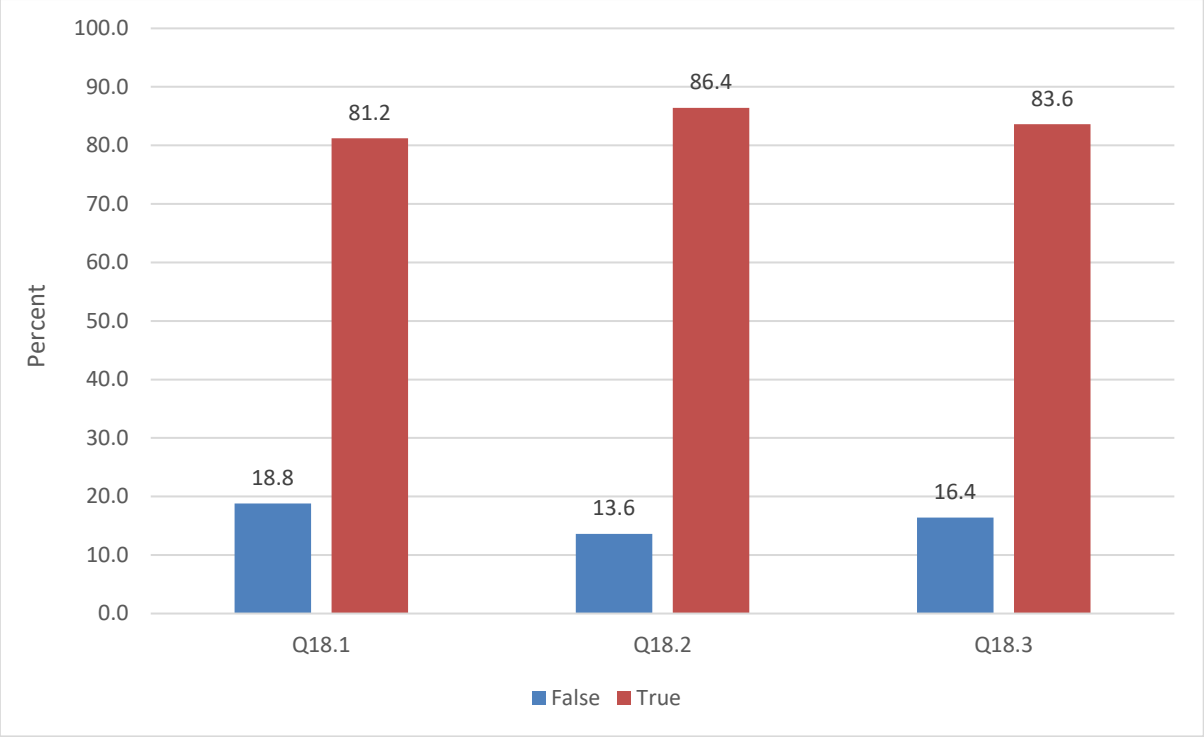


Figure 4: consumer confidence: Security & privacy Bar Chart

4.5 CROSS-TABULATIONS

A Chi square test of independence was performed to determine whether there was a statistically significant relationship between the variables (rows vs columns). The null hypothesis states that there is no association between the two. The alternate hypothesis indicates that there is an association. The table summarises the results of the Chi square tests.

See Appendix: (C– Crosstabs – Bio vs Rest)

The following significant relationships were found:

- The p-value between “The security awareness messages I see on e-commerce platforms inform my actions” and “I’m made aware of how my privacy is protected when transacting on e-commerce platforms” is 0.006. Respondents

therefore feel that privacy awareness is protected when transacting on e-commerce platforms and plays a significant role in terms of how respondents view the security awareness messages seen on e-commerce platforms informing their actions. The relationships tabulated below are indicative of the significantly higher number of respondents who scored True (79.3%) and agreed with the statement, “The security awareness messages I see on e-commerce platforms inform my actions”, compared to those who scored False (57.5%).

Table 7: P-Value Analysis 1

			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total
			False	True	
The security awareness messages I see on e-commerce platforms inform my actions	Strongly Disagree	Count	3	3	6
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	6.4%	1.5%	2.4%
	Disagree	Count	9	15	24
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	19.1%	7.4%	9.6%
	Not sure	Count	8	24	32
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	11.8%	12.8%
	Agree	Count	21	102	123
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	44.7%	50.2%	49.2%
	Strongly Agree	Count	6	59	65
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	12.8%	29.1%	26.0%
Total		Count	47	203	250

	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%

- The p-value between "The security awareness messages I see on e-commerce platforms inform my actions" and "Cybersecurity awareness programmes inform me about how to ensure that my data is secure online" is 0.001. That is, cybersecurity awareness programmes' role in ensuring that consumers are informed about data security played a significant role in terms of how respondents viewed how their actions were informed by the security messages they saw on e-commerce platforms. The relationships tabulated below are indicative of the significantly higher number of respondents who scored True (78.9%) and agreed with the statement, "The security awareness messages I see on e-commerce platforms inform my actions", compared to those who scored False (56.1%).

Table 8: P-Value Analysis 2

			Cybersecurity awareness programmes inform me about how to ensure that my data is secure online		Total
			False	True	
The security awareness messages I see on e-commerce platforms inform my actions	Strongly Disagree	Count	2	4	6
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	4.9%	1.9%	2.4%
	Disagree	Count	6	18	24
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	14.6%	8.6%	9.6%
	Not sure	Count	10	22	32
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	24.4%	10.5%	12.8%
	Agree	Count	21	102	123

		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	51.2%	48.8%	49.2%
	Strongly Agree	Count	2	63	65
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	4.9%	30.1%	26.0%
Total		Count	41	209	250
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%

- The p-value between “The security awareness messages I am sent inform my transacting decisions on e-commerce platforms” and “Cybersecurity awareness programmes inform me about how to ensure that my data is secure online” is 0.001. This shows that the role of cybersecurity awareness programmes informing consumers about how to ensure that their data is secure online played a significant role in terms of how respondents viewed the security awareness messages sent to them and their influence on their transacting decisions on e-commerce platforms. The relationships tabulated below are indicative of the significantly higher number of respondents who scored True (83.2%) agreed with the statement, “The security awareness messages I see on e-commerce platforms inform my actions”, compared to those who scored False (61%).

Table 9: P-Value Analysis 3

			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total
			False	True	
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Strongly Disagree	Count	0	2	2
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	1.0%	0.8%
	Disagree	Count	8	5	13
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	2.5%	5.2%
	Not sure	Count	8	24	32
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	11.8%	12.8%
	Agree	Count	21	104	125
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	44.7%	51.2%	50.0%
	Strongly Agree	Count	10	68	78
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	21.3%	33.5%	31.2%
Total		Count	47	203	250
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%

The p-value between the "Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms" and "I'm made aware of how my privacy is protected when transacting on e-commerce platforms" is 0.003. This shows that when consumers are made aware of how their privacy is protected by the e-commerce platform, it plays a significant role in terms of how the respondents view the way in which cybersecurity awareness programmes increase their level of confidence when transacting on e-commerce platforms. The relationships tabulated below are indicative of the significantly higher number of respondents who scored True (84.7%) and who

agreed with the statement, “The security awareness messages I see on e-commerce platforms inform my actions”, compared to those who scored False (66%).

The P-Value between “I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email” and “Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy’ is 0.000. This shows that the manner in which cybersecurity awareness programmes inform consumers about their responsibility towards maintaining their privacy had a significant role in how inclined consumers were to read cybersecurity awareness messages they see on platforms than those sent to them via email.

Table 10: P-Value Analysis 4

			I’m made aware of how my privacy is protected when transacting on e-commerce platforms		Total
			False	True	
Cybersecurity awareness programs increase my level of confidence for transacting on e-commerce platforms	Strongly Disagree	Count	0	2	2
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	1.0%	0.8%
	Disagree	Count	8	5	13
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	2.5%	5.2%
	Not sure	Count	8	24	32
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	11.8%	12.8%
	Agree	Count	21	104	125
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	44.7%	51.2%	50.0%
	Strongly Agree	Count	10	68	78
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	21.3%	33.5%	31.2%
Total		Count	47	203	250
		% within I’m made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%

Table 11: P-Value Analysis 5

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total
			False	True	
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Strongly Disagree	Count	1	4	5
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	2.9%	1.9%	2.0%
	Disagree	Count	9	21	30
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	9.7%	12.0%
	Not sure	Count	9	17	26
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	7.9%	10.4%
	Agree	Count	11	95	106
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	32.4%	44.0%	42.4%
	Strongly Agree	Count	4	79	83
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	11.8%	36.6%	33.2%
Total		Count	34	216	250
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	100.0%	100.0%	100.0%

The p-value between “I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email” and “Cybersecurity awareness programmes inform me about how to ensure that my data is secure online” is 0.027. This shows that the manner in which cybersecurity awareness programmes inform consumers about their

responsibility towards maintaining their privacy had a significant role in how inclined consumers were to read cybersecurity awareness messages they see on platforms than those sent to them via email.

Table 12: P-Value Analysis 6

			Cybersecurity awareness programmes inform me about how to ensure that my data is secure online		Total
			False	True	
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Strongly Disagree	Count	1	4	5
		% within cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.4%	1.9%	2.0%
	Disagree	Count	10	20	30
		% within cybersecurity awareness programmes inform me about how to ensure that my data is secure online	24.4%	9.6%	12.0%
	Not sure	Count	5	21	26
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	12.2%	10.0%	10.4%
	Agree	Count	18	88	106
		% within cybersecurity awareness programmes inform me about how to ensure that my data is secure online	43.9%	42.1%	42.4%
	Strongly Agree	Count	7	76	83
		% within cybersecurity awareness programmes inform me about how to ensure that my data is secure online	17.1%	36.4%	33.2%
Total		Count	41	209	250
		% within cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%

The p-value between “I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases” and “Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy” is 0.045. This shows that the manner in which cybersecurity awareness programmes inform consumers about their responsibility towards maintaining their privacy plays a significant role in them remembering the learnings of cybersecurity awareness programmes when making purchases on e-commerce platforms.

Table 13: P-Value Analysis 7

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total
			False	True	
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Strongly Disagree	Count	1	2	3
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	0.9%	1.2%
	Disagree	Count	5	26	31
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	15.2%	12.1%	12.6%
	Not sure	Count	7	22	29
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	21.2%	10.3%	11.7%
	Agree	Count	18	115	133
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	54.5%	53.7%	53.8%
	Strongly Agree	Count	2	49	51
		% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	6.1%	22.9%	20.6%

Total	Count	33	214	247
	% within cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	100.0%	100.0%	100.0%

All p-values more than 0.05 do not have a significant relationship; therefore, the below statements have no significant relationships. The common variable in relation to how participants responded to cybersecurity awareness programmes in these statements is privacy, which did not influence how they viewed cybersecurity awareness programmes and what they do for them on e-commerce platforms.

Table 14: Relationship analysis between variables

Variable	P-Value
Cybersecurity awareness programmes are important for me * I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.723
With awareness programmes in place, I feel empowered about the decisions I take when transacting on e-commerce platforms * I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.103
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime * I'm made aware of how	0.059

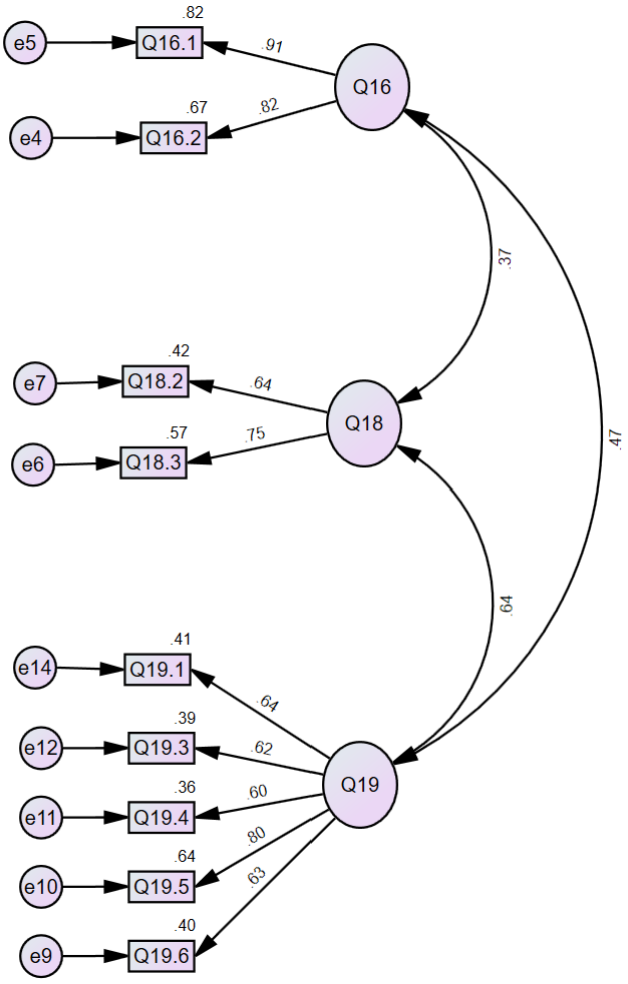
my privacy is protected when transacting on e-commerce platforms	
I would shop more online if there were awareness programmes available to increase my knowledge * I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.238
I would shop more online if there were awareness programmes available to increase my knowledge * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.238

4.6 CORRELATIONS

Bivariate correlation was performed on the (ordinal) data. The results are found in Appendix B. Positive values indicate a directly proportional relationship between the variables and a negative value indicates an inverse relationship. All significant relationships are indicated by a * or **. For example, the correlation value between "The security awareness messages I see on e-commerce platforms inform my actions" and "I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform" is 0.335. This is a directly related proportionality. Respondents indicate that the more security messages they receive, the more likely they are to read the cybersecurity messages, and vice versa.

4.7 STRUCTURAL EQUATION MODEL

Figure 5: SEM DIAGRAM



The path diagram for the modified structural equation model (SEM) is shown above. The model is a multivariate statistical result that was obtained using structural relationships, and applying a combination of factor analysis and multiple regression analysis techniques. It is used to analyse and understand whether or not there were multivariate relationships between variables and other

structural relationships between measured variables. The dimensions are coded as under reliability in Appendix D.

4.8 Result (Default model)

The minimum was achieved as follows:

Chi-square = 45.294

Degrees of freedom = 24

Probability level = .005

This Chi-square tests the null hypothesis that the over-identified (reduced) model fits the data as well as does a just-identified (full, saturated) model. In a just-identified model, there is a direct path (not through an intervening variable) from each variable to each other variable. In such a model, the Chi-square will always have a value of zero, since the fit will always be perfect. The probability should not be significant. In this model, the Chi square p-value is < 0.050 (p = 0.005).

Maximum Likelihood Estimates

Table 15: Regression Weights (Group number 1 – Default Model)

			Estimate	S.E.	C.R.	P	Label
Q16.2	<---	Q16	1.000				
Q16.1	<---	Q16	1.193	.146	8.193	***	par_1
Q18.3	<---	Q18	1.000				
Q18.2	<---	Q18	.791	.126	6.298	***	par_2
Q19.6	<---	Q19	1.000				
Q19.5	<---	Q19	1.601	.173	9.245	***	par_3
Q19.4	<---	Q19	1.251	.163	7.658	***	par_4
Q19.3	<---	Q19	1.208	.154	7.849	***	par_5
Q19.1	<---	Q19	1.139	.142	8.004	***	par_6

The variables loaded strongly along their various factors (significant p-values indicated by *** p < 0.001). These verify the exploratory factor analysis (EFA) obtained under factor analysis.

Table 16: Standardised Regression Weights (Group number 1 – Default model)

			Estimate
Q16.2	<---	Q16	.819
Q16.1	<---	Q16	.906
Q18.3	<---	Q18	.754
Q18.2	<---	Q18	.644
Q19.6	<---	Q19	.629
Q19.5	<---	Q19	.799
Q19.4	<---	Q19	.601
Q19.3	<---	Q19	.621
Q19.1	<---	Q19	.637

- The parameters are estimated by maximum likelihood (ML) methods, which represent an iterative procedure that attempts to maximise the likelihood that obtained values of the criterion variable will be correctly predicted. All of the coefficients were above the suggested value of 0.600. Two statements that loaded poorly were omitted from the model.

- **Model Fit Summary**

  The suggested acceptable value for relative Chi-square, CMIN/DF, should not be greater than 5, which is used to reduce dependency on sample size. A good model is indicated by RMSEA value of less than, or equal to 0.05.

Table 17: CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	30	45.294	24	.005	1.887
Saturated model	54	.000	0		
Independence model	9	735.306	45	.000	16.340

- CMIN is a Chi-square statistic comparing the tested model and the independence model to the saturated model. The ratio, CMIN/DF, the relative Chi-square, is an index of how much the fit of data to model has been reduced by dropping one or more paths. The CMIN/DF is less than the acceptable value of five (1.887). This meets the CMIN condition.

Table 18: Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.938	.885	.970	.942	.969
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

- These goodness of fit indices compare the model to the independence model rather than to the saturated model. The Normed Fit Index (NFI) is simply the difference between the two models' chi-squares divided by the chi-square for the independence model. For this data, the NFI is 0.938, which is more than the recommended value of 0.90 for a good fit. The Comparative Fit Index (CFI) uses a similar approach (with a non-central Chi-square) and is said to be a good index for use even with small samples. It ranges from 0 to 1, like the NFI, and 0.90 indicates good fit. The CFI value is 0.969, implying a good fit.

Table 19: RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.060	.032	.086	.253
Independence model	.248	.233	.264	.000

- The Root Mean Square Error of Approximation (RMSEA) estimates lack of fit compared to the saturated model. RMSEA of 0.050 or less indicates good fit, and between .05 and .08 an adequate fit. LO 90 and HI 90 are the lower and upper ends of a 90% confidence interval on this estimate. The model is an adequate fit, with the PCLOSE value (0.253) being non-significant. This condition is met (recommended > 0.050).

Regression Analysis

The level of significance relates to the strength of the relationships. The correlations are tested below.

Table 20: Covariance's (Group number 1 – Default Model)

			Estimate	S.E.	C.R.	P	Label
Q16	<-->	Q18	.077	.020	3.906	***	par_7
Q19	<-->	Q16	.172	.036	4.766	***	par_8
Q19	<-->	Q18	.087	.016	5.573	***	par_9

Table 21: Correlations (Group number 1 – Default Model)

			Estimate
Q16	<-->	Q18	.367
Q19	<-->	Q16	.470
Q19	<-->	Q18	.640

Null hypothesis: There is no correlation between each of the dimensions

Alternate hypothesis: There is a significant correlation.

All relationships are significant ($p < 0.001$). The results indicate a strong, directly proportional relationship between the latent variables, with each of the *r* estimates being positive.

4.9 CONCLUSION

This chapter presented an analysis of the study's results, which have been presented in table format. The data was collected from 250 anonymous respondents who indicated that they participate in e-commerce by making purchases on these platforms.

Conclusion for H1: Cybersecurity awareness programmes positively influence consumer confidence when transacting on e-commerce platforms

The responses in the survey generally indicate that e-commerce consumers are positively influenced by the cybersecurity awareness programmes, which they are exposed to with the scores in item 19.2 revealing that consumers would indeed shop more online if awareness programmes were there to increase their knowledge with an overall score of 71.2%. Additionally the scores on item 19.3 indicated with an overall agreement percentage of 81.6% that the learning obtained from cybersecurity awareness programmes were remembered by consumers which indicates that they are aware of cyber threats when making purchases because of the exposure to cybersecurity awareness programmes. The obtained scores revealed a Cronbach alpha of 0.772, which is above the confidence level. The hypothesis is accepted

Conclusion for H2: Cybersecurity awareness programmes motivate e-commerce consumers to transact cautiously in order to enhance their security and privacy which increases consumer confidence

The general responses from both questions 16 & 18 do not conclusively indicate that cybersecurity awareness programmes motivate cautious transacting behaviour. However, the results conclusively indicate that there is an influence in terms of the decisions taken by consumers with a 79.6 % of respondents agreeing that their transacting decisions are informed by the security awareness messages they see on e-commerce platforms. Additionally item, 18.1 to 18.3 had an overall higher score of above 80%, which indicates that consumers are made aware of their responsibilities and how the e-commerce platform ensures data security and privacy. The obtained scores on both items revealed a Cronbach alpha of 0.747 and 0.635 respectively. Therefore, the hypothesis is accepted as being true.

Two of the low loading factors (statements) were omitted from the SEM model. An inspection of the coefficients for each latent variable indicated high factor loadings. In addition, the path coefficients are reflected on the diagram. All of the coefficients are positive (proportional relationships were found) between the latent variables.

As this was a newly developed construct, it is also expected that the structural relationships may not have fitted accurately. However, certain indices are met and the model is an adequate fit.

CHAPTER 5. DISCUSSION OF RESULTS

5.1 Introduction

The purpose of this chapter is to provide a discussion of research findings related to research questions that guided the study. This chapter will explain the results in relation to the prior literature review. The purpose of this study is to explore the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa. This study asks the following two research questions: **To what extent does cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms?**

Emanating from the main research question, the sub- question emerged:

- ***How do cybersecurity awareness programmes influence e-commerce consumer confidence?***

The motivation behind this study was to assist business owners of e-commerce platforms to understand what is required in order increase consumer confidence through cybersecurity awareness programmes in response to the surge in cyberattacks, which may have dire consequences for their businesses. Another motivation was to demonstrate how e-commerce consumers perceive cybersecurity awareness programmes when shopping online. Cyberattacks are on the rise worldwide and South Africa as a developing country with many socio economic challenges is trying to stay on par with the world. This study explored the following variables, Consumer confidence: Motivation, Consumer confidence: security & Privacy and Cybersecurity awareness programmes in order to gain an

understanding of the role of cybersecurity awareness programmes in building e-commerce consumer confidence.

The discussion of the results will be the centre of this chapter. The first section will discuss the results pertaining to hypothesis 1, followed by results pertaining to hypotheses two followed by the conclusion.

5.2 Inclusion criteria

This study only included responses from respondents who consented to taking part in the research and those who indicated that they participate in e-commerce by making purchases online.

5.3 Discussion pertaining to H1

The protection motivation theory (PMT) postulates that cues to action influence security behaviour.(Li et al., 2019). The PMT is based on the protective behaviour that is exuded by the subject based on the perceived threat and their assessment of personal vulnerability towards the threat (Hong and Furnell, 2021). The Theory of planned behaviour on the other hand is focused on the consumer's attitude, their subjective norms, how they perceive the control, they have on their behaviour as well as decision making ability (Hong and Furnell, 2021). The results of this study suggest that consumers are in agreement that awareness programmes to some extent influence their behaviour as item 19.2 had an agreement level of 71.2 % stating that "they would shop more online if there were awareness programmes available to increase their knowledge. This may be seen as a positive influence as it encourages more engagement with the platform.

Hueca et al. (2020) Stated that awareness programmes are about influencing user behaviour through relevant information about cyber risks while Bada et al. (2019), on the other hand studied “why cybersecurity awareness campaigns fail to change behaviour” and came to the conclusion that acquiring knowledge though awareness programmes does not necessarily provide motivation to individuals to behave as guided by the programmes. In another study by van Bavel et al. (2019) which explored the use of the protection motivation theory to improve online behaviour the results of this study indicated that messages about cybersecurity threats which were communicated to users actually resulted in the abandonment of the online purchasing exercise completely instead of implementing appropriate behaviours that demonstrate that they are knowledgeable about cybersecurity threats. Consistent with this study’s results Smith (2004) stated that platforms with security related messages which in this case are referred to as awareness programmes are related to negative consumer risk perceptions but from a consumers perspective would positively influence their purchase intentions. knowledgeable people can make informed decisions and cybersecurity awareness programmes are another form of training programmes which may be used to increase knowledge of the consumer (Zwilling et al., 2020) . Item 19.4 of this study suggests that the knowledge received from these programmes comes in handy when consumers shop e-commerce platforms as it received a total agreement rate of 74.4% indicating that consumers actually read the cybersecurity awareness messages displayed to them when interacting with e-commerce platforms. Subsequently these programmes serve as an introduction to secure online behaviours which must be exercised by consumers (Hueca et al., 2020). This indicates that consumers are aware of the eminent

threats as the platforms make it a point to ensure that the knowledge is imparted through the awareness programmes. It therefore becomes imperative for consumers to have the necessary knowledge to make informed decisions in the face of threat. As the results also indicated that consumers agreed that cybersecurity awareness programmes are important to them in item 19.6 with an agreement rate of 88.7%. This may also be seen as a positive as consumers acknowledge the importance of these programmes.

Item 19.5 has a result of 15% of respondents who indicated that they disagree that they acknowledge and read the cybersecurity awareness messages they receive to increase their level of cybersecurity awareness. This suggests that there is a level of ignorance towards cybersecurty awareness messages by e-commerce consumers. Which means that these programmes have no impact or influence on these consumers. This study is concerned with wether the education provided by these programmes builds consumer confidence when transacting on e-commerce platforms. This cannot be the case when consumers do not consume the content of these programmes which should ultimatly be enforced. Kritzinger and Von Solms (2010) concluded in their study about the protection of home users that in enforcement of the consumption of awareness programmes is a must for regulators in order to make an impact. The correlations in the below table indicate the following, cybersecurity awareness programmes play a significant role in ifluencing consumer behavior and increasing their level of confidence when transacting on e-commerce platforms

The significant correlations between the below tabulated statements suggest that there is direct proportionality and that consumer actions are informed based on

acquired knowledge provided by cybersecurity awareness programmes. In line with the theory of protection motivation which indicates that ques of action influence security behaviour the statement “I would shop more online if there were awareness programmes available to increase my knowledge “ has a significant correlation with “Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms “. This suggests that for the fact that they are cybersecurity awareness programmes on an e-commerce platform consumer’s level of confidence increases resulting in positive outcomes for owners of these platforms. The overall responses of the participants on all items under this section of the survey appear to be positive.

Table 22: H1 correlations

Statement	Correlating statement	Bivariate Correlation score
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	The security awareness messages I see on e-commerce platforms inform my actions	.335**
I would shop more online if there were awareness programmes available to increase my knowledge	Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	.265**

I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	.372**
Cybersecurity awareness programmes are important for me	Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	.395**

5.4 Discussion pertaining to H2

Cybersecurity awareness programmes motivate e-commerce consumers to transact cautiously in order to enhance their security and privacy, which increases consumer confidence.

A study by Shah and Agarwal (2020) states that sufficient motivation is required in order for a person to exhibit the relevant cybersecurity behaviour supported by their decision making ability and relevant prompts to support their actions. The findings on of this study also indicate that consumer decisions are influenced through the messages communicated by cybersecurity awareness programmes. The results of this study highlight quite a high number of respondents who agreed that cybersecurity awareness messages seen on e-commerce platforms inform their actions with 75.2% of respondents agreeing to that particular item. A study

by van Bavel et al. (2019) similarly tested whether consumers navigated safely while making purchases online by providing them with coping messages while shopping online as part of an experiment. This study found that participants who were exposed to these coping messages opted to rather drop out of the experiment to purchase online rather than continue with their purchase. This could occur even when e-commerce consumers are exposed to coping messages because consumers are wary when transacting. In line with this study the participants indicated that their actions were informed by the messages they were exposed to. It must be noted that this item is tabled in item 16.1, which dealt with security awareness programmes seen by consumers on the e-commerce platforms and the actions they take post seeing these messages. Therefore, their actions could result in them either continuing with the transactions cautiously, completely ignoring what the message advised or instilling fear in the customer and they completely abandon the transaction. The Theory of planned behaviour suggests that peoples normative beliefs inform which actions they take based on motivating factors, which may be presented to them (Ajzen, 1991). Messages communicated by the cybersecurity awareness programmes on e-commerce platforms could motivate them to act securely as the fear of being victims of cybercrime becomes eminent.

On the contrary, item 16.2, which makes a reference to decisions taken by consumers when transacting on e-commerce platforms post receiving cybersecurity awareness messages not on the e-commerce platform itself. 53% of respondents agreed that these messages informed their transacting decisions while 26% strongly agreed. A low number of participants strongly disagreed and disagreed. 1.2% and 9.2% respectively. There is a notable difference in

cybersecurity messages that are communicated on the e-commerce platform itself and off the platform where the most influence in terms of agreements resulted from messages communicated outside of the platform. Literature on the theory of planned behaviour indicates that self efficacy is based on the influences which are received in preparation for performing certain actions and or making certain choices.(Ajzen, 1991). This is suggests that the messages received as indicated in item 16.2 are more effective than those seen on e-commerce platforms. Item 16.5 on the other hand addresses whether e-commerce consumers actually read the messages they see on e-commerce platforms, 42.4% and 33% agreed and strongly agreed respectively. This suggests that the remainder of respondents who represented 2% and 12% whom strongly disagreed and disagreed may not engage with cybersecurity awareness programmes.

Items 16.3 and 16.4 are statements used to understand and measure whether cybersecurity awareness programmes instils confidence in e-commerce consumers or not. Respondents to item 16.3 indicate that 50% agree while 31.2% strongly agreed with this statement. This is a significant amount of overall agreement. Item 16.4 also had a strong rate of agreement at 53% and 30.4% strongly agreeing in terms of responses.

The Bivariate correlation performed on the ordinal data showed positive values to indicate directly proportional relationship between the variables and a negative value indicates an inverse relationship. All significant relationships are indicated by a * or **.

There are positive correlations between the below tabulated statements. This is directly related proportionality. The overall responses of the participants on all items under this section of the survey appear to be positive, which is consistent with the using “Nudges” coping messages to motivate and influence the consumers to mitigate against eminent cyber threats.

Table 23: H2 correlations

Statement	Correlating statement	Correlation score
The security awareness messages I see on e-commerce platforms inform my actions	Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime (Motivation)	.334**
	I would shop more online if there were awareness programmes available to increase my knowledge	.281**
	I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	.335**

	I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	.363**

5.4.1 Consumer confidence: Security & Privacy

This item generally had high scores where consumers indicated that they are aware of how to maintain their privacy to ensure that their data is secure online. Khan (2019) States that security is one of the most important aspects, which prevent consumers from engaging with e-commerce platforms. When transacting online, consumers must provide their personal identifiable information in order to make payments in the era of identity theft and misrepresentation. Furthermore Khan (2019)found that it is the responsibility of the e-commerce platform to ensure security and data protection for their customers. This finding is consistent with the findings of this study in item 18.1 where consumers agree that they are made aware of how their privacy is protected when transacting on e-commerce platforms to ensure that their data is secure. This is demonstrated in the table below. Muneer et al. (2018) States that in todays connected world it is very easy to pry on an e-commerce consumer's computer. The study by Muneer et al. (2018) which attempted to provide a view of privacy for e-commerce and possible solutions suggests that consumers are aware that although e-commerce platforms state that they will protect the users data this is not always the case. This may be contained in their privacy policies which forms part of awareness

programmes according to Hueca et al. (2020). There are issues with use of personal identifiable data by third parties and security breach issues placing consumers at continuous risk. The protection motivation theory posits that people have an intention to act in a particular manner based on what they know i.e. coping messages that they may have been exposed to. (van Bavel et al., 2019) Norman et al. (2015) states that the protection motivation theory is based on fear appeals and their influence on behaviour. Fear appeals could come in the form of warning messages such as those communicated by cybersecurity awareness programmes encouraging consumers to be aware, and how to ensure that they protect themselves from the adverse effects that could come as a result of cyberattacks. Therefore, when fear is invoked consumers may be motivated to behave in the manner directed by the e-commerce platform. (Norman et al., 2015) where there is a lack of security e-commerce growth is slowed down due to a lack of consumer confidence. (Ruppel et al., 2003). Therefore, it becomes pertinent to ensure that consumers are aware of what they should do to ensure that their privacy and security is maintained when the responsibility rests with them, however the e-commerce platforms equally have a responsibility to make consumers aware of how they ensure security and privacy. Consistently the results in the study from item 18.1 to 18.3 have a significantly higher response rate of agreement. Furthermore item 18.2 has a 86.4% rate of agreement with respondents agreeing that it is true that Cybersecurity awareness programmes inform them about their responsibility towards maintaining their privacy. This is consistent with the literature as Bakar et al., (2013) stated that consumer behaviour should be of a responsible and secure nature, which demonstrates that they are knowledgeable about their role while participating in e-commerce. The

scoring of these items is an indication that when consumers are made aware of how their data is protected, their responsibility towards maintaining privacy and when privacy becomes a priority then security is deemed to being taken seriously by the e-commerce platform consumers which may result in them having confidence in the e-commerce platform as stated by (Ruppel et al., 2003). According to Lu (2009), consumer confidence increases when the privacy and security of consumers is taken seriously which has a direct influence on transacting confidence of consumers. On the contrary, item 18.1 had a false response rate of 18.8%, which suggests that some e-commerce platforms are still lagging behind and have not implemented awareness programmes, or the awareness programmes that have been implemented are not effective in driving the necessary awareness in order to avoid adverse consequences for their platforms.

5.5 Conclusion

This chapter discussed the results of this research in relation to the defined hypotheses with reference to various studies in literature to place an emphasis on findings in support, similar or contradictory to the results. The data was collected from 250 respondents who voluntarily participated and indicated that they participate in e-commerce in South Africa. The results revealed that e-commerce consumers are influenced by cybersecurity awareness programmes to make decisions when transacting however, their confidence is reliant of the platforms ability to secure their information and ensure privacy. The results further revealed that cybersecurity awareness programmes build consumer confidence

when they communicate relevant information pertaining to security and privacy and provide the relevant motivation to consumers in the form of messages to assist them with making informed decisions when transacting especially where their PII is concerned. The preceding chapter will conclude the study results with reference to the research questions posed and make recommendations for further studies also bearing in mind the shortcomings identified in this study.

CHAPTER 6. Conclusions & Recommendations

6.1 Introduction

The purpose of this chapter is to provide a summary of the conclusions drawn from the results of this study about the hypotheses and to provide an answer to the main research question and the sub research question. The conclusions will be categorized per hypothesis followed by answers specifically to the research questions posed. The results will be rationalised in accordance with which research question they are answering. Recommendations are provided based on the answers to the research questions and findings of this study and subsequently areas for further research identified.

6.2 Deductions

The objective of this study was to explore the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa. In order to explore the role of cybersecurity awareness programmes on e-commerce consumer confidence the following unknown elements were explored: consumer confidence, in relation to motivation, consumer confidence in relation to privacy, and security and cybersecurity awareness programmes. The research question posed was aimed at exploring to what extent cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms. This question plays a fundamental role in providing insights into how cybersecurity awareness programmes play a role in building consumer confidence for transacting on e-commerce platforms. While the study's sub question was about, how cybersecurity awareness programmes influence e-

commerce consumer confidence. This sub question the sub question was about explored how these programmes influence e-commerce consumer behaviour when transacting through the messages they communicate. The responses to these research questions are provided in the section analysis in the results chapter. The study's Post literature review and the results of this study enabled the following conclusions to be reached:

6.2.1 Conclusions regarding Hypothesis 1

The results of this study shows high levels of agreement in all statements where cybersecurity awareness programmes were tested. Average overall level of agreement for Q19.1 to Q19.5 is 75% and Q19.6 has an overall level of agreement of 84%, which emphasizes that over and above the consumers being influenced, they also believe in the importance of cybersecurity awareness programmes. Subsequently being a positive influence as these programmes are aimed at promoting and increasing awareness of cybercrime and to enable consumers to ensure safe practices and behaviours online. These findings were supported by the literature review. A study by Muhirwe and White (2016) found in their study that cybersecurity awareness has a significant effect on security behaviours. Contradictory to this study (Bada et al., 2019) stated that it is simplistic to merely provide awareness programmes and think that behaviour will change , it is simply not the case as understanding of the material being consumed has not been confirmed. There is a concern about the 15.4% of respondents who disagreed that they acknowledge and read cybersecurity awareness messages as human beings are the weakest link as far as cybersecurity is concerned and reputational damage to platforms may be because of cybercrime being experienced on a platform. This is a growing

concern that must be continuously addressed through various relevant and appropriate interventions.

In a study by van Bavel et al. (2019) which experimented by applying the PMT it was found that those that were exposed to coping messages were influenced to behave securely online and this is one of the positive outcomes which cybersecurity awareness programmes are to achieve in order to drive the cybersecurity agenda. This is consistent with the result of this study on item 19.3 where 74.4% of e-commerce consumers who agreed that they remember the learnings of cybersecurity awareness programmes when making purchases online. While (van Bavel et al., 2019) in their study about using nudges to improve security behaviour found that some consumers completely abandon their purchases when exposed to awareness programmes of any sort. Therefore, it may also be concluded that security awareness programmes communicate messages, which could have an adverse impact on consumers rather than the desired impact or instilling confidence when making purchases on e-commerce.

Due to the high response rate on this section of the survey, this hypothesis is accepted.

6.2.2 Conclusions regarding Hypothesis 2

Hong and Furnell (2021) State that when an organisation takes information security seriously this promotes consumer confidence. While Li et al. (2019) study on cybersecurity awareness policies and their impact on employees found that when the organisations environment is pro information security employees are positively influenced in terms of how they deal with their perceived threat and the actual threat which results in compliant cybersecurity behaviour. To support this

finding this study's results on item 18.1 had an overall score of 81.2% of respondents selecting that it was true that they were made aware of how their privacy is protected when transacting on e-commerce platforms. This indicates that these respondents could be positively influenced to trust that the platform has their best interests at heart. Bakar et al. (2013) Contradicted this by concluding that it is the responsibility of the consumer to ensure that they educate themselves regarding security and privacy so as to not become victims of cybercrime. However, this study is about demonstrating that it is also not solely the consumers' responsibility and when e-commerce platforms ensure that they participate in ensuring that they make their consumers aware they build consumer confidence it may result in boosting their sales.

In a study by (Lu, 2009) it is indicated that the manner in which consumer transaction data is protected which contains consumer PII must be explained to consumers. While (Smith, 2004) concluded that it is imperative for organisations to declare their privacy and security measures in order to build a relationship of trust with consumers which results in consumer confidence. These communications from part of the cybersecurity awareness programmes. Consistent with the correlation analysis done for this study it may be concluded that cybersecurity awareness programmes do indeed communicate by making consumers aware of cyber threats and cybercrime and how their privacy is protected when transacting online with a P-value of 0.059. while (Van Niekerk, 2017) found that cybersecurity awareness programmes must not be generic as they could potentially have no effect on the individuals consuming them and should much rather be targeted.

The results of this study are consistent with literature considering the following correlating statements. “I would shop more online if there were awareness programmes available to increase my knowledge”, which, correlated with the following statement “Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms” statistically showed a significant relationship between the two with a significant p- value score of .266 which is less than 0.05 therefore resulting in the hypothesis being supported.

6.3 Research Questions

To what extent does cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms?

To answer the research question the results of this study show that the role of cybersecurity awareness programmes is to influence consumers to make decisions with awareness of cybercrime as they transact on e-commerce platforms. This is related to their behaviour and alertness when transacting online. The extent has not been quantified but articulated in terms of the influence, which is evident in the results of this study. Consumers have indicated that cybersecurity awareness programmes increase their level of confidence for transacting on e-commerce platforms, this is validated in the results by the performing a chi square test of independence to determine whether there was a statistically significant relationship between the variables where p value of > 0.05 was obtained.

The P-value between “Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms” and “Cybersecurity awareness programmes inform me about how to ensure that my data is secure

online” is 0.002. This indicates that when consumers are informed about the measures they need to take to ensure that their data is secure online had a significant impact on how consumers viewed the manner in which cybersecurity awareness programmes increased their level of confidence for transacting on e-commerce platforms. The results further showed that with awareness programmes in place consumers would shop more. This shows that the presence of awareness programmes has an influence on the consumers’ decision to shop more on e-commerce platforms. This is a positive implication for e-commerce platform owners. There is limited research on the extent to which consumer confidence is built by cybersecurity awareness programmes. In order to address this shortcoming this study received a response rate of 81.2% from respondents who indicated that they are made aware of how their privacy is protected when transacting on e-commerce platforms.

Other scholars studied the trust construct and concluded that when consumers trust then they become confident when shopping on that particular platform (Smith, 2004). Khan (2019) Also, found that e-commerce websites have the responsibility to provide information security and privacy of their consumers. While (Smith, 2004) found that by increasing awareness of security and privacy will increase consumer confidence in dealing with the eminent risks associated with making purchases online as more and more consumers are on the lookout for platforms that exude a sense of care towards their privacy and security. The National institute of standards and technology (NIST) framework provides guidelines on how awareness programmes may be developed. This must be done in conjunction with addressing specific audiences such as e-commerce consumers to avoid the development of generic programmes which have no

effect on the target audience (Van Niekerk, 2017). Which is a shortcoming that was identified in literature where it is not specific as to the extent to which consumer confidence is built. The SANS report also provides insights on what successful security awareness programmes got right. (Lance Spitzner 2019)

1. **The sub question fundamental to this research;** *How do cybersecurity awareness programs aimed at consumers influence their confidence to make purchases on e-commerce platforms?*

- By deploying awareness programmes on the platforms themselves to influence consumer actions through the messages communicated by cybersecurity awareness programmes. The results of this study had a high response rate as far as participants who agreed that cybersecurity awareness messages seen on e-commerce platforms inform their actions with 75.2% of respondents agreeing to that particular item. The results of a similar study by van Bavel et al. (2019) proved to have similar results where users chose to abandon their online transacting due to being exposed to coping messages. Bada et al. (2019) states that by providing security awareness campaigns which are easily understood by the audience is important as well as ensuring that the content is easy to apply and for the motivation to behave appropriately in the face of the treat exists. This is important for owners of e-commerce platforms to understand so that they deploy engaging content, which influences consumers positively and motivates them to conclude their transactions on the e-commerce platform.

- Therefore in answering the research question the following correlation was made ,“I would shop more online if there were awareness programmes available to increase my knowledge “ had a significant correlation with “Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms “. This suggests that for the fact that there are cybersecurity awareness programmes deployed on an e-commerce platform consumer’s level of confidence increases resulting in positive outcomes for owners of these platforms. A shortcoming that was identified was that the type of cybersecurity programmes as well as their content was not defined which requires further research

6.4 Recommendations

- The results of this study may be used to facilitate further understanding of what is required and is deemed important to e-commerce consumers when shopping online. Specifically looking at item 18.1 consumers indicated that they are made aware of how their privacy is protected however an extention to the question is recommended to understand what aspects of privacy which are communicated increase their confidence when making purchases on e-commerce platforms.

- This study may expand its scope to outside of the Gauteng province and add more variables to explore for a broader view to the issue at hand.

- It may also be used by e-commerce platform owners to understand what is important to the consumers as far as cybersecurity is concerned in relation to the variables tested in this study and it is recommended that more variables may be studies in order to broarden the view and ensure

that all types of consumers are catered for. Like any other scholarly study this study has limitations and did not take into consideration moderating variables i.e. Gender, Age, level of education, income bracket, and duration of e-commerce experience and how they contribute to the role which cybersecurily awareness plays in building consumer confidence.

- It is recommended that this research must be expanded to include why cybersecurity awareness programmes are at times not acknowledged and read by e-commerce consumers, how as well as when would be the most appropriate time to expose these messages to consumers.
- It is a recommendation that the SEM model be revised in terms of the measured variables constituting the latent variables to improve factor loadings.

- It is recommended to extend the scope of this research to understand what type of messages contained in cybersecurity awareness programmes cause what type of actions in consumers in order to aid e-commerce platform owners to place only relevant messages, which will be impactful on their platforms.
- This study only explored some factors which may have a role in building e-commerce consumer confidence, other factors may be added to widen the scope and add to the growing body of knowledge regarding cybersecurity awareness programmes and their role
- It is recommended that this study be exposed to a larger sample size in order to ensure generalization as the sample size is not representative of the entire South African e-commerce consumer population
- This research used a set of questions per variable to measure the outcomes. Specific questions may be asked directly about the variables to gather specific consumer views

6.5 Suggestions for further research

Further research must be conducted on;

- Factors which are deemed to be motivating to consumers to engage in cybersecurity awareness programmes
- Which factors influence consumers to willingly engage with cybersecurity awareness programmes?
- The implications of not making consumers aware of how their privacy and security is protected by e-commerce platforms
- What type of awareness programmes are appropriate for e-commerce consumers
- What are the factors which are considered by e-commerce platform owners before deploying a cybersecurity awareness programme

6.6 Conclusion

In conclusion, this study set out to explore the role of cybersecurity awareness programmes in building consumer confidence when transacting on e-commerce platforms in South Africa. Firstly, consumers need to be made aware that the messages they see on e-commerce platforms related to cybersecurity awareness are indeed cybersecurity awareness programmes aimed at playing a particular role i.e. making consumers aware of cybercrime, protection mechanisms they can use to avoid becoming a victim of cybercrime. As indicated by the study by (Deloitte, 2015) Human beings remain the weakest link against the growing threat of cybercrime. It is therefore imperative for cybersecurity awareness programmes to play a significant role in influencing consumer behaviour to transact more cautiously to reduce the effects of cybercrime on e-commerce as a growing business sector within the South African Economy. This chapter concluded the study by incorporating literature and the findings of the study to answer the

research questions and provided recommendations for future research based on the findings.

REFERENCES

Abbad, M., Abbad, R., & Saleh, M. (2011). Limitations of e-commerce in developing countries: Jordan case. *Education, Business and Society: Contemporary Middle Eastern Issues*.

Aggarwal, R., & Ranganathan, P. (2019). Study designs: part 2–descriptive studies. *Perspectives in clinical research, 10*(1), 34.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bakar, E. A., Chang, L. L., & Saidin, A. Z. (2013). Knowledge, attitude and practices of consumers in e-commerce transactions. 2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M),

Bandara, R., Fernando, M., & Akter, S. (2020). Privacy concerns in E-commerce: A taxonomy and a future research agenda. *Electronic Markets, 30*(3), 629-647.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety, 15*(1), 48-64.

Cooper, D., & Schindler, P. (2014). Business Research Methods.© The McGraw−Hill Companies. *New York*.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic commerce research and applications, 2*(3), 203-215.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Dan, C. (2014). Electronic commerce: state-of-the-art. *American Journal of Intelligent Systems, 4*(4), 135-141.

Davis, L. (2019). *What does the current South African ecommerce landscape look like?* Flicker Leap. https://flickerleap.com/south-african-ecommerce-landscape/

Deloitte. (2015). The Deloitte consumer review. Consumer data under attach: The growing threat of cybercrime

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: a synergy approach. *Case Stud. Inf. Warf. Secur. Res. Teach. Stud, 1*.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal, 5*(6), 00149.

Falahat, M., Lee, Y.-Y., Foo, Y.-C., & Chia, C.-E. (2019). A model for consumer trust in e-commerce. *Asian Academy of Management Journal, 24*(2), 93-109.

Fisher, M. J., & Marshall, A. P. (2009). Understanding descriptive statistics. *Australian critical care, 22*(2), 93-97.

Girsang, M. J., Hendayani, R., & Ganesan, Y. (2020). Can Information Security, Privacy and Satisfaction Influence The E-Commerce Consumer Trust? 2020 8th International Conference on Information and Communication Technology (ICoICT),

Government, S. A. (2021). Cybercrimes Act 19 of 2020 [Act].

Gundu, T., Maronga, M. I., & Boucher, D. (2019). Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace. Proceedings of 4th International Conference on the,

Gupta, A. (2014). E-Commerce: Role of E-Commerce in today's business. *International Journal of Computing and Corporate Research, 4*(1), 1-8.

Gupta, R., & Agarwal, S. (2017). A Comparative Study of Cyber Threats in Emerging Economies. *Globus: An International Journal of Management & IT, 8*(2), 24-28.

Gurung, A., Luo, X., & Raja, M. (2008). An empirical investigation on customer's privacy perceptions, trust and security awareness in E-commerce environment. *Journal of Information Privacy and Security, 4*(1), 42-60.

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications, 57*, 102710.

Hueca, A., Manley, B., & Rogers, L. (2020). *Building a Cybersecurity Awareness Programme*.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(2), 85-105.

Khan, M., Xu, X., Dou, W., & Yu, S. (2016). OSaaS: Online shopping as a service to escalate E-commerce in developing countries. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS),

Khan, S. W. (2019). Cyber security issues and challenges in E-commerce. Proceedings of 10th international conference on digital strategies for organizational success,

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 52*(1), 29-41.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Lance Spitzner , D. d., Alyssa Ideboen, Dr. Heng Xu, Dr. Nan Zhang, Hannah Andrews, Adefunke Sonaike. (2019). *2019 SANS Security Awareness Report* [Security awareness report](The rising era of awareness training, Issue.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.

Lu, S. (2009). On consumer confidence in the online store. Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009),

Mcanyana, W., Brindley, C., & Eedat, Y. (2020). INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA. Accenture. https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf#zoom=50

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin, 18*(1), 3-9.

Malapane, T. A. (2019). A risk analysis of e-commerce: A case of South African online shopping space. 2019 Systems and Information Engineering Design Symposium (SIEDS),

Mashiane, T., Dlamini, Z., & Mahlangu, T. (2019). A rollout strategy for cybersecurity awareness campaigns. Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa,

Matbouli, H., & Gao, Q. (2012). An overview on web security threats and impact to e-commerce success. 2012 International Conference on Information Technology and e-Services,

Muhirwe, J., & White, N. (2016). CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems, 17*(2).

Muneer, A., Razzaq, S., & Farooq, Z. (2018). Data Privacy Issues and Possible Solutions in E-commerce. *Journal of Accounting & Marketing, 7*(3), 1000294.

Munjal, S. (2016). Cyber Crimes–Threat for the e-commerce. *Journal of Maharaja Agrasen College of Higher Education, 3*(1).

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General cyberspace: Cyberspace and cyber-enabled spaces. *IEEE Internet of Things Journal, 5*(3), 1843-1856.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. *Predicting and changing health behavior*, 70-106.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Ruppel, C., Underwood-Queen, L., & Harrington, S. J. (2003). E-Commerce: The roles of trust, security, and type of e-commerce involvement. *e-Service, 2*(2), 25-45.

Schindler, P. S. (2019). *Business Research Methods* (13th ed.). McGraw-Hill/Irwin.

Shah, P. R., & Agarwal, A. (2020). Cybersecurity Behaviour of Smartphone Users Through the Lens of Fogg Behaviour Model. 2020 3rd International Conference on Communication System, Computing and IT Applications (CSCITA),

Singh, S., & Silakari, S. (2009). A survey of cyber attack detection systems. *International Journal of Computer Science and Network Security, 9*(5), 1-10.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review*.

Sürücü, L., & MASLAKÇI, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal, 8*(3), 2694-2726.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*(6), 1273-1296.

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.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication, 20*, 113-132.

Yaseen, H., Alhusban, M. d., Alhosban, A., & Dingley, K. (2017). Making Sense of E-Commerce Customers Awareness in a Developing Country Context: A Framework for Evaluation. *Electronic Journal of Information Systems Evaluation, 20*(2), pp102-115-pp102-115.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR), 54*(1), 1-39.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, 1-16.

APPENDIX A: RESEARCH INSTRUMENT

Dear Participant,

My name is Grace Tsholofelo Lebogo and I am a Masters student at the University of the Witwatersrand Business School in Johannesburg.

Part of my studies require me to undertake a research project. My research project is to explore the role of cybersecurity awareness programmes in building e-commerce consumer confidence in South Africa under the supervision of Dr Kiru Pillay.

Cybersecurity awareness programmes in the context of this study refer to programmes, which are specifically designed to educate users on the dangers of, and appropriate behaviours and practices to adopt, when transacting on e-commerce platforms. For example messages about phishing, online fraud scams, etc.

For the purpose of this study, e-commerce refers to the use of any technology-enabled device, which is connected to the internet for the purchase of goods and services.

The objective of this study is to investigate whether consumer confidence would improve / increase on e-commerce platforms if there were awareness programmes. As part of this project, I would like to invite you to participate in answering a survey, which will take approximately 10 minutes. This research

project will not put you at risk or compromise your personal information in any manner. Your participation will be anonymous and no personal information will be requested from you. There are no costs involved for you to participate in this study.

Your participation is voluntary and you may at any point during the completion of this survey choose to withdraw from it. There will be no penalties. You may only complete the survey once.

I kindly request that you complete the survey by 20th of February 2022

Should you have questions about this survey or the study please feel free to contact me on the following details: 1785892@students.wits.ac.za.

Yours sincerely

Grace Tsholofelo Lebogo 060 870 7013

Dear Participant,

My name is Grace Tsholofelo Lebogo and I am a Masters student at the University of the Witwatersrand Business School in Johannesburg. Part of my studies require me to undertake a research project. My research project is to investigate whether cybersecurity awareness programmes build consumer confidence when transacting on e-commerce platforms in South Africa under the supervision of Dr Kiru Pillay. The objective of this study is to investigate whether

consumer confidence would improve / increase on e-commerce platforms if there were awareness programmes.

As part of this project, I would like to invite you to participate in answering a survey, which will take approximately 10-15 minutes.

This research project will not put you at risk or compromise your personal information in any manner. Your participation will be anonymous and no personal information will be requested from you. There are no cost involved for you to participate in this study. Your participation is voluntary and you may at any point during the completion of this survey choose to withdraw from it. There will be no penalties. You may only complete the survey once.

Should you have questions about this survey or the study please feel free to contact me on the following details: 1785892@students.wits.ac.za.

Yours sincerely Grace Tsholofelo Lebogo
060 870 7013

Consent

I agree to voluntarily participate in the following research study:
Understanding cybersecurity awareness programmes in building E-commerce consumer confidence in South Africa.

I understand my right as a participant to choose to withdraw my participation for whatever reason at any point and will not be subjected to any form of discrimination, penalties or any level of prejudice as a result.

I understand that my submission will be treated with confidentiality and will not be used for any other purpose except for the purpose of this study and all data provided will be anonymous.

I consent ☐

I do not consent ☐

I participate in e-commerce by making purchases on e-commerce platforms in South Africa

YES ☐

No ☐

Please select the appropriate answer which applies best to you in relation to the below attributes.

Consumer confidence: Motivation

Statement	Strongly Agree	Agree	Not sure	Strongly disagree	Disagree
The security awareness messages I see on e-commerce platforms					

inform my actions					
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms					
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms					
with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce					

I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email					

Consumer confidence: Security & Privacy

Statement	True	False
I'm made aware of how my privacy is protected when transacting on e-commerce platforms		
Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		
Cybersecurity awareness programmes inform me about how to ensure that my data is secure online		

Cybersecurity awareness programmes

Statement	Strongly Agree	Agree	Not sure	Strongly disagree	Disagree
Cybersecurity awareness					

programmes are effective in making me aware of cyber threats and cybercrime					
I would shop more online if there were awareness programmes available to increase my knowledge					
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases					
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform					
I acknowledge and read the cybersecurity awareness messages I receive to increase my					

level of cybersecurity awareness.					
Cybersecurity awareness programmes are important for me					

APPENDIX B: CORRELATIONS

Correlations													
			The security awareness messages I see on e-commerce platforms inform my actions	The security awareness messages I am sent inform my transacting decisions on e-commerce platforms	Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce	I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime	I would shop more online if there were awareness programmes available to increase my knowledge	I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	Cybersecurity awareness programmes are important for me
Spearman's rho	The security awareness messages I see on e-commerce platforms inform my actions	Correlation Coefficient	1.000										
		Sig. (2-tailed)											
		N	250										
	The security awareness messages I am sent inform my transacting decisions on e-	Correlation Coefficient	.709**	1.000									
		Sig. (2-tailed)	0.000										
		N	250	250									

	commerce platforms												
	Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Correlation Coefficient	.415**	.385**	1.000								
		Sig. (2-tailed)	0.000	0.000									
		N	250	250	250								
	with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce	Correlation Coefficient	.435**	.411**	.663**	1.000							
		Sig. (2-tailed)	0.000	0.000	0.000								
		N	250	250	250	250							
	I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Correlation Coefficient	.247**	.252**	.235**	.364**	1.000						
		Sig. (2-tailed)	0.000	0.000	0.000	0.000							
		N	250	250	250	250	250						
	Cybersecurity awareness	Correlation Coefficient	.334**	.369**	.362**	.490**	.346**	1.000					
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000						

	programmes are effective in making me aware of cyber threats and cybercrime	N	247	247	247	247	247	247					
	I would shop more online if there were awareness programmes available to increase my knowledge	Correlation Coefficient	.281**	.204**	.265**	.312**	.314**	.226**	1.000				
		Sig. (2-tailed)	0.000	0.001	0.000	0.000	0.000	0.000					
		N	247	247	247	247	247	247	247				
	I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Correlation Coefficient	.277**	.284**	.372**	.393**	.251**	.486**	.250**	1.000			
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000				
		N	247	247	247	247	247	247	247	247			
	I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when	Correlation Coefficient	.335**	.283**	.198**	.378**	.356**	.363**	.275**	.428**	1.000		
		Sig. (2-tailed)	0.000	0.000	0.002	0.000	0.000	0.000	0.000	0.000			
		N	247	247	247	247	247	247	247	247	247		

	displayed at the time when I interact with the platform												
	I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	Correlation Coefficient	.363**	.333**	.345**	.409**	.453**	.510**	.358**	.516**	.536**	1.000	
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000		
		N	247	247	247	247	247	247	247	247	247	247	
	Cybersecurity awareness programmes are important for me	Correlation Coefficient	.339**	.262**	.323**	.395**	.337**	.365**	.343**	.376**	.330**	.552**	1.000
		Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
		N	247	247	247	247	247	247	247	247	247	247	247
**. Correlation is significant at the 0.01 level (2-tailed).													

APPENDIX C: CROSSTABULATIONS

CROSSTABS

/TABLES=Q16.1 Q16.2 Q16.3 Q16.4 Q16.5 Q19.1 Q19.2 Q19.3 Q19.4 Q19.5 Q19.6 BY Q18.1 Q18.2 Q18.3

/FORMAT=AVALUE TABLES

/STATISTICS=CHISQ

/CELLS=COUNT COLUMN

/COUNT ROUND CELL

/METHOD=EXACT TIMER(5).

											See line 54 for example
											All significant p-values have been highlighted
	N of Rows in Working Data File	250									
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.									

	Cases Used	Statistics for each table are based on all the cases with valid data in the specified range(s) for all variables in each table.									
Syntax		CROSSTABS /TABLES=Q16.1 Q16.2 Q16.3 Q16.4 Q16.5 Q19.1 Q19.2 Q19.3 Q19.4 Q19.5 Q19.6 BY Q18.1 Q18.2 Q18.3 /FORMAT=AVALUE TABLES /STATISTICS=CHISQ /CELLS=COUNT COLUMN /COUNT ROUND CELL									

		/METHOD=EXACT TIMER(5).									
Resources	Processor Time	00:00:01.41									
	Elapsed Time	00:00:01.62									
	Dimensions Requested	2									
	Cells Available	524245									
The security awareness messages I see on e-commerce platforms inform my actions * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											

Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
The security awareness messages I see on e-commerce platforms inform my actions	Strongly Disagree	Count	3	3	6						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	6.4%	1.5%	2.4%						

	Disagree	Count	9	15	24						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	19.1%	7.4%	9.6%						
	Not sure	Count	8	24	32						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	11.8%	12.8%						
	Agree	Count	21	102	123						

		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	44.7%	50.2%	49.2%						
	Strongly Agree	Count	6	59	65						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	12.8%	29.1%	26.0%						
Total		Count	47	203	250						
		% within I'm made aware of how my privacy is protected when	100.0%	100.0%	100.0%						

		transacting on e-commerce platforms									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	14.269[a]	4	0.006	0.007				This line is the Pearson's Chi Square Test. If the p-value (Asymptotic Significance (2-sided)) < 0.05, then it implies that there			

Likelihood Ratio	13.140	4	0.011	0.013				is a significant relationship between the variables.
Fisher-Freeman-Halton Exact Test	13.753			0.006				This line is the Fisher's Exact Test. If the p-value (Exact Sig. (2-sided)) < 0.05, then it implies that there
Linear-by-Linear Association	13.973[b]	1	0.000	0.000	0.000	0.000		is a significant relationship between the variables. (If > 0.05, there is no significant relationship.)

N of Valid Cases	250							**(These two tests are similar. You can use one of the two). <u>It is preferable to use the Fisher's test value</u>**			
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is 1.13.								**(Use the Chi Square value if the Fisher p-value is not available.)**			
b. The standardized statistic is 3.738.											
The security awareness messages I see on e-commerce platforms inform my actions * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											

Crosstab											
			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
The security awareness messages I see on e-commerce platforms inform my actions	Strongly Disagree	Count	1	5	6						
		% within Cybersecurity awareness programmes inform me about my	2.9%	2.3%	2.4%						

		responsibility towards maintaining my privacy									
	Disagree	Count	8	16	24						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	23.5%	7.4%	9.6%						
	Not sure	Count	9	23	32						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	10.6%	12.8%						

	Agree	Count	13	110	123						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	38.2%	50.9%	49.2%						
	Strongly Agree	Count	3	62	65						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	8.8%	28.7%	26.0%						
Total		Count	34	216	250						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	19.174[a]	4	0.001	0.001							
Likelihood Ratio	17.517	4	0.002	0.002							

Fisher-Freeman-Halton Exact Test	17.940			0.001							
Linear-by-Linear Association	14.698[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	250										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .82.											
b. The standardized statistic is 3.834.											
The security awareness messages I see on e-commerce platforms inform my actions * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											

			Cybersecurity awareness programmes inform me about how to ensure that my data is secure online		Total							
			False	True								
The security awareness messages I see on e-commerce platforms inform my actions	Strongly Disagree	Count	2	4	6							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	4.9%	1.9%	2.4%							
	Disagree	Count	6	18	24							

		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	14.6%	8.6%	9.6%						
	Not sure	Count	10	22	32						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	24.4%	10.5%	12.8%						
	Agree	Count	21	102	123						
		% within Cybersecurity awareness programmes inform me about how to	51.2%	48.8%	49.2%						

		ensure that my data is secure online									
	Strongly Agree	Count	2	63	65						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	4.9%	30.1%	26.0%						
Total		Count	41	209	250						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						

Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	16.152[a]	4	0.003	0.004							
Likelihood Ratio	18.446	4	0.001	0.001							
Fisher-Freeman-Halton Exact Test	18.431			0.001							
Linear-by-Linear Association	12.690[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	250										
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is .98.											

b. The standardized statistic is 3.562.											
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	1	2	3						

The security awareness messages I am sent inform my transacting decisions on e-commerce platforms	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	2.1%	1.0%	1.2%						
	Disagree	Count	10	13	23						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	21.3%	6.4%	9.2%						
	Not sure	Count	6	19	25						
		% within I'm made aware of how my privacy is protected when	12.8%	9.4%	10.0%						

		transacting on e-commerce platforms									
	Agree	Count	24	109	133						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	51.1%	53.7%	53.2%						
	Strongly Agree	Count	6	60	66						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	12.8%	29.6%	26.4%						

Total		Count	47	203	250						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	14.159[a]	4	0.007	0.010							
Likelihood Ratio	13.005	4	0.011	0.015							

Fisher-Freeman-Halton Exact Test	13.662			0.006							
Linear-by-Linear Association	12.937[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .56.											
b. The standardized statistic is 3.597.											
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms	Strongly Disagree	Count	0	3	3						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	1.4%	1.2%						

	Disagree	Count	8	15	23						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	23.5%	6.9%	9.2%						
	Not sure	Count	7	18	25						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	20.6%	8.3%	10.0%						
	Agree	Count	17	116	133						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	50.0%	53.7%	53.2%						
	Strongly Agree	Count	2	64	66						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	5.9%	29.6%	26.4%						
Total		Count	34	216	250						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	20.018[a]	4	0.000	0.003							
Likelihood Ratio	19.854	4	0.001	0.001							
Fisher-Freeman-Halton Exact Test	18.957			0.000							
Linear-by-Linear Association	14.774[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .41.											
b. The standardized statistic is 3.844.											
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
The security awareness messages I am sent inform my transacting decisions on e-commerce platforms	Strongly Disagree	Count	0	3	3							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	0.0%	1.4%	1.2%							
	Disagree	Count	7	16	23							
		% within Cybersecurity awareness programmes inform me about how to	17.1%	7.7%	9.2%							

		ensure that my data is secure online									
	Not sure	Count	9	16	25						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	22.0%	7.7%	10.0%						
	Agree	Count	22	111	133						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	53.7%	53.1%	53.2%						

	Strongly Agree	Count	3	63	66						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	7.3%	30.1%	26.4%						
Total		Count	41	209	250						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	17.665[a]	4	0.001	0.003							
Likelihood Ratio	18.465	4	0.001	0.001							
Fisher-Freeman-Halton Exact Test	17.433			0.001							
Linear-by-Linear Association	10.883[b]	1	0.001	0.001	0.001	0.000					
N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .49.											
b. The standardized statistic is 3.299.											

Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	0	2	2						

Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	1.0%	0.8%						
	Disagree	Count	8	5	13						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.0%	2.5%	5.2%						
	Not sure	Count	8	24	32						
		% within I'm made aware of how my privacy is protected when	17.0%	11.8%	12.8%						

		transacting on e-commerce platforms									
	Agree	Count	21	104	125						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	44.7%	51.2%	50.0%						
	Strongly Agree	Count	10	68	78						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	21.3%	33.5%	31.2%						

Total		Count	47	203	250						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	18.978[a]	4	0.001	0.001							
Likelihood Ratio	15.425	4	0.004	0.004							

Fisher-Freeman-Halton Exact Test	15.103			0.003							
Linear-by-Linear Association	10.071[b]	1	0.002	0.002	0.001	0.001					
N of Valid Cases	250										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .38.											
b. The standardized statistic is 3.173.											
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Strongly Disagree	Count	0	2	2						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	0.9%	0.8%						

	Disagree	Count	5	8	13						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	14.7%	3.7%	5.2%						
	Not sure	Count	10	22	32						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	29.4%	10.2%	12.8%						
	Agree	Count	13	112	125						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	38.2%	51.9%	50.0%						
	Strongly Agree	Count	6	72	78						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	17.6%	33.3%	31.2%						
Total		Count	34	216	250						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	19.043[a]	4	0.001	0.002							
Likelihood Ratio	15.993	4	0.003	0.003							
Fisher-Freeman-Halton Exact Test	16.268			0.001							
Linear-by-Linear Association	11.963[b]	1	0.001	0.001	0.001	0.000					

N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .27.											
b. The standardized statistic is 3.459.											
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
Cybersecurity awareness programmes increase my level of confidence for transacting on e-commerce platforms	Strongly Disagree	Count	0	2	2							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	0.0%	1.0%	0.8%							
	Disagree	Count	5	8	13							
		% within Cybersecurity awareness programmes inform me about how to	12.2%	3.8%	5.2%							

		ensure that my data is secure online									
	Not sure	Count	10	22	32						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	24.4%	10.5%	12.8%						
	Agree	Count	21	104	125						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	51.2%	49.8%	50.0%						

	Strongly Agree	Count	5	73	78						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	12.2%	34.9%	31.2%						
Total		Count	41	209	250						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	15.846[a]	4	0.003	0.005							
Likelihood Ratio	15.729	4	0.003	0.003							
Fisher-Freeman-Halton Exact Test	15.470			0.002							
Linear-by-Linear Association	12.126[b]	1	0.000	0.001	0.001	0.000					
N of Valid Cases	250										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .33.											
b. The standardized statistic is 3.482.											

with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	0	1	1						

with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	0.5%	0.4%						
	Disagree	Count	6	9	15						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	12.8%	4.4%	6.0%						
	Not sure	Count	7	17	24						
		% within I'm made aware of how my privacy is protected when	14.9%	8.4%	9.6%						

		transacting on e-commerce platforms									
	Agree	Count	23	111	134						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	48.9%	54.7%	53.6%						
	Strongly Agree	Count	11	65	76						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	23.4%	32.0%	30.4%						

Total		Count	47	203	250						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	7.504[a]	4	0.112	0.120							
Likelihood Ratio	6.770	4	0.149	0.166							

Fisher-Freeman-Halton Exact Test	7.367			0.103							
Linear-by-Linear Association	5.214[b]	1	0.022	0.023	0.016	0.006					
N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .19.											
b. The standardized statistic is 2.284.											
with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce	Strongly Disagree	Count	0	1	1						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	0.5%	0.4%						

	Disagree	Count	5	10	15						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	14.7%	4.6%	6.0%						
	Not sure	Count	9	15	24						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	6.9%	9.6%						
	Agree	Count	17	117	134						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	50.0%	54.2%	53.6%						
	Strongly Agree	Count	3	73	76						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	8.8%	33.8%	30.4%						
Total		Count	34	216	250						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	22.917[a]	4	0.000	0.000							
Likelihood Ratio	20.751	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	21.314			0.000							
Linear-by-Linear Association	17.471[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .14.											
b. The standardized statistic is 4.180.											
with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
with awareness programmes in place I feel empowered about the decisions I take when transacting on e-commerce	Strongly Disagree	Count	0	1	1							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	0.0%	0.5%	0.4%							
	Disagree	Count	5	10	15							
		% within Cybersecurity awareness programmes inform me about how to	12.2%	4.8%	6.0%							

		ensure that my data is secure online									
	Not sure	Count	12	12	24						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	29.3%	5.7%	9.6%						
	Agree	Count	20	114	134						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	48.8%	54.5%	53.6%						

	Strongly Agree	Count	4	72	76						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	9.8%	34.4%	30.4%						
Total		Count	41	209	250						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	30.183[a]	4	0.000	0.000							
Likelihood Ratio	26.476	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	26.726			0.000							
Linear-by-Linear Association	19.332[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .16.											
b. The standardized statistic is 4.397.											

I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	1	4	5						

I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	2.1%	2.0%	2.0%						
	Disagree	Count	11	19	30						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	23.4%	9.4%	12.0%						
	Not sure	Count	3	23	26						
		% within I'm made aware of how my privacy is protected when	6.4%	11.3%	10.4%						

		transacting on e-commerce platforms									
	Agree	Count	14	92	106						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	29.8%	45.3%	42.4%						
	Strongly Agree	Count	18	65	83						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	38.3%	32.0%	33.2%						

Total		Count	47	203	250						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	9.801[a]	4	0.044	0.042							
Likelihood Ratio	9.075	4	0.059	0.065							

Fisher-Freeman-Halton Exact Test	9.222			0.046							
Linear-by-Linear Association	1.047[b]	1	0.306	0.315	0.172	0.036					
N of Valid Cases	250										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .94.											
b. The standardized statistic is 1.023.											
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Strongly Disagree	Count	1	4	5						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	2.9%	1.9%	2.0%						

	Disagree	Count	9	21	30						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	9.7%	12.0%						
	Not sure	Count	9	17	26						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	26.5%	7.9%	10.4%						
	Agree	Count	11	95	106						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	32.4%	44.0%	42.4%						
	Strongly Agree	Count	4	79	83						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	11.8%	36.6%	33.2%						
Total		Count	34	216	250						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	23.196[a]	4	0.000	0.000							
Likelihood Ratio	20.897	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	21.532			0.000							
Linear-by-Linear Association	17.241[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .68.											
b. The standardized statistic is 4.152.											
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
I am more inclined to read cybersecurity awareness messages that I see on an e-commerce platform than those sent to me via email	Strongly Disagree	Count	1	4	5							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.4%	1.9%	2.0%							
	Disagree	Count	10	20	30							
		% within Cybersecurity awareness programmes inform me about how to	24.4%	9.6%	12.0%							

		ensure that my data is secure online									
	Not sure	Count	5	21	26						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	12.2%	10.0%	10.4%						
	Agree	Count	18	88	106						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	43.9%	42.1%	42.4%						

	Strongly Agree	Count	7	76	83						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	17.1%	36.4%	33.2%						
Total		Count	41	209	250						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	10.341[a]	4	0.035	0.035							
Likelihood Ratio	9.873	4	0.043	0.048							
Fisher-Freeman-Halton Exact Test	10.343			0.027							
Linear-by-Linear Association	8.677[b]	1	0.003	0.003	0.003	0.001					
N of Valid Cases	250										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .82.											
b. The standardized statistic is 2.946.											

Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	0	1	1						

Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	0.5%	0.4%						
	Disagree	Count	8	10	18						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.4%	5.0%	7.3%						
	Not sure	Count	7	26	33						
		% within I'm made aware of how my privacy is protected when	15.2%	12.9%	13.4%						

		transacting on e-commerce platforms									
	Agree	Count	18	104	122						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	39.1%	51.7%	49.4%						
	Strongly Agree	Count	13	60	73						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	28.3%	29.9%	29.6%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	9.531[a]	4	0.049	0.050							
Likelihood Ratio	8.146	4	0.086	0.092							

Fisher-Freeman-Halton Exact Test	8.632			0.059							
Linear-by-Linear Association	3.646[b]	1	0.056	0.061	0.037	0.012					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .19.											
b. The standardized statistic is 1.910.											
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime	Strongly Disagree	Count	0	1	1						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	0.5%	0.4%						

	Disagree	Count	8	10	18						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	24.2%	4.7%	7.3%						
	Not sure	Count	9	24	33						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	27.3%	11.2%	13.4%						
	Agree	Count	14	108	122						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	42.4%	50.5%	49.4%						
	Strongly Agree	Count	2	71	73						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	6.1%	33.2%	29.6%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	28.185[a]	4	0.000	0.000							
Likelihood Ratio	25.546	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	25.699			0.000							
Linear-by-Linear Association	24.624[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .13.											
b. The standardized statistic is 4.962.											
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
Cybersecurity awareness programmes are effective in making me aware of cyber threats and cybercrime	Strongly Disagree	Count	0	1	1							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	0.0%	0.5%	0.4%							
	Disagree	Count	10	8	18							
		% within Cybersecurity awareness programmes inform me about how to	25.6%	3.8%	7.3%							

		ensure that my data is secure online									
	Not sure	Count	11	22	33						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	28.2%	10.6%	13.4%						
	Agree	Count	15	107	122						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	38.5%	51.4%	49.4%						

	Strongly Agree	Count	3	70	73						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	7.7%	33.7%	29.6%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	37.844[a]	4	0.000	0.000							
Likelihood Ratio	32.743	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	32.738			0.000							
Linear-by-Linear Association	31.759[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .16.											
b. The standardized statistic is 5.636.											

I would shop more online if there were awareness programmes available to increase my knowledge * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	2	3	5						

I would shop more online if there were awareness programmes available to increase my knowledge	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	4.3%	1.5%	2.0%						
	Disagree	Count	8	17	25						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.4%	8.5%	10.1%						
	Not sure	Count	7	34	41						
		% within I'm made aware of how my privacy is protected when	15.2%	16.9%	16.6%						

		transacting on e-commerce platforms									
	Agree	Count	13	72	85						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	28.3%	35.8%	34.4%						
	Strongly Agree	Count	16	75	91						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	34.8%	37.3%	36.8%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	5.211[a]	4	0.266	0.263							
Likelihood Ratio	4.571	4	0.334	0.376							

Fisher-Freeman-Halton Exact Test	5.296			0.238							
Linear-by-Linear Association	2.480[b]	1	0.115	0.123	0.069	0.018					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .93.											
b. The standardized statistic is 1.575.											
I would shop more online if there were awareness programmes available to increase my knowledge * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
I would shop more online if there were awareness programmes available to increase my knowledge	Strongly Disagree	Count	1	4	5						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	1.9%	2.0%						

	Disagree	Count	2	23	25						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	6.1%	10.7%	10.1%						
	Not sure	Count	9	32	41						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	27.3%	15.0%	16.6%						
	Agree	Count	15	70	85						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	45.5%	32.7%	34.4%						
	Strongly Agree	Count	6	85	91						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	18.2%	39.7%	36.8%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	8.374[a]	4	0.079	0.077							
Likelihood Ratio	8.688	4	0.069	0.080							
Fisher-Freeman-Halton Exact Test	8.855			0.051							
Linear-by-Linear Association	1.992[b]	1	0.158	0.186	0.095	0.026					

N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .67.											
b. The standardized statistic is 1.412.											
I would shop more online if there were awareness programmes available to increase my knowledge * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
I would shop more online if there were awareness programmes available to increase my knowledge	Strongly Disagree	Count	1	4	5							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.6%	1.9%	2.0%							
	Disagree	Count	5	20	25							
		% within Cybersecurity awareness programmes inform me about how to	12.8%	9.6%	10.1%							

		ensure that my data is secure online									
	Not sure	Count	9	32	41						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	23.1%	15.4%	16.6%						
	Agree	Count	15	70	85						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	38.5%	33.7%	34.4%						

	Strongly Agree	Count	9	82	91						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	23.1%	39.4%	36.8%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	4.173[a]	4	0.383	0.373							
Likelihood Ratio	4.340	4	0.362	0.389							
Fisher-Freeman-Halton Exact Test	4.903			0.266							
Linear-by-Linear Association	3.067[b]	1	0.080	0.084	0.050	0.014					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .79.											
b. The standardized statistic is 1.751.											

I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases * I’m made aware of how my privacy is protected when transacting on e-commerce platforms

Crosstab											
			I’m made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	1	2	3						

I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	2.2%	1.0%	1.2%						
	Disagree	Count	8	23	31						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.4%	11.4%	12.6%						
	Not sure	Count	8	21	29						
		% within I'm made aware of how my privacy is protected when	17.4%	10.4%	11.7%						

		transacting on e-commerce platforms									
	Agree	Count	23	110	133						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	50.0%	54.7%	53.8%						
	Strongly Agree	Count	6	45	51						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	13.0%	22.4%	20.6%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	4.759[a]	4	0.313	0.314							
Likelihood Ratio	4.650	4	0.325	0.345							

Fisher-Freeman-Halton Exact Test	5.373			0.225							
Linear-by-Linear Association	4.188[b]	1	0.041	0.047	0.027	0.009					
N of Valid Cases	247										
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is .56.											
b. The standardized statistic is 2.046.											
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Strongly Disagree	Count	1	2	3						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	0.9%	1.2%						

	Disagree	Count	5	26	31						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	15.2%	12.1%	12.6%						
	Not sure	Count	7	22	29						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	21.2%	10.3%	11.7%						
	Agree	Count	18	115	133						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	54.5%	53.7%	53.8%						
	Strongly Agree	Count	2	49	51						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	6.1%	22.9%	20.6%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	8.078[a]	4	0.089	0.099							
Likelihood Ratio	8.645	4	0.071	0.073							
Fisher-Freeman-Halton Exact Test	9.137			0.045							
Linear-by-Linear Association	5.101[b]	1	0.024	0.029	0.018	0.007					

N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .40.											
b. The standardized statistic is 2.258.											
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
I remember the learnings of cybersecurity awareness programmes when making e-commerce purchases	Strongly Disagree	Count	2	1	3							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	5.1%	0.5%	1.2%							
	Disagree	Count	11	20	31							
		% within Cybersecurity awareness programmes inform me about how to	28.2%	9.6%	12.6%							

		ensure that my data is secure online									
	Not sure	Count	8	21	29						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	20.5%	10.1%	11.7%						
	Agree	Count	17	116	133						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	43.6%	55.8%	53.8%						

	Strongly Agree	Count	1	50	51						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.6%	24.0%	20.6%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	26.158[a]	4	0.000	0.000							
Likelihood Ratio	25.644	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	25.396			0.000							
Linear-by-Linear Association	25.160[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .47.											
b. The standardized statistic is 5.016.											

I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	1	4	5						

I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	2.2%	2.0%	2.0%						
	Disagree	Count	9	24	33						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	19.6%	11.9%	13.4%						
	Not sure	Count	3	24	27						
		% within I'm made aware of how my privacy is protected when	6.5%	11.9%	10.9%						

		transacting on e-commerce platforms									
	Agree	Count	25	98	123						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	54.3%	48.8%	49.8%						
	Strongly Agree	Count	8	51	59						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	17.4%	25.4%	23.9%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	3.874[a]	4	0.423	0.422							
Likelihood Ratio	3.928	4	0.416	0.467							

Fisher-Freeman-Halton Exact Test	3.904			0.391							
Linear-by-Linear Association	1.226[b]	1	0.268	0.296	0.153	0.034					
N of Valid Cases	247										
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is .93.											
b. The standardized statistic is 1.107.											
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	Strongly Disagree	Count	1	4	5						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	1.9%	2.0%						

	Disagree	Count	10	23	33						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	30.3%	10.7%	13.4%						
	Not sure	Count	3	24	27						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	9.1%	11.2%	10.9%						
	Agree	Count	15	108	123						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	45.5%	50.5%	49.8%						
	Strongly Agree	Count	4	55	59						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	12.1%	25.7%	23.9%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	10.844[a]	4	0.028	0.033							
Likelihood Ratio	9.437	4	0.051	0.060							
Fisher-Freeman-Halton Exact Test	9.813			0.033							
Linear-by-Linear Association	8.113[b]	1	0.004	0.005	0.004	0.002					

N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .67.											
b. The standardized statistic is 2.848.											
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
I read the cybersecurity messages that are communicated by the e-commerce platforms I shop on when displayed at the time when I interact with the platform	Strongly Disagree	Count	1	4	5							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.6%	1.9%	2.0%							
	Disagree	Count	15	18	33							
		% within Cybersecurity awareness programmes inform me about how to	38.5%	8.7%	13.4%							

		ensure that my data is secure online									
	Not sure	Count	2	25	27						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	5.1%	12.0%	10.9%						
	Agree	Count	15	108	123						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	38.5%	51.9%	49.8%						

	Strongly Agree	Count	6	53	59						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	15.4%	25.5%	23.9%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	25.931[a]	4	0.000	0.000							
Likelihood Ratio	20.714	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	20.572			0.000							
Linear-by-Linear Association	13.371[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .79.											
b. The standardized statistic is 3.657.											

I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness. * I'm made aware of how my privacy is protected when transacting on e-commerce platforms

Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	1	0	1						

I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	2.2%	0.0%	0.4%						
	Disagree	Count	10	27	37						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	21.7%	13.4%	15.0%						
	Not sure	Count	4	13	17						
		% within I'm made aware of how my privacy is protected when	8.7%	6.5%	6.9%						

		transacting on e-commerce platforms									
	Agree	Count	22	106	128						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	47.8%	52.7%	51.8%						
	Strongly Agree	Count	9	55	64						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	19.6%	27.4%	25.9%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	7.416[a]	4	0.115	0.124							
Likelihood Ratio	6.298	4	0.178	0.184							

Fisher-Freeman-Halton Exact Test	6.579			0.148							
Linear-by-Linear Association	4.321[b]	1	0.038	0.044	0.025	0.008					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .19.											
b. The standardized statistic is 2.079.											
I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness. * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	Strongly Disagree	Count	1	0	1						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	0.0%	0.4%						

	Disagree	Count	11	26	37						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	33.3%	12.1%	15.0%						
	Not sure	Count	6	11	17						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	18.2%	5.1%	6.9%						
	Agree	Count	15	113	128						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	45.5%	52.8%	51.8%						
	Strongly Agree	Count	0	64	64						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	29.9%	25.9%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	32.283[a]	4	0.000	0.000							
Likelihood Ratio	34.634	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	32.326			0.000							
Linear-by-Linear Association	26.748[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .13.											
b. The standardized statistic is 5.172.											
I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness. * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
I acknowledge and read the cybersecurity awareness messages I receive to increase my level of cybersecurity awareness.	Strongly Disagree	Count	1	0	1							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.6%	0.0%	0.4%							
	Disagree	Count	18	19	37							
		% within Cybersecurity awareness programmes inform me about how to	46.2%	9.1%	15.0%							

		ensure that my data is secure online									
	Not sure	Count	3	14	17						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	7.7%	6.7%	6.9%						
	Agree	Count	14	114	128						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	35.9%	54.8%	51.8%						

	Strongly Agree	Count	3	61	64						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	7.7%	29.3%	25.9%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	43.622[a]	4	0.000	0.000							
Likelihood Ratio	35.763	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	35.394			0.000							
Linear-by-Linear Association	37.522[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	247										
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .16.											
b. The standardized statistic is 6.125.											

Cybersecurity awareness programmes are important for me * I'm made aware of how my privacy is protected when transacting on e-commerce platforms											
Crosstab											
			I'm made aware of how my privacy is protected when transacting on e-commerce platforms		Total						
			False	True							
		Count	0	1	1						

Cybersecurity awareness programmes are important for me	Strongly Disagree	% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	0.0%	0.5%	0.4%						
	Disagree	Count	2	5	7						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	4.3%	2.5%	2.8%						
	Not sure	Count	5	15	20						
		% within I'm made aware of how my privacy is protected when	10.9%	7.5%	8.1%						

		transacting on e-commerce platforms									
	Agree	Count	19	84	103						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	41.3%	41.8%	41.7%						
	Strongly Agree	Count	20	96	116						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	43.5%	47.8%	47.0%						

Total		Count	46	201	247						
		% within I'm made aware of how my privacy is protected when transacting on e-commerce platforms	100.0%	100.0%	100.0%						
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	1.371[a]	4	0.849	0.822							
Likelihood Ratio	1.468	4	0.832	0.822							

Fisher-Freeman-Halton Exact Test	2.102			0.723							
Linear-by-Linear Association	.613[b]	1	0.434	0.461	0.246	0.060					
N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .19.											
b. The standardized statistic is .783.											
Cybersecurity awareness programmes are important for me * Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy											
Crosstab											

			Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy		Total						
			False	True							
Cybersecurity awareness programmes are important for me	Strongly Disagree	Count	1	0	1						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	3.0%	0.0%	0.4%						

	Disagree	Count	0	7	7						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	0.0%	3.3%	2.8%						
	Not sure	Count	10	10	20						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	30.3%	4.7%	8.1%						
	Agree	Count	17	86	103						

		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	51.5%	40.2%	41.7%						
	Strongly Agree	Count	5	111	116						
		% within Cybersecurity awareness programmes inform me about my responsibility towards maintaining my privacy	15.2%	51.9%	47.0%						
Total		Count	33	214	247						
		% within Cybersecurity awareness programmes inform me about my	100.0%	100.0%	100.0%						

		responsibility towards maintaining my privacy									
Chi-Square Tests											
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	39.847[a]	4	0.000	0.000							
Likelihood Ratio	33.005	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	31.671			0.000							
Linear-by-Linear Association	20.051[b]	1	0.000	0.000	0.000	0.000					

N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .13.											
b. The standardized statistic is 4.478.											
Cybersecurity awareness programmes are important for me * Cybersecurity awareness programmes inform me about how to ensure that my data is secure online											
Crosstab											
			Cybersecurity awareness programmes inform me about how to		Total					

			ensure that my data is secure online									
			False	True								
Cybersecurity awareness programmes are important for me	Strongly Disagree	Count	1	0	1							
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	2.6%	0.0%	0.4%							
	Disagree	Count	2	5	7							
		% within Cybersecurity awareness programmes inform me about how to	5.1%	2.4%	2.8%							

		ensure that my data is secure online									
	Not sure	Count	6	14	20						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	15.4%	6.7%	8.1%						
	Agree	Count	24	79	103						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	61.5%	38.0%	41.7%						

	Strongly Agree	Count	6	110	116						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	15.4%	52.9%	47.0%						
Total		Count	39	208	247						
		% within Cybersecurity awareness programmes inform me about how to ensure that my data is secure online	100.0%	100.0%	100.0%						
Chi-Square Tests											

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability					
Pearson Chi-Square	23.436[a]	4	0.000	0.000							
Likelihood Ratio	23.593	4	0.000	0.000							
Fisher-Freeman-Halton Exact Test	24.111			0.000							
Linear-by-Linear Association	19.228[b]	1	0.000	0.000	0.000	0.000					
N of Valid Cases	247										
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .16.											
b. The standardized statistic is 4.385.											

APPENDIX D: RELIABILITIES

/COMPRESSED.												
RELIABILITY										**Section**	**Number of Items**	**Cronbach's Alpha**
/VARIABLES=Q16.1 Q16.2 Q16.3 Q16.4 Q16.5									Q16	Consumer confidence: Motivation	5	0.747
/SCALE('ALL VARIABLES') ALL									Q18	Consumer confidence: Security & Privacy	3	0.635

/MODEL=ALPHA.									Q19	Cybersecurity awareness programmes	6	0.772
Reliability												
	N of Rows in Working Data File	250										
	Matrix Input											
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.										

	Cases Used	Statistics are based on all cases with valid data for all variables in the procedure.										
Syntax		RELIABILITY /VARIABLES=Q16.1 Q16.2 Q16.3 Q16.4 Q16.5 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA.										
Scale: ALL VARIABLES												

Case Processing Summary												
		N	%									
Cases	Valid	250	100.0									
	Excluded[a]	0	0.0									
	Total	250	100.0									
a. List wise deletion based on all variables in the procedure.												
Reliability Statistics												
Cronbach's Alpha	N of Items											

0.747	5											
RELIABILITY												
/VARIABLES=Q18.1 Q18.2 Q18.3												
/SCALE('ALL VARIABLES') ALL												
/MODEL=ALPHA.												
Reliability												
Notes												

	N of Rows in Working Data File	250										
	Matrix Input											
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.										
	Cases Used	Statistics are based on all cases with valid data for all variables in the procedure.										

Syntax		RELIABILITY /VARIABLES=Q18.1 Q18.2 Q18.3 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA.										
Scale: ALL VARIABLES												
Case Processing Summary												
		N	%									
Cases	Valid	250	100.0									

	Excluded[a]	0	0.0									
	Total	250	100.0									
a. Listwise deletion based on all variables in the procedure.												
Reliability Statistics												
Cronbach's Alpha	N of Items											
0.635	3											
RELIABILITY												

/VARIABLES=Q19.1 Q19.2 Q19.3 Q19.4 Q19.5 Q19.6												
/SCALE('ALL VARIABLES') ALL												
/MODEL=ALPHA.												
Reliability												
Notes												
Output Created												
Comments												

Input	Data											
	Active Dataset	DataSet0										
	Filter	<none>										
	Weight	<none>										
	Split File	<none>										
	N of Rows in Working Data File	250										
	Matrix Input											

Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.										
	Cases Used	Statistics are based on all cases with valid data for all variables in the procedure.										
Syntax		RELIABILITY /VARIABLES=Q19.1 Q19.2 Q19.3 Q19.4 Q19.5 Q19.6 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA.										

Resources	Processor Time	00:00:00.00										
	Elapsed Time	00:00:00.01										
Scale: ALL VARIABLES												
Case Processing Summary												
		N	%									
Cases	Valid	247	98.8									

	Excluded[a]	3	1.2									
	Total	250	100.0									
a. Listwise deletion based on all variables in the procedure.												
Reliability Statistics												
Cronbach's Alpha	N of Items											
0.772	6											

APPENDIX E: ETHICS CERTIFICATE

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

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

Ethics Clearance Certificate

Ethics protocol number: WBS/DB1785892/663
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Exploring the role of cybersecurity awareness programs in building e-commerce consumer confidence in South Africa
Investigator / Researcher	Ms Grace Lebogo
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.
Issue Date of Certificate	2021-11-25
Expiry date	Date of submission of the project report
Chairperson	Prof Anthony Stacey ☎ +27 11 717 3587 +27 82 880 4531 anthony.stacey@wits.ac.za

Declaration by Researcher

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

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

Signature

26/11/2021
Date: