



**Security practices of smartphone users at UKZN Westville
Campus and its effects on the Institutional Information Systems**

**By
Oluwafisayo Kaka
208513240**

**A dissertation submitted in fulfilment of the requirements for the degree of
Master of Commerce**

**School of Management, Information Technology and Governance
Discipline of Information Systems & Technology
In the 2021 Academic Year**

**Supervisor
Dr K. Naidoo**

DECLARATION

I, Oluwafisayo Kaka, declare that

- (i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.
- (ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.
- (iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
- (iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
 - a) Their words have been re-written but the general information attributed to them has been referenced;
 - b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.
- (v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.
- (vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

 07/07/2021
Signed: Date:

ACKNOWLEDGEMENTS

Gratitude to the All-Mighty God for the completion of this research. Special thanks to my supervisor Karunagaran Naidoo for his guidance, dedication, and patience during the span of this research. Achieving this research would have been impossible without you. Finally, to my parents and siblings, I am eternally grateful for your encouragement, understanding and support, especially in challenging moments of this study.

ABSTRACT

Technology has evolved through the years and brought about innovations in telecommunication tools such as smartphones, widely used today for various reasons, like educational purposes. Similar to other mobile devices, smartphones are prone to online attacks, and their usage on a university network may lead to cyber-attacks on a university's information systems. Many universities utilise information systems such as mobile websites and mobile applications like Office Outlook email, Moodle and Turnitin. Therefore, ensuring adequate online security is fundamental to mitigate online threats, but such actions are disregarded by most students who are considered the security administrators of their smartphones. This study used a quantitative research method to assess smartphone users' security practices at the UKZN Westville Campus and its effects on the Institutional Information Systems. The University of KwaZulu-Natal's information systems includes a mobile website that enables students to access UKZN student central for academic and support services. The university also uses mobile applications such as MyUKZN, Turnitin and Moodle. The study gathered data via paper-based and online questionnaires from the University of KwaZulu-Natal students that own and use smartphones to connect to the internet via the university's WIFI on campus. The findings of this study revealed that online threats might occur through students disregard for the university's online security guidelines. Some students' lack of online security knowledge was also discovered, making these individuals' smartphones possible entry points for online attacks. Regardless of online security skill level, students demonstrated inconsistent security behaviour. The above mentioned inadequate security practices by students can result in the UKZN experiencing a data breach, financial loss, disruption of services, intellectual property theft, and much more damages. The findings further indicated that students that possess good security skills do not readily implement security measures because the process is assumed to be stressful.

KEYWORDS: Smartphone, Online Security, Students, Behaviour, Threats, Protection Motivation Theory, and Information Systems

LIST OF ABBREVIATIONS

No.	Abbreviation	Full Name
1	ANOVA	Analysis of Variance
2	API	Application Programming Interfaces
3	BYOD	Bring Your Own Device
4	GPS	Global Positioning System
5	HSSREC	Humanities and Social Sciences Research Ethics Committee
6	ICS	Information Communication Service
7	IoT	Internet of Things
8	JISC	Joint Information Systems Committee
9	MMS	Multimedia Message
10	OS	Operating Systems
11	PC	Personal Computers
12	PDA	Personal Digital Assistant
13	PDF	Portable Document Format
14	PMT	Protection Motivation Theory
15	POPI	Protection Of Personal Information
16	RAT	Routine Activity Theory
17	SMS	Short Message Service
18	SQL	Structured Query Language
19	TAM	Technology Acceptance Model
20	TRA	Theory of Reasoned Action
21	URL	Uniform Resource Locator
22	UKZN	University of KwaZulu-Natal
23	UI	User Interface
24	WIFI	Wireless Fidelity

TABLE OF CONTENTS

DECLARATION	i
ACKNOWLEDGEMENTS	ii
ABSTRACT.....	iii
KEYWORDS	iii
LIST OF ABBREVIATIONS.....	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES.....	ix
LIST OF FIGURES	x
CHAPTER 1	1
1.1 Overview.....	1
1.2 Background	2
1.3 Problem Statement	4
1.4 Research Questions	5
1.5 Research Objectives	5
1.6 Research Rationale.....	5
1.7 Significance of the study	6
1.8 Structure of the study	7
1.9 Conclusion.....	8
CHAPTER 2	9
2.1 Introduction	9
2.2 The evolution of smartphones	9
2.3 The Role of Smartphones in education	10
2.4 Data price and the use of smartphones on campus.....	10
2.5 The effects of using smartphones to access the internet on a university campus	11
2.5.1 Problem of Privacy	11

2.5.2 Lack of insight on the consequence of online security of smartphone.....	13
2.5.3 The consequences of using certain apps and visiting mobile sites.....	13
2.5.4 Illegal access to smartphones and phishing	14
2.5.5 Non-compliance to online security guidelines	15
2.5.6 Little control on sites visited and download source	15
2.5.7 Universities support the use of smartphones for educational activities	18
2.5.8 Assessing student smartphone security practices at universities.....	18
2.6 Theoretical framework	20
2.6.1 The Routine Activity Theory.....	21
2.6.2 The Theory of Reasoned Action (TRA)	21
2.6.3 The Technology Acceptance Model (TAM)	22
2.6.4 The Institutional Theory	22
2.6.5 The Protection Motivation Theory	23
2.7 Theoretical frameworks similarities.....	23
2.8 Theoretical frameworks differences.....	24
2.9 The Chosen Framework	24
2.9.1 Threat Appraisal	26
2.9.2 Perceived Vulnerability	26
2.9.3 Perceived Severity	26
2.9.4 Rewards	26
2.9.5 Coping Appraisal.....	26
2.9.6 Response Efficacy	26
2.9.7 Self-efficacy.....	27
2.9.8 Response Cost	27
2.10 Conclusion.....	27
CHAPTER 3	28
3.1 Introduction	28

3.2 Research Design	28
3.4 Study Site	29
3.5 Target Population	29
3.6 Sampling Strategies.....	29
3.7 Sample Size	29
3.8 Sample	30
3.9 Data Collection Method	30
3.10 Ethical Considerations.....	31
3.11 Data Collection.....	32
3.12 Measurements.....	33
3.13 Data Analysis	34
3.13.1 Analysis Overview	35
3.14 Data Quality Control	35
3.15 Conclusion.....	36
CHAPTER 4	37
4.1 Introduction	37
4.2 Rate of Response	37
4.3 Findings of the study	38
4.4 Reliability Test	39
4.5 Demographics and study variables analysis.....	39
4.6 Protection Motivation Inferential Analysis	53
4.6.1 Perceived Vulnerability analysis against Response Efficacy	54
4.6.2 Perceived Severity analysed against Self Efficacy	58
4.6.3 Inference test for Self Efficacy	65
4.7 Answers for main research questions	66
4.7.1 The answer for research question one	66
4.7.2 The answer for research question two	67

4.7.3 The answer for research question three	69
4.8 Conclusion.....	69
CHAPTER 5	70
5.1 Introduction	70
5.2 Dissertation Conclusion	70
5.3 Limitations and Future Research.....	71
5.4 Recommendations	71
5.6 Conclusion.....	74
REFERENCES	75
APPENDIX.....	84
Turnitin report	84
Questionnaire	85
Tables and charts – data	90
Ethical Clearance.....	135

LIST OF TABLES

Table 4.1 Cronbach's Alpha test.....	39
Table 4.2 Demography.....	40
Table 4.3 T-Test for Perceived Vulnerability Threat Appraisal.	42
Table 4.4 The UKZN ICS Alerts Students to Fraudulent Emails.....	48
Table 4.5 T-Test for Response Efficacy Coping Appraisal.	49
Table 4.6 T-Test for Self Efficacy Coping Appraisal.....	52
Table 4.7 Questions 5.1 and 11, The Impact of Threat Appraisal on Coping Appraisal.....	55
Table 4.9 Questions 6.2 and 14 The Impact of Threat Appraisal on Coping Appraisal.....	59
Table 4.11 Questions 6.7 and 15 The Impact of Threat Appraisal on Coping Appraisal.....	61
Table 4.12 Questions 7 and 15 The Impact of Threat Appraisal on Coping Appraisal.....	62
Table 4.13 Questions 6.1 and 16 The Impact of Threat Appraisal on Coping Appraisal.....	63
Table 4.14 Questions 6.5 and 16 The Impact of Threat Appraisal on Coping Appraisal.....	63
Table 4.15 Questions 6.8 and 16 The Impact of Threat Appraisal on Coping Appraisal.....	64
Table 4.16 Questions 6.2 and 17 The Impact of Threat Appraisal on Coping Appraisal.....	64

LIST OF FIGURES

Figure 2.1 Protection Motivation Theory.	25
Figure 4.1 Data Loss if UKZN Online Security Guideline is Disregarded.	41
Figure 4.2 A Data Breach May Result in a Major Problem for UKZN.	42
Figure 4.3 Lack of Understanding of Security Guideline.	45
Figure 4.4 A Disregard for Online Security Guidelines can Compromise Student Accounts.	47
Figure 4.5 The Stress to Implement Security Measures Discourages Following UKZN Security Guidelines.	53

CHAPTER 1

Introduction

1.1 Overview

Online security has become an essential element when using technology in the digital age. The increased adoption of digitalisation brings online vulnerabilities, increasing the cyber-criminals interest in technology users (Leukfeldt, 2017). With the continual advancement of technology, smartphones have become more diverse and serve numerous purposes, such as learning, communication, banking, and much more (Chauhan & Upamannyu, 2017). In recent years, the evolution of technology has led to smartphones and other mobile devices taking more preference in the classroom over laptops because of mobility and ease of access (Siew, Ng, Che-Hassan, Hassan, Mohammad-Nor, Ain, & Abdul-Malek, 2017). However, compromised smartphones connected to a university's network increase the likelihood of an institution-wide cyber-attack (Polyakov, 2017). In addition, the exposure of organisational information systems to online threats has been linked to smartphone users' security behaviours (Mutarurwa, Flowerday, & Cilliers, 2018).

With regards to online security, people are considered security administrators of their smartphones by using security measures and guidelines to protect their devices; and the right security actions are often taken for granted by people (Holicza & Kadena, 2018). Hence, individuals are commonly viewed as the weakest part of the security of an information system (Shouran, Priyambodo, & Ashari, 2019). Information security experts alike have concerns about how smartphone users surf the web and react to cyber threats (Van Bavel, Rodriguez Priego, Vila, & Briggs, 2019).

The 5G technology also contributed to the online security problems of smartphones; due to the increased usage of the Internet of Things (IoT) connected to various smart devices which may not be secured (Jurcut, Niculcea, Ranaweera, & Le Khac, 2020). Incidentally, smartphones contain confidential information that needs to be protected (Gartner, 2019). A recent report by Accenture stated that South African smartphone users have become increasingly targeted by cybercriminals because many residing in the country are relatively inexperienced or not technically skilled to handle online threats (Accenture, 2020b).

With the viewpoint described above, the study is focused on the security practice of smartphone users and the effects on institutional information systems. The research was initially conducted physically using students at the University of KwaZulu-Natal and later switched to the online collection method due to Covid-19 protocols put in place by the university. The study concentrated on the online security practices of students to threats targeted at their smartphones. Following the prior mentioned problem, students need to know that their online security behaviour, when connected to the university's wireless network, can expose the institution to online threats. Therefore, this study provides recommendations to assist the University of KwaZulu-Natal to reduce organisation-wide threats to the institution's information systems.

Chapter one discusses the background of the study. The chapter also explains the problem statement of the research. The three research questions aligned with the research objectives are subsequently discussed. Insight is then given on the rationale behind the research. The significance of the study to the university and students is likewise discussed. The structure for each chapter of the study is explained before the conclusion of this chapter.

1.2 Background

The industrial age's progression to the age of technology has seen the development of numerous innovative technologies. An example of such technology is the smartphone (Ballantyne, Wong, & Morgan, 2017). The range of functionality of smartphones, in recent years, has expanded to activities that were previously limited to desktop computers (Godwin-Jones, 2017). South Africa gradually adopted mobile education by using quality digital tools to increase students access to educational resources and support within and outside the classroom (O'Hagan, 2017). However, the use of smartphones could cause online security risks due to frequent visits to safe and unsafe websites (Amro, 2018). Despite online threats, several universities have adopted mobile applications for students to perform academic and support activities due to the adoption of smartphone usage on campuses (Atas & Celik., 2019). The MyUKZN application by the University of KwaZulu-Natal is an example of a mobile application that provides students with information and self-service capabilities (Mueni, 2019).

Research has indicated that many smartphone applications are either not secure or risk-free of malware attacks (Ahvanooy, Li, Rabbani, & Rajput, 2017). Malware consists of two factors:

an infection vector and an infection payload. The infection vector is the technique utilised to distribute malicious applications. The second factor is the infection payload which is the content used to attack a person's technological device (Van Niekerk & Maharaj, 2017). In the event of a successful hack on a student's mobile device such as a smartphone, a data breach, information theft, among other damaging things, can occur to both students and the university (Singh, Wai-Chan, & Zulkefli, 2017). Smartphone owners' security decisions on the device are personal and essential, although different mobile operating systems' complexities make universal security controls challenging to achieve (Weichbroth & Lysik, 2020).

Good cybersecurity for smartphones often depends on the willingness of the user to avoid identified threats. The user's response is based on how the individual perceives security threats and the coping mechanism used to tackle the threat (Dang-Pham & Pittayachawan, 2015). A behavioural disconnect also exists with how people treat their Personal Computers (PC) security compared to smartphones. More security measures are implemented on the PC with the belief that smartphones are less vulnerable than PCs (Kithome, 2017). However, a smartphone interface is small with little or no security indicators, making it hard to separate phishing websites. As a result, it is easier to access fraudulent messages or emails on a smartphone (David, Kadobayashi, & Fall, 2017).

People often ignore security messages because of the perceived inconvenience of continuing with other smartphone activities (Alsaleh, Alomar, & Alarifi, 2017). As a consequence of human security actions, in 2018, some Iranian hackers illegally took information, such as; scientific research and dissertations, from 320 universities worldwide within five years. The hackers succeeded by sending malicious email links to the university communities, and victims accessed these links on various digital devices such as smartphones (Cohen, 2018). Kaspersky's insight on phishing attacks also reported a surge in email fraud as a tool for malicious attacks in recent years (Kaspersky, 2019).

Consequently, individuals' intent to conduct secure behaviour when using technology varies based on personal security awareness, knowledge and actions (Zwilling, Klien, Lesjak, Wiechetek, Çetin, & Basım, 2020). The responsibility of online security in South Africa does not fall only on students, as the university is equally responsible for protecting its information systems. The South African Protection of Personal Information Act (POPI Act) Section 19

subsection (1b) states that organisations must take the proper measures to prevent unlawful access to the personal information of people (Republic of South Africa, 2021).

Considering the unpredictable behaviour of online security practices when threats are targeted at students' smartphones, the researcher aimed to assess factors influencing students' online security behaviours. Furthermore, the study sought to determine the effects of security practices on the university's information system. An additional evaluation was intended to discover if good online security skill is enough to protect students from becoming victims of online threats.

1.3 Problem Statement

Educational institutions set security guidelines for personal devices, including smartphones, because their use may lead to cyber-attacks on an institution's information systems (Dang-Pham & Pittayachawan, 2015). Cyber threats are dominant, although organisations invest on information system security to cover vulnerabilities in hardware such as smartphones (Ogutcu, Testik, & Chouseinoglou, 2016). Online attacks may occur within universities, and without protective compliance, various security problems may occur, affecting the university and students alike. The purpose of online attacks varies from hacking for fun to dangerous criminal acts of stealing important information among other things (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2018). The cost of the above-mentioned online security problems includes but is not limited to financial loss and data breach (Moallem, 2019).

This study aimed to create awareness of online security issues, provide guidance and training for smartphone users to lessen the risks brought by unreliable security practices. The research is vital considering that most students using smartphones want to explore the internet with minor security restrictions over a university network, making universities prone to cyber-attacks (Coleman & Purcell, 2015). For example, to access academic and support services, the University of KwaZulu-Natal students use mobile sites and applications such as UKZN student central, Office Outlook email, MyUKZN mobile application, etc (University of KwaZulu-Natal, n.d). Previous research indicates that hackers can penetrate university information systems, such as using mailing platforms to send malicious emails to students while pretending to be university staff (Nurse, 2018).

1.4 Research Questions

The research questions listed are extracted from the research problem of this study:

1. What are the factors influencing the security practices of UKZN smartphone users to counter security threats?
2. How are the security practices of UKZN smartphone users affecting the university's information systems?
3. Does the possession of good security skills by students ensure taking the right security measures?

1.5 Research Objectives

1. To discover the factors that influence the security practices of smartphone users to counter security threats targeted at their smartphones.
2. To assess how the security practices of UKZN smartphone users affects the university's information systems.
3. To evaluate if the possession of good security skills by students ensures taking the right security measures.

1.6 Research Rationale

With the wide range of smartphone use, it is apparent that the ease of use enables people to utilise smartphones in numerous places such as university campuses. Past research suggests that many students use smartphones on campus to access academic services, social networking platforms, browse the web and access emails (Atas & Celik., 2019). Students, however, need to learn about security-related problems attached to the use of smartphones on campus. Similarly, students need to know the benefits of good security practices (Taha & Dahabiyeh, 2021). Therefore, this study enables identifying security practices related to smartphone use that can influence cyber-attacks on university information systems.

In 2015, the Republic of South Africa committed to the use of technology to leverage challenges in the education sector as part of the national development plan for 2030 (Republic of South Africa, 2015). Consequently, smartphone use in South African universities is not new, but most of the stakeholders believe that many students misuse technologies (Ngesi, Landa, Madikiza, Cekiso, Tshotsho, & Walters, 2018). The non-compliance to online security rules is linked to personal security traits (Weems, Ahmed, Richard III, Russell, & Neill, 2018).

Malware is used to exploit smartphones security issues by attaching itself to applications or files. Other malware exploits the weaknesses of the smartphone, for instance, the Global Positioning System (GPS), internet access, the gathering of information through multimedia messages, calls, and malicious applications (Kadir, Stakhanova, & Ghorbani, 2018).

Consequently, this research outlines essential information for a university to ensure that students' data and university information systems are not exposed to online attacks. The University's Information Communication Service department can utilise this research's recommendations to provide insights into reducing information systems compromises. The proposed solutions enable decision-makers to create suitable methods and guidelines to protect institutional information systems and student data. Equally, it enlightens smartphone users on campus on the types of online security threats empowered by personal security practices.

1.7 Significance of the study

In Africa, there is a development to combine physical and wireless learning infrastructure in universities, and it is called blended learning. To achieve blended learning, South Africa used wireless distribution for internet access to leverage technological devices like smartphones to enable students to gain online access (Mayisela, 2013). Smartphones offer a level of flexibility that a laptop may not provide in certain situations. For example, some students use their smartphones to complete assignments while commuting (Lieberman, 2019). Though smartphones offer a lot of functionalities, most people treat the security of Personal Computers different from smartphones (Koyuncu & Pusatli, 2019).

A smartphone user's variation in security actions can lead to information and financial loss or data exposure of smartphone users and the institution. Many higher institutions devise different methods of handling online security, assuming that people will inevitably make mistakes. Some universities use measures such as monitoring online traffic in and out of the institution to identify harmful activities and isolate the problem to reduce overall risk (Deloitte, 2018). Hence, this research offers insight into the extent to which smartphone users' security practices on university campuses can contribute to cyber-attacks on an institution's information systems and the possible consequences of such attacks.

Students also need to understand the advantages and disadvantages of using smartphones on campus to access the internet via the university's wireless network. Knowing the previously mentioned issue allows students to cultivate better online security practices when using smartphones on campus. The research findings also intend to enable the university where the study was conducted to strengthen security guidelines and support services for student smartphone users who access the internet over the university's wireless network. If this study was not conducted, the university might continue to address cyber-security issues related to smartphone usage on a secondary level without tackling the actual security practices of smartphone users that can be costly to the institution.

1.8 Structure of the study

Chapter one discussed the background of the study and the problem statement. The research objectives which are aligned with the research questions are explained in detail. The rationale behind the research and its significance to the university are also discussed. Furthermore, the chapter describes the structure of the entire study.

Chapter two examines existing literature on the issue of security practices of smartphone users. The chapter also assesses the implications of security practices on university information systems using the viewpoint of this study's three research questions. The chapter also explains the identification and selection of an appropriate theoretical framework to guide the assessment of existing literature.

Chapter three explains the research methodology adopted to conduct the research. The research design employed in this study is described at the beginning. Furthermore, the sampling method and the sample size determined from the chosen population are discussed. The data collection instrument adopted, and the analytic method suited for the instrument are discussed in chapter three. Moreover, ethical considerations and procedures used to conduct the study are likewise explained. Finally, the study's data collection procedure and data control are described in the latter part of this chapter.

Chapter four utilises the research methodology described in the previous chapter to analyse and interpret collected data. In this chapter, the research findings and interpretation are discussed.

The results include the descriptive analysis and inferences utilised to derive answers for the three research questions, as stated in chapter one.

Chapter five concludes the research by summarising the findings of the study. The chapter presents the research limitations discovered. It further provides recommendations to solve the research problem. The chapter concludes with the highlighted areas for future research and the overall research conclusion.

1.9 Conclusion

Chapter one discussed the research background, introducing the research topic, the security practice of smartphone users and the effects on institutional information systems. The chapter also explained the research problem and the main research questions as well as the research objectives. In addition, the rationale of the research, the significance of the study, and the structure of the study were similarly discussed. Chapter two examines the six constructs from the selected theoretical framework for the research. The chapter then reviews relevant literature on the research topic. Chapter three highlights several theoretical frameworks considered for this research, and further discussed is the Protection Motivation Theory eventually chosen.

CHAPTER 2

Literature Review

2.1 Introduction

Chapter two discusses existing literature in line with the research objectives, highlighting the history of smartphones, the significance of smartphones in education, and the online security challenges universities face. The use of smartphones on campus is a relatively common culture for different purposes, such as communication and academic reasons (Mwambakulu & Chikumba, 2021). With the increasing use of smartphones on university campuses, this study focuses on the security behaviour of smartphone users and its effects on the university's information systems.

2.2 The evolution of smartphones

The evolution of smartphones began with the first mobile phone, Motorola Dyna Tac, created in 1973. Although large, the phone had a similar shape to mobile phones of recent years, with calling and texting capabilities (Anh, 2016). The smartphone's predecessor is the Personal Digital Assistant (PDA). It was a pocket-sized computer with a touch screen and stylus utilised for input. It could also perform calculations, take notes and make schedules. Most PDA versions had no wireless network communication capability (Edwards, 2018). The developmental change in mobile technology led to the creation of multi-functional smartphones (Lewis & Zaheer, 2018).

IBM created the pioneer smartphone known as Simon, and it was available for purchase in 1994. The smartphone integrated both primary mobile functions, touch screen and Personal Digital Assistant, PDA features, such as calculator, email capability, and mobile applications (Smith, 2018). In addition, smartphones provide a more exclusive experience and allow individuals to use the internet at any time virtually (Nayak, 2018). Wireless data transmission was introduced in the late 90s to different devices such as smartphones. It was achieved using an electromagnetic method such as radio frequencies to create wireless communication between personal devices (Rajotiya, 2019). The advanced capabilities of smartphones are likewise derived from mobile processors, enabling various tasks to be conducted on a smartphone (Thirumoorthy, 2020).

Technological advancements introduced mobile applications on smartphones to offer more features for end-users to use on such devices. Thus, more applications can be downloaded from mobile platforms such as the Google Play Store or iOS Store (Baktha, 2017). Hence, smartphones in recent times are used in place of laptops, personal computers, television, and radio to get information, communicate, purchase items online, electronic banking, learning and other activities (Nayak, 2018).

2.3 The Role of Smartphones in education

The popularity of smartphones among youth is due to the device utilisation for various activities such as gaming, social media and email: the benefits have recently led more students to own these devices (Jason, 2017). Hence, South Africa has been engaging in projects facilitating the use of technology such as smartphone usage to enable tutoring, learning support beyond the classroom, access to more resources to improve learning in the country (O'Hagan, 2017). Smartphones have created mobile learning, enabling virtual learning for students (Dias & Victor, 2017). It allows easy access to conduct various activities and is widely used by students to support academic activities (Chaputula & Mutula, 2018). A study by Atas & Celik (2019) also indicated that university students that use smartphones spend an average of four hours on their smartphones to access the internet.

2.4 Data price and the use of smartphones on campus

In South Africa, universities provide free Wi-Fi to students. Mobile devices connect to the internet over public Wi-Fi to access social sites, emailing, video watching or browsing (Research ICT Africa, 2016). The internet availability and accessibility for students is part of the ICT innovation in education Africa to aid learning (Internet Society, 2017). The use of a free Wi-Fi network connection is convenient for people. However, it includes security and privacy risks because most public wireless networks are unencrypted, and the spread of malware is easy in such situations (Maimon, Becker, Patil, & Katz, 2017).

The provision of free Wi-Fi is essential because the price of the internet data bundle is expensive in South Africa than in some other African countries such as Tunisia and Mauritius, making affordability and data use in the country difficult. South Africa ranked 111 out of 172 for 1 gigabyte purchasing power (Research ICT Africa, 2020). Although the price of data in

South Africa is expensive, Statista reported that South Africa has a mobile internet penetration rate of 52.8% of the population, that is, 31.29 million people (Statista, 2021c).

With costly data prices, using campus Wi-Fi is preferable for students and does not involve costs. Unfortunately, various mobile threats exist, such as physical, online, and application-based threats (Nagarjun & Ahamad, 2018). In 2018 Deloitte reported that different universities utilise diverse approaches to secure online traffic; some used in-house Information Technology and IT expert while others employ security companies to monitor university security round the clock (Deloitte, 2018). Similarly, considering that university wireless networks experience network-related issues such as eavesdropping, institutions find ways to deal with networks and security procedures. Universities further use firewall software to monitor unusual activities on their network while protecting vital information (Losonczi, Vackova, & Necas, 2019). Therefore, training students on how phishing and information gathering works help to gauge threats. An example is examining the email header of a suspicious email and discarding emails from unknown or questionable sources (Salahdine & Kaabouch, 2019).

2.5 The effects of using smartphones to access the internet on a university campus

The subsequent discussions are relevant literature assessing numerous studies that have provided insight into the impact of using smartphones to access the internet over a university's network.

2.5.1 Problem of Privacy

Privacy has various definitions; however, it can be defined as the right of individuals to control which information about themselves can be revealed to other people (Lukacs, 2017). Cyber threats pose a problem to the online privacy of people (Toch, Bettini, Shmueli, Radaelli, Lanzi, Riboni, & Lepri, 2018). Individuals often state personal concerns for online privacy, but recent research indicates that people's careless online behaviour contradicts the identified security concerns (Barth, De Jong, Junger, Hartel, & Roppelt, 2019).

The potential reasons for the failure of individuals to protect themselves online could be due to lack of knowledge regarding privacy exposure consequences, cost-benefit analysis of protection and the inability of people to defend themselves (Gerber, Zimmermann, & Volkamer, 2019). In organisations, behavioural and device standards are necessary considering

an individual's privacy, data security, integrity, and communication; these considerations are for the overall digital protection on a personal computer and mobile device (Deloitte, 2019).

Mobile malware popularity has made a trend whereby malware writers create malware to expose individuals' personal and private information on these devices (Riasat, Sakeena, Wang, Hannan Sadiq, & Wang, 2017). However, malware attacks are usually directed towards privacy invasion of people online (Ali, Islam, Rauf, Ud Din, Guizani, & Rodrigues, 2018). Privacy is a significant problem for people online, and effort should be made to protect an individual's private data (Gerber et al., 2019).

Online packets exchanged over a network can be exposed or revealed and intercepted (Kausar, Aljumah, Alzaydi, & Alroba, 2019). Collective information derived from Wi-Fi networks on individuals include but is not limited to name, address, email, phone number. Vital data can be transferred to third party companies from smartphone application servers (Thompson & Warzel, 2019). The University of Australia experienced a data breach that affected staff and students alike, stealing data from the date of the theft ranging back to 19 years affecting about 200,000 individuals (Martin, 2019).

Sensitive information can also be stolen from smartphones connected to the internet through other means. The Short Message Service (SMS), a common way of communicating, can be used for malicious intent. For example, phishing, which is widely used to send malicious emails to individuals, can be combined with SMS to create smishing attacks. Smishing sends malicious links of dangerous websites and applications via texts to people (Mishra & Soni, 2020). Short Message Service attacks such as those mentioned above are primarily successful because many people access and read their text without expecting to open malicious messages (Phishlabs, 2019).

On smartphones, SMS worms are also used to send messages to people and infect their phones. The threat is dependent on the phone user's security behaviour or consciousness (Xiao, Fu, Li, Hu, & Jiang, 2017). Short Message Service trojan is another way to intercept outgoing and incoming messages sending a copy of the wordings to the email of the cyber-attackers, which exposes the smartphone owner's information (Kaspersky, 2019). An instance of a mobile attack is the Operation Sheep Campaign, formerly known as Man-in-the-Disk vulnerability. It uses utility applications to steal smartphone user contact information without permission and

transfers them to remote servers (Winder, 2019). Mobile spyware is likewise used to monitor the activities of the smartphone owner, location, and vital information such as logins and password details. The spying is done silently until it is detected (Kaspersky, 2019).

2.5.2 Lack of insight on the consequence of online security of smartphone

The use of Bring Your Own Device (BYOD) raises concerns about universities security and privacy s (Siani, 2017). The University of Maryland conducted a study that indicated a link between discipline affiliation security awareness and vulnerability to clicking on malicious links (Diaz, Sherman, & Joshi, 2019). Therefore, knowing people's security awareness is essential to create the right security training program to prevent cyber victimisation (Broadhurst, Skinner, Sifniotis, Matamoros Macias, & Ipsen, 2018).

Around the world, tertiary institutions provide online security awareness to students. The University of KwaZulu-Natal does the same with the vital information and guidelines on its website alongside the physical support for students (University of KwaZulu-Natal, 2018). The Universities' security policies further help control and partition valuable research work, making it hard for attackers to access essential data and information (Joint Information Systems Committee, 2018). However, the outcry by people for privacy protection and the unsuccessful implementation of data protection by them is connected to that lack of knowledge (Gerber et al., 2019).

2.5.3 The consequences of using certain apps and visiting mobile sites

Phishing attacks in recent years have become more sophisticated, and ransomware is also used to exploit organisation weaknesses (Accenture, 2017). The widely used learning platform, Moodle, was hacked in 2017. The hackers exploited the PHP based system using Structured Query Language (SQL) injection. The hackers gained unauthorised access by modifying the PHP code of the Moodle server to take advantage of a registered user's preference (Brook, 2017). The result of a data breach for any university is costly. The effect of hacking goes beyond the student information and is felt by the university itself; the results include financial loss, reputation damage of the university and its stakeholders, and impact on daily processes (Deloitte, 2018).

The advancement of technology has increased the need for organisations to have cybersecurity insurance to protect against the loss of important information due to online attacks such as malware intrusion (KPMG, 2018). An IBM report previously indicated that South Africa scores low on automated security deployment for a data breach with 16% full automation out of 100%, which translates to losing millions of Rands to an online security breach (IBM, 2019).

It is recommended that organisations explore actions such as data monitoring and practice security readiness to tackle online crime and prevent or lessen online security problems (KPMG, 2018). Higher institutions must also conduct security risks to proffer what online risk levels are considered acceptable (Deloitte a, 2018). Organisations cybersecurity insurance can also help cover liability claims, provide IT experts, forensic investigations, and breach-related legal advice (European Insurance and Occupation Pension Authority, 2018). Accenture created a model to estimate the cybercrime risk of an organisation in the following sequence: estimate the expected cost of cybercrime as a percentage of an organisation's revenue, then calculate total sector revenue multiplied by the anticipated cost of cybercrime in the sector. Subsequently, an analysis is conducted on how better cybersecurity protection reduces the organisation's risk (Accenture, 2019).

Organisations should consider technical prevention, including monitoring anomaly-based online traffic and code loading verification (Cheng, Liu, & Yao, 2017). Assessing existing security practices and behaviours provides better modes of preparation for people. Cybersecurity training is also an important activity that is either role-based or knowledge-based; the former is meant for technical administrators while the latter is for end-users. Knowledge-based security training is a one-size-fits-all method that uses a general guide for protection (Croasdell, Elste, & Hill, 2018).

2.5.4 Illegal access to smartphones and phishing

Cybercriminals target victims' security judgment in certain situations rather than online security measures. People can fall victim to phishing attacks such as email spam, so evaluating the victim's response is essential. Generic, tailored, and targeted phishing are the three categorisations of malicious attacks (Broadhurst et al., 2018). The use of malicious emails to trick victims into clicking on deceptive websites and decisively providing their username and password to unknown persons is called phishing. A report by Chapman provides an example

of a phishing attack aimed at students is a scholarship fraud that requested both personal and banking details of the victim (Chapman, 2019).

In 2019, two major malware campaigns, SimBad and Operation Sheep, infected over 250 million smartphones through 220 malicious Android apps (Avast, 2019). The SimBad malware displays advertisements in the background, opening a Uniform Resource Locator (URL) within the browser as the threat actor. The malware starts a phishing attack and exposes the smartphone to other malicious applications (Winder, 2019). Device exposure is enabled when the malicious software connects to a remote server to receive orders which can further infect the smartphone with more malware (Afifi-Sabet, 2019). Covid-19, in 2020 helped propel the use of surveillance technology by most governments to monitor the spread of the disease. This effort includes the use of mobile applications, geo-locator tracking, and Bluetooth signals. The implication of collecting personal information led to Covid phishing campaigns targeted at mobile device owners (Accenture, 2020a).

2.5.5 Non-compliance to online security guidelines

Human error and negligence were identified as factors that cause digital breaches (Ponemon, 2017). As a result, information security management systems in organisations are essential to create, implement, maintain, and improve information management systems based on the organisation's size and needs. The system uses risk management to protect confidentiality, integrity, and availability of information (Al Dhahri, Al Sarti, & Abdul Aziz, 2017).

Organisations, however, do not control personal devices and applications installed on these devices, making it difficult to enforce policies on individuals, and the organisation is left susceptible to cyber-attacks (Rivadeneira & Rodriguez, 2018). Smartphone users are not always compliant to security controls, and past research has indicated that an increase in self-efficacy is linked to the right actions to handle security issues (Belanger & Crossler, 2019). Similarly, many university students assume adequate protection for information technology and network infrastructure is provided by universities (Chapman, 2019).

2.5.6 Little control on sites visited and download source

Smartphones play a significant role in people's lives due to reliance on the internet alongside online resources, and online attacks have increased with the usage of the device (Talal, Zaidan,

Bahaa, Albahri, Alsalem, Albahri, Alamoodi, Kiah, Jumaah, & Alaa, 2019). Generally, people have a tendency of visiting unsafe sites (Van der Kleij & Leukfeldt, 2019). Popular websites that are usually visited include social networking sites where personal information can be stolen including that of the victim's friends. These attacks pose location privacy breaches, identity clone attacks, clickjacking, and many other attacks (Almarabeh, 2019).

A recent Statista report revealed that the active global social media population is 4.2 billion people, and 4.15 billion are active through their mobile devices. Facebook has the largest audience of 2.6 billion monthly active users among social networking sites (Statista, 2021b). Mobile malware also increased in 2020, yet more mobile applications are being downloaded. An estimated 218 billion mobile applications were downloaded in 2020 worldwide (Statista, 2021a).

Downloading mobile applications has its negative aspects, which start with accepting the terms and conditions of the application. People usually overlook conditions that allow access to the user's smartphone information, pictures, and contacts (Chawdhry, Paullet, Douglas, & Compimizzi, 2016). On the side of developers, each application has a privacy grade, rated from D to A+. Applications with an A+ rate privacy grade only collect information needed for the performance of the application. In contrast, applications rated between B and D collect more information beyond those necessary for the performance of the application, which can exploit users' information for money (Cecere, Le Guel, & Lefrere, 2018).

Downloading malicious mobile applications from numerous sources is common. It is becoming prevalent to download malicious applications from legitimate sources such as Google Play and Apple Store due to a degree of illegal infiltration on these platforms (Sarang, 2018). For the second quarter of 2020, McAfee reported that new mobile malware increased by 12% from the previous quarter. The report further indicated an increasing trend of hidden mobile applications that gathers data from mobile devices, and the data is later sent to the application developer (McAfee, 2020).

Several mobile Operating Systems (OS) have been created; however, Google Android and Apple iOS are the most widely used mobile OS. Android is open source and suitable for developers to customise, while iOS is built on specific hardware and components (Gyorodi, Zmaranda, Georgian, & Györödi, 2017). Android and Apple application stores have different

criteria for application development. The Apple store provides Application Programming Interfaces (APIs) to conduct security functionalities for developers like desktop OS, UNIX. In contrast, the Google Play store for Android is open-source and cost-effective for many people to develop an application for the Android OS (Ahvanooey et al., 2017). Apple is considered to be more secure because it does not release the source code application to developers. At the same time, Android relies on open-source; that is, developers can work with the operating system's source code, which can cause vulnerabilities that can be exploited by hackers (Norton, 2020).

The severity levels of online threats sometimes differ from one mobile OS to another (Kaspersky, 2019). Smartphones using Apple Operating System (iOS) experience fewer attacks because the mobile applications are tightly scrutinised on Apple's application store, unlike Google's Play store that has mobile development approach with less scrutiny (Talal et al., 2019). The Lotoor is an example of mobile malware found on the Android OS. The malware exploits various vulnerabilities to enable root control.

In the 2019 Check Point cyber-attack trends report, Triada, Lotoor, and Hidad were the leading smartphone threats in three continents with 38% in Europe, 12% in the Middle East, and 10% in the African region (EMEA), respectively (Check Point, 2019). The triada malware is also found on smartphones with Android OS, and it has variations such as the triada adware or spam applications that users can click (Google, 2019). Above 1.4 million mobile malware was reported in 2020 (McAfee, 2020).

Digital intrusions allow malware and information loss. The initial attack mainly leads to a second one, and malware has variations that serve different purposes, including private information extraction, SMS, search optimisation, and dynamic download (Riasat et al., 2017). The first malware to infect a smartphone was the Cabir in 2004. Cabir was a worm that hijacks the phone User Interface (UI) then replicated itself, which runs down a smartphone's battery (Sowells, 2018). A spyware attack is also a severe threat because hackers can conduct limitless attacks on smartphones via remote access (Symantec, 2018). Mobile malware can be further classified into banking malware, mobile ransomware, Multimedia Message (MMS) malware, mobile adware, and SMS Trojans (Kaspersky, 2019).

For example, institutions recommend using official email to secure communication to reduce the possibility of phishing attacks (Clark, Oorschot, Ruoti, Seamons, & Zappala, 2018). With online security, smartphone users are the first in line for security defence as an incident detection trigger (Verizon, 2019). The response to online threats can take several forms, but it is not limited to the use of strong passwords (Van der Kleij & Leukfeldt, 2019). Security measure is essential because a website can sometimes be compromised due to different reasons such as loopholes within a website hosting platform, compromised site credentials and several other factors (Palaniappan, Sangeetha, Rajendran, Sanjay, Goyal, & Bindhumadhava, 2020).

2.5.7 Universities support the use of smartphones for educational activities

The 2013 POPI Act of South Africa, established for implementation from July 1, 2020, states that organisations are responsible for the integrity and confidentiality of individuals' information under their management or custody. To guard against unauthorised information access, loss, or damage from internal and external sources (Republic of South Africa, 2013). The Act is not the first of its kind globally, as the first privacy legislation was established in the early '70s. The act originated from the use of technology with information due to the concern over inappropriate information practice. Subsequently, more countries, including South Africa, have enacted privacy laws and bills (De Bruyn, 2014). The POPI Act uses international standards to guide how personal information is utilised or processed lawfully and even restrict information (Da Veiga & Swartz, 2017).

Every organisation within South Africa must comply with the POPI Act law if the institute collects, processes, stores, and convey information daily. Organisations are held accountable for data exposure (Kandeh, Botha, & Fletcher, 2018). Various universities worldwide provide technical security support for staff and end-users, and the University of KwaZulu-Natal is one such institution. The university offers phishing and spam awareness through an online guide, quiz, advice, and physical and online helpdesk to protect students (University of KwaZulu-Natal, 2018).

2.5.8 Assessing student smartphone security practices at universities

Studies have indicated that an individual secure or insecure behaviour to technology usage influences personal security assessment and action (Weems et al., 2018). Self-efficacy has been identified to influence and predict people's online security behaviour, which can aid their

willingness and capability to follow positive online security training (Conetta, 2019). Poor security decisions can lead to unauthorised access to personal information and, eventually, identity theft (Belanger & Crossler, 2019). Organised online crime is a significant issue especially, phishing attacks. These attacks focus on data and intellectual properties, and more attacks are concentrated in the education sector, especially universities (Chapman, 2019).

Online attacks add up to why it is recommended that people not click on links in emails before determining the authenticity of the sender and the possible consequence of opening the link (Bruceb, 2017). For example, the University of Fraser Valley experienced a malicious attack. Some students received and accessed suspicious emails on different devices requesting personal information that included email, address, grade, and course credit details. The hackers did this to extort money from the university (Canadian Security, 2017). In 2017, a group of Iranian hackers also took intellectual property worth \$3.4 billion from multiple universities worldwide. The hacking occurred between 2013 to 2017, and the stolen information was sold to interested stakeholders such as corporate organisations (Cohen, 2018).

The aforementioned discussion indicates that university authorities and students are liable for poor security practices, but the former bears most of the cyber threat burden. Consequently, analysing the literature from a student's perspective is vital to advance scholarly insight into the research problem, the security practices of smartphone users at UKZN Westville Campus as a threat to institutional information systems.

According to the reviewed literature, four paragraphs; Lack of insight on the consequences of online security of smartphones; Illegal access to smartphones or phishing; Non-compliance to online security guidelines; Little control on sites visited and download source, provided literary study for research question one. The two paragraphs “The problem of privacy” and “The consequences of using certain apps and visiting mobile sites” gave background knowledge to research question two. Finally, the paragraph “Assessing student smartphone security practices at universities” provided the literary background for question three.

Research question one: What are the factors influencing the security practices of UKZN smartphone users to counter security threats? Focuses on factors influencing security behaviours, such that the paragraph “Lack of insight on the consequences of online security of smartphones” on page 11 assessed the online security knowledge of people. On page 13, an

assessment was done on “Illegal access to smartphones or phishing” to understand how phishing attacks affect the coping appraisal of victims. The paragraph “Non-compliance to online security guidelines” on page 14 assessed the nonconformity of individuals to online security. On page 14 also, another factor in security behaviour was examined in the paragraph “Little control on sites visited and download source”. It discussed how people browse and download mobile applications randomly. These paragraphs allowed the assessment of research question one.

Research question two: How are the security practices of UKZN smartphone users affecting the university's information systems? This question focuses on the security practices of individuals and the outcome of these actions on the university's information systems. The paragraph “The problem of privacy” on page 10 examined people's behaviour towards information privacy and the related issues. The paragraph, “The consequences of using certain apps and visiting mobile sites”, on page 12, discussed the outcome of people's online behaviour and the effect of such behaviour.

Research question three: Does the possession of good security skills by students ensure taking the right security measures? Focuses on the possible link between good security skills and conducting the right security actions. The research question was evaluated in the paragraph, “Assessing student smartphone security practices at universities,” on page 17.

2.6 Theoretical framework

In the process of exploring relevant literature to this research topic, several theoretical frameworks were examined. The theoretical frameworks, namely: the Routine Activity Theory, The Theory of Reasoned Action, Technology Acceptance Model, Institutional Theory, and Protection Motivation Theory, were examined due to their adoption in past research regarding human behaviour in relation to technology usage (Bjorck, 2004; Faklaris, Dabbish, & Hong, 2019; Holt, Van Wilsem, Weijer, & Leukfeldt, 2018; Vance, Siponen, & Pahnla, 2012; Wang & Wang, 2014). The above-mentioned theories provide insight into human behaviour when using technology and its possible effects. To study the research problem, the researcher assessed these theories because each of them offers some of the following constructs: technology use and norms of people, organisational security rules, behavioural intent, actions

and expectations of behaviour, perceived severity and vulnerability of security threats, rewards, response cost, self-efficacy, response efficacy, and many other constructs.

Bjorck (2004) used the institutional theory to research information technology security in organisations. Vance, Siponen and Pahnla (2012) conducted a study on the motivation of security compliance practice utilising the protection motivation theory for the analysis. In 2014, Wang and Wang (2014) used TAM to assess user behaviour to information security technology. Researchers such as Holt et al. (2018) used Routine Activity Theory to conduct a study on self-control and routine activities to assess malware infection victimisation. The theory of Reasoned Action was adopted by Faklaris et al. (2019) to investigate end-user security approaches in 2019. The theories mentioned above are discussed further below.

2.6.1 The Routine Activity Theory

The Routine Activity theory aims to discover large-scale criminal activities and the indicated pattern of occurrence using changing online criminal rate trends (Miró-Llinares, 2014). It focuses on an environmental construct that provides the opportunity for cyber-crimes (Mshana, 2015). It focuses on criminal offenders and not the victims (Rossmo & Summers, 2015). Cohen and Felson created the Routine Activity theory in 1979; the theory explains how and why crimes occur (Argun & Daglar, 2016). Routine Activity theory states that routine activities enable the convergence of cybercriminals and increase exposure and risk of possible victimisation (Kranenbarg, 2018).

The Routine Activity theory was not employed in this research since the theory examines the illegal activities of online perpetrators and not the victim's online security practices and (Rossmo & Summers, 2015). The theory also examines the motivation of criminals that commit illegal actions and victim-offenders that want retaliation for a past negative experience such as financial loss (Kranenbarg, 2018). Although this theory assesses routine behaviour, it does not explain the motivation behind security behaviour which the study aims to examine. The theory is different from the Theory of Reasoned Action (TRA), which considers the victim's action.

2.6.2 The Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA) states that behavioural intents are precursors to actions. The expectation of behaviours can result in specific outcomes; however, actions can be altered

or amplified (Aiken, Davidson, & Amann, 2016). The theory was created based on attitude theory and social cognitive practices. It states that an individual's attitude can either be positive or negative (Hagger, 2019).

The theory of Reasoned Action was not selected because the theory focuses on predicting people's behaviour based on their doings (Aiken et al., 2016). This study does not aim to forecast security practices but rather derive answers from informed security behaviours of research participants. The Theory of Reasoned Action (TRA) differs from the Technology Acceptance Model (TAM), in linking technology to personal behavioural use.

2.6.3 The Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is a theory that describes a person's behaviour to the use of information technology (Davis, Bagozzi, & Warshaw, 1989). The theoretical framework originated from the Theory of Reasoned Action (TRA), which discusses general technology usage. The theory examines people's intentions of accepting or rejecting technology (Momani, Jamous, & Hilles, 2017). Technology Acceptance Theory (TAM) examines individuals' technology acceptance based on the following constructs: perceived usefulness, the perceived increase in productivity, effectiveness, and performance outcome. The theory has since evolved into multiple versions (Van den Berg & Van der Lingen, 2019). This theory was not employed in this study because it assesses technology acceptance for usage and not the security behaviour of end-user towards technology usage. This theory is different from the institutional theory that considers rules, norms, and routines concerning technology use.

2.6.4 The Institutional Theory

The institutional theory identifies factors that can either increase or decrease the contextual risk in an institution (Sen & Borle, 2015). The institutional theory focuses on the social structure, which assesses norms, routines, and rules for social actions (Mohamed, 2017). The norm construct examines normative acts concerning social obligations and values to which a behaviour can be compared. The rules construct explores the regulative aspect of how individuals are encouraged to follow the guiding principles of an organisation. , The routine construct assesses people's behaviour based on practice (De Prá Carvalho, Da Cunha, De Lima, & Carstens, 2017).

The institutional theory was not utilised because it considers rules, norms, and routines concerning technology use and not the security behaviour in response to online threats. The theory differs from the Protection Motivation Theory examines the reason behind the security behaviour of technology users.

2.6.5 The Protection Motivation Theory

The Protection Motivation Theory relates to a fear appeal to three major factors; the extent of a harmful incident, the likelihood of the incident occurring, and the efficiency of a protective reaction (Rogers, 1975). The theory assesses the factors that contribute to the actions that either help conducts protective measures or not when using technology (Clubb & Hinkle, 2015). The theory asserts that 'fear appeals' attempts to instil fear to encourage protective motivation and action. The fear appeal promotes threat appraisal and coping responses to derive protection motivation (Aurigemma, Mattson, & Leonard, 2016). Research by Van Bavel et al. (2019) conducted in 2018 indicated how the theory was used to investigate end-users security behaviours because of the rise in cybercrimes threat awareness as security behaviour is still a concern for security experts.

The protection motivation theory was chosen to investigate the research problem because the constructs examine technology users' behaviour to cyber threats and the effects of these actions. The theory enables the examination of how people assess perceived online threats and the coping appraisal of their security skills to respond to such identified threats (Shillair, 2020). This theory's constructs allow the analysis of threat appraisal, focusing on perceived vulnerability, perceived severity, and rewards; the coping appraisal analyses self-efficacy, response efficacy, and response costs of people. The discussed assessments also give an insight into the outcome of people's security practices (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2021). The evaluation of people's security behaviour using the protection motivation theory aligns with the objectives of this study, hence, the selection for use.

2.7 Theoretical frameworks similarities

Similarities exist within the discussed theories. The institutional theory focuses on social structure and factors that can either increase or decrease the contextual online risk (Sen & Borle, 2015). The Protection Motivation theory likewise assesses the behavioural factors that contribute to the actions that either help conduct protective measures or not when using

technology (Clubb & Hinkle, 2015). The Theory of Reasoned Action (TRA) similarly examines behavioural intents that are precursors to actions, and the expectation of behaviours can result in specific outcomes (Aiken et al., 2016). The Routine Activity Theory focuses on the routine actions that increase exposure and risk of possible victimisation (Kranenbarg, 2018). Technology Acceptance Theory (TAM) also examines individuals' behaviour toward technology acceptance (Van den Berg & Van der Lingen, 2019). the theories mentioned above have certain similarities about people's behaviour concerning technology.

2.8 Theoretical frameworks differences

All the assessed theoretical frameworks have differences. Technology Acceptance Model (TAM) theory explains users' attitudes toward information technology acceptance (Davis et al., 1989). The Theory of Reasoned Action (TRA), unlike the Technology Acceptance Model (TAM), is general; it does not specify the opinions that allow certain behaviours. TRA focuses on human attitude, either good or bad, and subjective norms are apparent influences others might have on an individual (Nguyen, Hens, MacAlister, Johnson, Lebel, Tan, Nguyen, Nguyen, & LebeL, 2018).

The Routine Activity Theory focuses on criminal offenders, not the victims (Rossmo & Summers, 2015), making the Routine theory different from the other assessed theories. The institutional theory focuses on the social structure that examines norms, routines, and rules concerning technology use (Mohamed, 2017), but not how technology users view and respond to security threats. The protection motivation theory provides a different perspective as it considers technology users' behaviour to cyber threats and the effects of these actions (Boerman et al., 2021). Based on the discussion above, the researcher identified the distinguishing factors among various theories to help understand the research problem.

2.9 The Chosen Framework

Prior to the selection of a suitable theoretical framework for this study, the Routine Activity theory and the Institutional Theory were examined more closely as they both focus on the research of human routines that can cause harm concerning technology usage (Bjorck, 2004; Rossmo & Summers, 2015). The Theory of Reasoned Action explores similar constructs with the Protection Motivation Theory such as subjective norms in handling security-related issues (Mills & Sahi, 2019). The Theory of Reasoned Action focuses on social cognitive behaviour.

The theory does not assess the rewards and response cost of activities, threats, and coping appraisal of a person's security behaviour (Hagger, 2019; Shillair, 2020).

The Protection Motivation Theory was considered appropriate for this research to examine the security practices of smartphone users using the following constructs to analyse the problem; perceived vulnerability, perceived severity, self-efficacy, response efficacy, rewards, response costs, threat appraisal, and coping appraisal. From the discussion above, the Protection Motivation theory is suitable for this study because it assesses how people form protection motivation, resulting in security practices against online threats.

The chosen theory's constructs as illustrated in Figure 2.1 enabled the analysis of behavioural constructs to derive the protection motivation of smartphone users when accessing information systems on campus. Thus, the use of the theory helps discover the security behaviour of smartphone users and the effects of the outcomes on the university's information systems. The constructs of the chosen theoretical framework are further discussed in the following paragraphs.

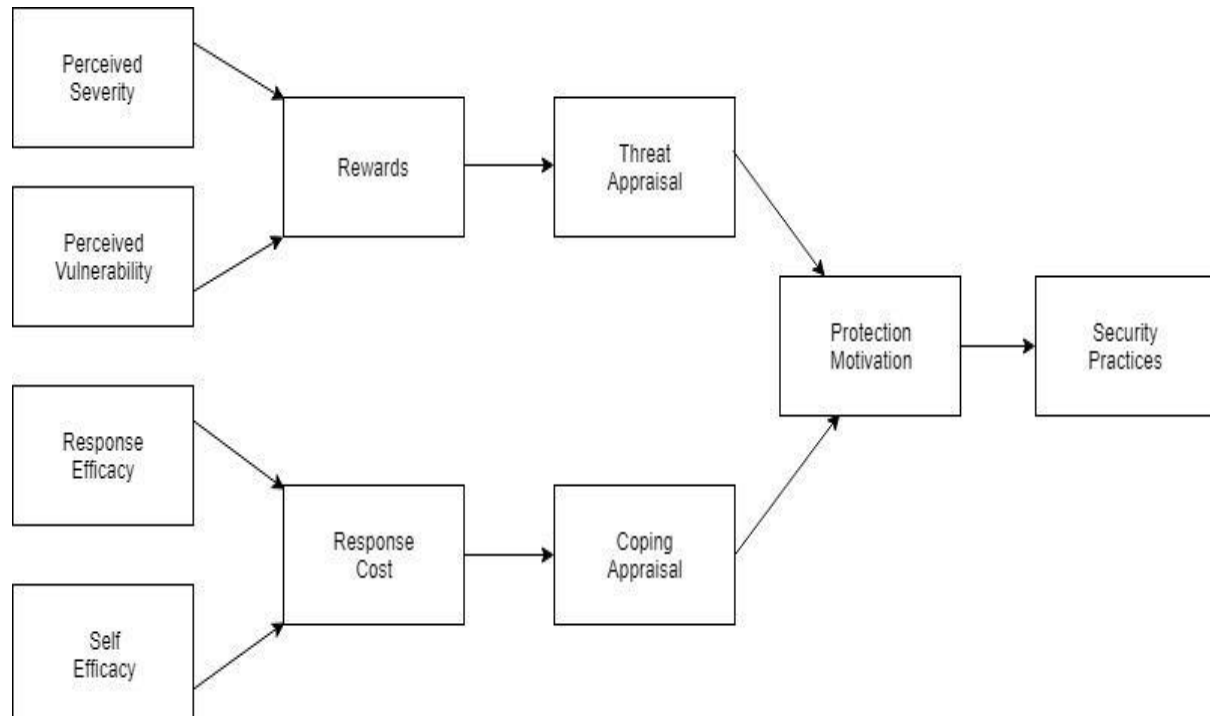


Figure 2.1 Protection Motivation Theory.

2.9.1 Threat Appraisal

The threat appraisal evaluates the severity of an occurrence and considers the seriousness (Rogers, 1975). It also influences security compliance, thus individuals' danger awareness affects security behaviour (Martin, Nathan, Morris, & Harvey, 2018).

2.9.2 Perceived Vulnerability

The perceived vulnerability is the likelihood that an individual may experience harm (Rogers, 1975). Research indicates that smartphones are prone to different vulnerabilities, such as smishing and phishing attacks (Mishra & Soni, 2020).

2.9.3 Perceived Severity

Unlike perceived vulnerability, perceived severity denotes the belief that an individual has about the extent of harm from a negative behaviour (Rogers, 1975). It is the perceived impact of the threat (Aurigemma et al., 2016).

2.9.4 Rewards

Rewards refer to the aspects of beginning or continuing negative behaviour (Rogers, 1975). The reward can be diverse when a person does not partake in the prescribed security action (Aurigemma et al., 2016).

2.9.5 Coping Appraisal

A coping appraisal is a way an individual reacts to threats (Rogers, 1975). The coping appraisal is a balance between either being at risk or not and the likelihood of conducting an action related to the problem. However, low coping appraisal with a high threat appraisal is perceived as a lack of protective behaviour like avoidance (Oakley, Himmelweit, Leinster, & Casado, 2020).

2.9.6 Response Efficacy

Response efficacy believes that adopting a behaviour as a response will help reduce a threat (Rogers, 1975). Response efficacy is the efficiency of a vital protection action (Aurigemma et al., 2016).

2.9.7 Self-efficacy

Self-efficacy is the confidence an individual possesses to conduct a coping response successfully (Rogers, 1975). It is also known as how individuals trust that they can handle a threat using a recommended behaviour (Sun, Yu, Lin, & Tseng, 2016).

2.9.8 Response Cost

The response cost is the cost linked with a suggested behaviour (Rogers, 1975). It considers how costly a response action in a situation will be (Oakley et al., 2020).

All the constructs of the protection motivation theory are utilised in this study. There are three constructs, each under two major ones. Threat appraisal consists of the following constructs: perceived vulnerability, perceived severity and threat rewards. The coping appraisal construct consists of response efficacy, self-efficacy and response cost. The threat appraisal with the coping appraisal of individuals forms the protection motivation for responding to online threats targeted at their smartphones. Research question one used the threat appraisal constructs, perceived vulnerability, perceived severity, and coping appraisal constructs, response efficacy and self-efficacy to derive an answer. Research question two used the threat appraisal construct, reward, for understanding research participants opinions on security behaviour reward. However, the inferred security behaviour reward of the study's population was attained from research question one's inferential answer. Research question three used coping appraisal constructs, response efficacy and self-efficacy and response cost to derive an answer.

2.10 Conclusion

Chapter two reviewed existing literature related to this research and highlighted the history of smartphones with significance in education, especially at universities. The online security challenges universities face and security-related effects of end-user behaviour were similarly evaluated. The information helped to assess the security behaviour of students at universities. The chapter examined several theoretical frameworks before explaining the theoretical framework adopted in this research, the Protection Motivation Theory. Chapter three uses the literature reviewed in the second chapter and the research problem in chapter one to explain the research methodology employed in this research to ensure that it's successfully conducted.

CHAPTER 3

Research Methodology

3.1 Introduction

Chapter three explains the research method utilised in this study, sample and population size. The procedures utilised to design the research instrument, data collection method, and ethical considerations were discussed. In addition, the statistical approach used for data analysis was also explained.

3.2 Research Design

A research design is an assessment that exists within research methodologies such as the qualitative, quantitative, and mixed-method to provide a definite direction for a research approach (Creswell, 2014). A survey design was utilised for this study to collect data online due to covid restrictions. A survey design is associated with the quantitative method (Saunders, Lewis, & Thornhill, 2019). The University of KwaZulu-Natal was the chosen tertiary institution to conduct the study. The research focused on students that own and use smartphones to connect to the internet through the university's Wi-Fi. Responses from the research participants facilitated getting and analysing the relevant information required to understand the research topic.

3.3 Research Methodology

A research methodology is a detailed method and plan used to conduct a study (Langkos, 2014). Research can use qualitative, quantitative, or mixed-method. The quantitative method tests objective theories through the assessments of connections between variables. The qualitative method examines and tries to understand how people or groups of people attribute to a social issue. The mixed-method combines both quantitative and qualitative methods (Creswell, 2014). The quantitative method was chosen to understand the research problem through smartphone users' opinions collected via a survey. It was easy to collect and analyse data from hundreds of people using the quantitative survey method, unlike the qualitative method, which requires more procedures and time to collect data and analyse when using focus groups, interviews and observations (Saunders et al., 2019). The quantitative technique enabled the researcher to receive data for statistical analysis to fulfil the study's objectives.

3.4 Study Site

The study site is where the research will be conducted to collect data (Creswell, 2014). The location selected was the University of KwaZulu-Natal, Westville campus. The students from the university utilise and access websites, applications, and other information systems through devices such as smartphones while connected to the university's Wi-Fi. The study site also provided easy access for the researcher to collect opinions from students using smartphones on campus.

3.5 Target Population

The target population are the individuals a researcher is interested in researching (Majid, 2018). The University of KwaZulu-Natal students were the target population for the study. Students who use smartphones on campus access different university information systems for education and support services. The University of KwaZulu-Natal mobile websites and applications, such as MyUKZN that provide students with information, and self-service capability, are examples of such an information system. Additionally, the population were smartphone users that can fall victim to the problem being investigated.

3.6 Sampling Strategies

A quantitative research method consists of two major sampling strategies: probability and non-probability sampling. Probability sampling uses randomly chosen people from a population to become the sample size. In contrast, non-probability sampling does not involve random selection (Taherdoost, 2016). A non-probability method, called convenience sampling, was utilised to determine the population for this research. Convenience sampling identifies the characteristics of the sample population with consideration to the researcher's proximity to the target population for the ease of data collection (Saunders et al., 2019). The researcher is studying at the University of KwaZulu-Natal Westville campus and had easy access to collect opinions of students who use smartphones at the campus.

3.7 Sample Size

A research sample size is when some people are chosen proportionately from the actual population size to assess the entire population's behaviour (Singh & Masuku, 2014). When a research population is large, a fraction must be selected with the error margin stipulated at +/- 4%. This makes the confidence level of the actual population 95%, and the result of using 400

people of an actual population size will give the same error margin of $\pm 4\%$ (Creswell, 2014). The total number of registered students at UKZN as of June 2020 was 46,770, and 12,102 were from the Westville Campus (University of KwaZulu-Natal, 2020). The statistics for students' smartphones connected to the institution's network were not unavailable on the university's information portal at the time of this research. Therefore, the study utilised a sample size of 400 out of the 12,102 enrolled UKZN students as of June 2020 that use smartphones on campus, using the confidence level above.

3.8 Sample

The study's sample population consisted of registered undergraduate and postgraduate students studying at diverse disciplines at the University of KwaZulu-Natal, Westville campus. These were students who connect their smartphones to the university's Wi-Fi on the Westville Campus.

3.9 Data Collection Method

Research can use various data collection instruments based on the best methodology that will help yield the correct findings. When conducting research, there are three methods: qualitative, quantitative, and mixed-method. The qualitative method uses words to deduce conclusions; the quantitative method uses numbers to produce results, while the mixed method combines the characteristics of both the quantitative and qualitative methods (Creswell, 2014). Data collection approaches include but are not limited to questionnaires and interviews (Shanks & Bekmamedova, 2018).

With interviews, respondents and researchers have a discussion to gather necessary information (Phillips, 2016). In contrast, a survey is a type of research instrument that is easy to explain and understand, and it is used to collect a large amount of data. When data is collected through the survey method, questionnaires are used (Saunders et al., 2019).

Diverse research on protection motivation towards technology security has successfully utilised the questionnaire to gather data (Boerman et al., 2021; Dang-Pham & Pittayachawan, 2015; Yoon, Hwang, & Kim, 2012). Hence, the researcher utilised structured questionnaires for data collection; it provided a numeric description of opinions among students.

The anonymity of survey respondents is guaranteed (Creswell, 2014). Data collection using a questionnaire is timely and relatively convenient to use. It is easy to administer in public places (Kabir, 2016). For data collection, a question format can either be open-ended or close-ended. Open-ended questions are often asked during interviews to get unbiased views of respondents (Phillips, 2016). Close-ended questions answer questions by ticking the most appropriate option as a response. Close-ended questions are also easy to examine statistically; nevertheless, it limits possible responses given by participants (Jackson, 2016).

The quantitative method was chosen because it was easier and faster to collect and analyse data from hundreds of people using a survey (Saunders, Lewis, & Thornhill, 2016). A questionnaire was used, as a quantitative research instrument. The questionnaire allows timely collection and analysis of data from many people, unlike an interview that takes time to set up and analyse (Booth, Noyes, Flemming, Gerhardus, Wahlster, Van der Wilt, Mozygemba, Refolo, Sacchini, Tummers, & Rehfuess, 2016). Hence, the data collection tool best suited to get timely information from many students conveniently was the questionnaire. A close-ended questionnaire was used to gather data in this research.

The questionnaire for this study was split into three sections. First is the demographics that consisted of gender, age, educational level, and internet usage time. The second section focused on the three sub-constructs of threat appraisal. The third section focused on the three sub-constructs of coping appraisal from the protection motivation theory. The segmentation of the questions allowed participants to read through the questions, answer and track the progression of the data collection activity effortlessly. The data format scales such as the nominal and ordinal scales of the questions presented were efficiently coded quantitatively into the SPSS software.

3.10 Ethical Considerations

Before data can be collected for analysis, ethical considerations, and permission needs to be obtained. All ethical issues must be considered for research. Researchers are required to seek ethical approval from an organisation's gatekeeper to ensure the organisation's code of ethics is followed (Creswell, 2014). Ethical clearance is also vital due to the limits of inquiry and legislative differences in people's rights and data protection. The ethical policy on research

ethics must be adhered to by researchers (Parveen & Showkat, 2017). The researcher obtained an ethical clearance from the University of KwaZulu-Natal leadership to conduct this study.

To obtain ethical clearance, the researcher first applied for a gatekeeper's letter through the email which was sent to the UKZN registrar seeking permission to conduct the study at UKZN Westville Campus. A gatekeeper's approval letter was granted by the university which allowed the researcher to collect data on the university campus. The researcher then signed up on the Research Information Gateway platform of UKZN using personal students' LAN log-in details. The successful sign up enabled the researcher to access the ethics application form. The ethics electronic form tabs were filled by providing key student's information, project details, research methodology procedures, and uploading required documents as attachments.

The attachments were Portable Document Format (PDF) documents uploaded under the attachment section. These documents consisted of the research instrument, the Humanities and Social Sciences Research Ethics Committee (HSSREC) informed consent letter for the School of Management, IT & Governance. In addition, the gatekeepers' approval letter, the curriculum vitae of the researcher, the proposal outcome letter, and the email of proposal approval were also uploaded. Upon completing the form, the application was saved and sent to the researcher's supervisor for approval. The research office electronically sent the application outcome, the ethical clearance approval letter to the researcher.

The researcher issued informed consent letters to the participants about the study prior to data collection. The population must not be pressured into signing the consent form (Creswell, 2014). Participants must know the type of questions to be asked, the data usage method, and problems or potential problems linked to the data collection. The target population must also sign the consent letter before taking part in the research which informs them of their right to withdraw at any point, with respondent's anonymity and protection of information (Fleming & Zegwaard, 2018).

3.11 Data Collection

Data collection is the gathering of information through a structured or semi-structured method (Creswell, 2014). Data was collected from both UKZN postgraduate and undergraduate students at the Westville Campus. The information collection format was initially paper-based

questionnaires until the national lockdown was implemented in South Africa. Data collection was then switched to an online method following the advice from the University of KwaZulu-Natal's research office. An electronic amendment request was sent to the Humanities and Social Sciences Research Ethics Committee (HSSREC) research office.

The request email quoted the protocol reference number for the approved ethical clearance. The email also stated the need to follow the new data collection protocol set by the research office. The new protocol indicated the need for ethical clearance amendment to adapt from physical data collection method to an online format. The request for the ethical clearance amendment for data collection was approved by the research office and sent electronically to the researcher.

Data was collected online through a Google form advertised on the university's online notice system. After the collection objective was met, data was exported through a Microsoft Excel worksheet to the researcher's local computer. The Excel worksheet was formatted for compatibility in the SPSS analysis software. The statistical analysis was conducted on the collected data to get the respondents' viewpoint. The analysis then enabled the derivation of valuable information from the collected data and also eliminated bias by the researcher on the research problem.

Data analysis was conducted firstly, to answer the research questions and achieve the research objectives to understand the factors influencing the security practices of smartphone users. Secondly, to know if these practices have security implications that can lead to cyberattacks on the University of KwaZulu-Natal's information systems. Thirdly, to assess if students' possession of good security skills ensures implementing suitable security measures.

3.12 Measurements

Variable measurement is essential before the commencement of data analysis. It is necessary to establish the research constructs and measurement method for the constructs (Loeb, Dynarski, McFarland, Morris, Reardon, & Reber, 2017). The measurement scale is part of data collection, analysis, and research output. Collected data, which can either be constants or variables, are values or measurements. A constant does not change while changes in values

characterise variables. Variable data are usually used in research; types include nominal, ordinal, continuous, and discrete (Mishra, Pandey, Singh, & Gupta, 2018).

For this research, the nominal and ordinal scales were utilised due to the types of questions asked. The nominal scale classification distinguishes between response characteristics. The ordinal scale differs from the nominal because it arranges classifications in a ranking, increasing or decreasing the order of the response scale (Aini, Zuliana, & Santoso, 2018). The Dichotomous scale which is a two-point nominal scale was used for questions in the demography section. The Likert scale and ordinal scale for measuring attitude were used in the remaining sections of the questionnaire.

3.13 Data Analysis

Data analysis displays all statistical tests conducted (Creswell, 2014). The statistical research method can either be descriptive or inferential. The descriptive method finds patterns in data (Loeb et al., 2017). The inferential method is a statistical calculation to derive correlation and results between research data (Kaur, Stoltzfus, & Yellapu, 2018). The descriptive analysis was used to get and statistically present the opinions of research participants as tables, pie charts and histograms. The inferential analysis was also used to derive comprehensive inference from participants threat and coping appraisals to answer the three research questions of the study. Hence, both the descriptive and inferential analysis was used to analyse the data on questionnaires collected from the research population. The data collected from the sample population was three hundred and eighty-four, 384 in total.

During data analysis, inferential tests such as the T-Test and Univariate Analysis of Variance (ANOVA) were used to analyse both independent and dependent constructs or variables of a study (Creswell, 2014). The Analysis of Variance (ANOVA) is a test that defines the connection and effects an independent variable has on dependent variables (Pallant, 2016). The Statistical Package for the Social Sciences, SPSS software program was essential to enable descriptive outputs such as charts, frequencies, inferential and established methods (George & Mallery, 2016).

3.13.1 Analysis Overview

Data analysis was conducted on all collected research data using descriptive and inferential analytic methods. The data utilised for the majority of this study fall under the categorical data, which are nominal and ordinal, while the remaining data, for example, age, is considered continuous data. Nominal data are named categories; this consists of the questions used to gather data on respondents' gender and educational level. The age of the sample population is classified as continuous or interval data, which utilises a range of numbers to obtain the necessary information. The ordinal data, which are ordered categories, are summarised data by median values. The Likert scale used in this study is an example of an ordinal data format. It formed the structure of most of the data collected. Hence, with the use of appropriate methods and tests, the data analysis was conducted.

The descriptive analysis method uses frequencies to present result outputs as tables, crosstabs, bar and pie charts and much more. A descriptive analysis displays the results as summarised percentages, while the inferential test investigates dependent variables independent of the research questions (Creswell, 2014; Langkos, 2014). Descriptive analysis was conducted on all questions of the study. Inferential analysis and tests conducted further enabled the three research questions posed in chapter one to be answered. Correlation analysis was conducted to get inference between variables because the research problem is correlational. The utilisation of correlational statistics tests the association between two or more variables (Schober, Boer, & Schwarte, 2018).

According to the data measurement, 41 out of 44 of the questions are ordinal. Given the format of the questions, appropriate tests were used to generate inferential analysis after the descriptive analysis. An inferential T-test was done. The T-test assesses the characteristics of the population (Kim & Park, 2019). The ANOVA was also conducted to get inferential results and data interpretation. Next, the data quality control for the study was conducted.

3.14 Data Quality Control

The data control test is important for research. The proof of validity and reliability are precursors to ensure the integrity and quality of a chosen research instrument. A reliability test is the stability of research findings (Mohajan, 2017). A research instrument validity indicates

the level at which the tool measures the intended measures reflecting the research accuracy (El Hajjar, 2018).

In conducting this research analysis, the Cronbach's alpha reliability test was used to validate the findings. Cronbach's alpha reliability test was conducted after the correlational test. Cronbach's alpha reliability test calculates the internal consistency to get a sufficient reliability scale for collected data (Pallant, 2016). The test enabled the researcher to test for the overall response consistency of the survey. The minimum acceptable alpha reliability level is 0.6, and the widely accepted alpha should be 0.70 or greater. However, a very high alpha signifies redundancy in items (Taber, 2017).

3.15 Conclusion

The research methodology explained the procedure used to conduct the study. The purpose and method of data collection were discussed. The use of SPSS as the statistical analysis package to process quantitative data was also explained. The data analysis and data quality control process of the study was also described. Chapter 4 used the research methodology from chapter 3, the theoretical framework in chapter two and the research problem in chapter one to analyse and interpret collected data.

CHAPTER 4

Analysis, Findings, and Interpretation

4.1 Introduction

This chapter analyses and interpret collected data and present the research findings. Data analysis is a vital part of research as it helps provide the research outcome. It reports on information gathered from a research survey and presents the findings. Chapter four explicitly analyse and discuss the descriptive and inferential analysis of the study and explain how the results answer the three research questions stated at the beginning of this study.

4.2 Rate of Response

In total, 384 out of 400 questionnaires were collected online from UKZN students at the Westville Campus. The researcher considered the number of registered students at the University of KwaZulu-Natal. Prior to the implementation of covid protocols by the university, the researcher used the convenience sampling method to distribute the questionnaire and collected data from students at the Westville campus. The convenience sampling method was used because the researcher is a registered student at the Westville campus, and this provided proximity to the sample population. However, due to the spread of the covid-19 virus, data collection was moved online platform. The online questionnaire link was sent to Westville students through the university's notice system to student emails.

An estimated 46,770 students were registered as of June 2020, and 12,102 of these students are from the Westville Campus. For a large research population, a fraction of the population is chosen with the error margin stipulated at $\pm 4\%$. The error margin makes the confidence level of the actual population 95%, and the result of using 400 individuals of an actual population size will provide an equal error margin of $\pm 4\%$ (Creswell, 2014). The initial sample size of the research was 400 students, and the researcher obtained 384 completed questionnaires from participants.

Before data collection, all respondents were requested to spare 10 minutes from either academic or other personal obligations to fill the online questionnaire. The physical questionnaires were collected after respondents filled each survey, while online questionnaires

were submitted electronically after completion. All the questionnaires were deemed usable for the research because each field in the online form was formatted as "Required" to stop respondents from skipping questions before submitting.

The study's questionnaire (Appendix B) comprised of three sections utilising the Protected Motivation Theory constructs. The sections present are Section one, Demographic data that included gender, age, education level of students, and smartphone browsing the internet frequency under the first section. Section two comprises data regarding Threat appraisal (Perceived vulnerability, Perceived severity and Rewards). Section three includes Coping appraisal (Self-efficacy, Response efficacy and Response costs) constructs to answer the research questions. The questionnaire has forty-four questions in total; the questionnaire had twenty-one major questions with twenty-eight sub-questions.

4.3 Findings of the study

The study's findings are presented in subsequent paragraphs, the reliability of the collected data is tested using the Cronbach's Alpha test. The reliability test precedes the descriptive and inferential analysis used to answer the research questions asked in chapter one. A descriptive analysis was conducted on all the questionnaire's questions to generate results displayed as frequencies, tables, and charts. The descriptive analysis provided insights into students' security practices when operating smartphones connected to the university's Wi-Fi. The One-Sample T-Test then helped derive P-values for all questions to test for a null hypothesis. A null hypothesis asserts that a research result will not indicate an effect but is controlled by scientific testing (Kabir, 2016). The P values of each question were present with the descriptive analysis.

The initial analysis section is followed by a correlation inference between threat appraisal and coping appraisal data. Given that the ordinal data format is 41 out of 44 questions, appropriate tests were used to conduct inferential analysis. The utilisation of correlational statistics tests the association between two or more variables. The ANOVA test was conducted to get inferential findings and data interpretation to answer the three research questions posed in chapter one. This inferential test enabled correlation analysis between students' threat appraisal and coping appraisal to determine factors that influence their security practices. How derived factors of influence can affect UKZN information systems? If possessing good security skills leads to good security practices?

4.4 Reliability Test

The Cronbach alpha test examines the reliability of research variables and statistical outcome which indicates the quality of a research instrument (Taber, 2017). A reliability test, a Cronbach's Alpha test, was conducted on the study's variables, and evident from Table 4.1, the data gathered is reliable, as displayed by the number 0.751. Thus, the survey items of this research possess an acceptable scale of reliability for the gathered responses and the data is also good.

Table 4.1 Cronbach's Alpha test.

Reliability Statistics	
Cronbach's Alpha	N of Items
.751	44

4.5 Demographics and study variables analysis

The descriptive analysis for all questions is explained with the P values of each t-test. The t-test was conducted to test the null hypothesis that the sample population is the same as the population's mean.

The summarised respondents' demographic statistics are presented in Table 4.2. The demography data indicated that most respondents were of the female gender, 61.20%. In comparison, the remaining 38.80% were male, indicating that the gender distribution is not equally balanced. The t-test for the respondents' gender is statistically significant, p-value, $t = 24.578$, $p < 0.001$.

Most of the respondents are young; 77.86% represent the 18 – 24 age group, and the second-largest age group of respondents, 16.41%, indicates ages between 25 – 34, which are middle-aged respondents. The t-test for the respondents' age is statistically significant, p-value, $t = 23.596$, $p < 0.001$.

The respondents consisted of both undergraduate students, 74.48% and postgraduate students, 25.52%. The t-test for the respondents' educational level is statistically significant, p-value, $t = 11.456$, $p < 0.001$.

For question 4 findings, most respondents, 56.77%, said that when using a smartphone connected to the UKZN network, the average time spent online per day is less than 5 hours, and another 33.07% spend 5 to 10 hours online per day. A study validated the above findings indicating that university students that use smartphones spend an average of four hours on their smartphone to access the internet (Atas & Celik., 2019). The t-test for the time per day respondents spend using a smartphone connected to the UKZN network is statistically significant, p-value, $t = -41.597$, $p < 0.001$.

Table 4.2 Demography.

Measure	Items	Percent
Gender	Male	38.8
	Female	61.2
Age	18 – 24	77.86
	25 – 34	16.41
	35 – 44	4.95
	45 or older	0.78
Educational Level	Undergraduate	74.48
	Postgraduate	25.52
When using a smartphone connected to the UKZN network the average time that I spend online per day is	Less than 5 hours	56.77
	5 - 10 hours	33.07
	10 - 15hours	9.64
	15 - 20 hours	0.52
	More than 20 hours	-

It is evident from question 5.1 findings, as seen in Figure 4.1 that most respondents, 69.27%, agreed that when using a smartphone connected to the UKZN Wi-Fi, UKZN may experience a data breach if the student disregards UKZN online security guideline. 20.05% had a neutral view, 5.73% strongly agreed, another 2.60% strongly disagreed, and 2.34% disagreed with the statement. The above-derived result establishes that most students who use smartphones at the UKZN Westville campus agree that a data breach can occur due to students' actions. The t-test, when using a smartphone connected to the UKZN Wi-Fi, UKZN may experience a data breach if the student disregards UKZN online security guideline, is reported to be statistically significant, p-value, $t = 19.975$, $p < 0.001$.

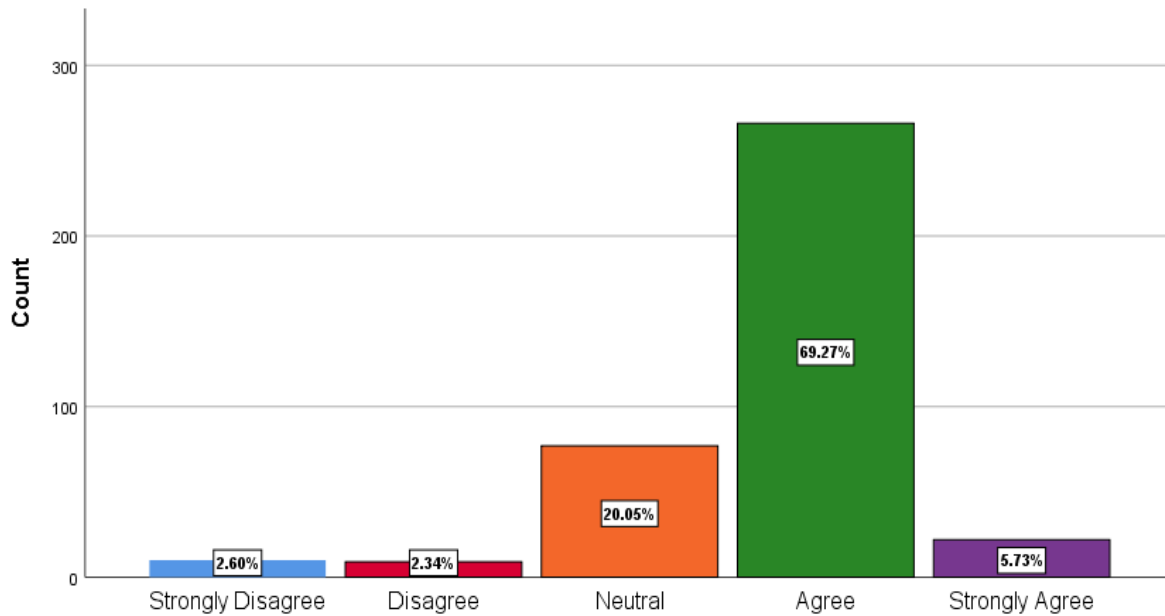


Figure 4.1 Data Loss if UKZN Online Security Guideline is Disregarded.

In question 5.2, many respondents, 81.77%, agreed that when using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if the individual disregard UKZN online security guideline. Respondents with a neutral view were 11.46%, with 4.95% strongly agreeing, but 1.56% disagreed, and the remaining 0.26% strongly disagreed. The derived result established that most students who use smartphones at the UKZN Westville campus agree that UKZN can experience a data loss due to personal security disregard. The t-test, when using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if the individual disregard UKZN online security guideline, is reported to be statistically significant, p-value, $t = 35.850$, $p < 0.001$. Past research indicates that the proper security actions are often taken for granted by people (Holicza & Kadena, 2018).

According to the result gathered in question 5.3, 54.17% of respondents agreed that when using a smartphone connected to the UKZN Wi-Fi, UKZN productivity can experience a disruption of services attack if the individual disregards the UKZN online security guidelines. Another set of respondents, 40.10%, had a neutral view of an interruption of service, 3.91% strongly agreed, 1.30% strongly disagreed, and another 0.52% strongly disagreed with the statement. The findings indicate that most students that use smartphones at the UKZN Westville Campus agree that a potential disruption of service at UKZN can occur due to their actions. Figure 4.2 illustrates that the t-test, when using a smartphone connected to the UKZN Wi-Fi, UKZN

productivity can experience a disruption of services attack if the individual disregards the UKZN online security guidelines, is statistically significant, p-value, $t = 19.030$, $p < 0.001$.

Table 4.3 T-Test for Perceived Vulnerability Threat Appraisal.

Questions	t	Sig. (2-tailed)
5.1 When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience a data breach if the student disregards UKZN online security guideline.	$t = 19.975$	$P < 0.000$
5.2 When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if the individual disregard UKZN online security guideline.	$t = 35.850$	$P < 0.000$
5.3 When using a smartphone connected to the UKZN Wi-Fi, UKZN productivity can experience a disruption of services attack if the individual disregards the UKZN online security guidelines.	$t = 19.030$	$P < 0.000$

As seen in Figure 4.3, the data gathered in question 6.1; findings revealed that 50.78% of respondents strongly agreed that when using their smartphone to connect the UKZN Wi-Fi, a data breach may result in a significant problem for UKZN, while 42.97% agreed, 4.34% had a neutral view and 1.82% disagreed. Many respondents strongly agree that a data breach can cause a significant problem for UKZN. The inferential t-test, when using their smartphone to connect the UKZN Wi-Fi, shows a data breach that may result in a significant problem for UKZN and it is reported to be statistically significant, p-value, $t = 41.980$, $p < 0.001$.

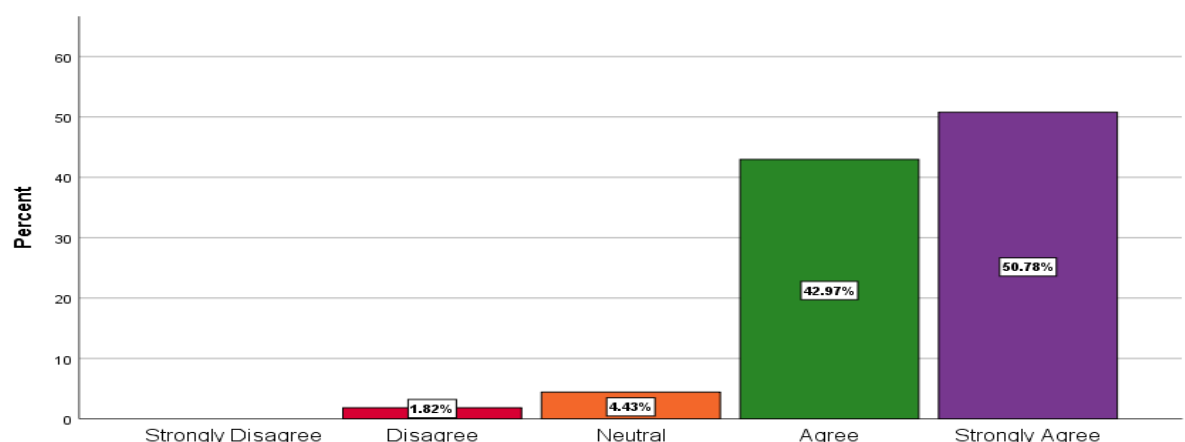


Figure 4.2 A Data Breach May Result in a Major Problem for UKZN.

In question 6.2, most respondents, 69.53%, strongly agreed that when using my smartphone to connect to the UKZN Wi-Fi, an unknown change in my student account password indicates a significant threat while 23.18% agreed to the statement. In comparison, 5.47% had a neutral view, 1.04% of respondents disagreed and 0.78% strongly disagreed with the view. The t-test, when using my smartphone to connect to the UKZN Wi-Fi, shows an unknown change in my student account password which indicates a significant threat reported to be statistically significant, p-value, $t = 43.904$, $p < 0.001$.

Apparent from question 6.3 analysis, many of the respondents, 43.23%, had a neutral view that when using my smartphone to connect the UKZN Wi-Fi, the presence of regular advertisement pop-up alerts indicates a significant threat, with 22.14% agreeing to the question, while 13.80% disagreed, 12.24% strongly disagreed, and the remaining 8.59% strongly agreed. The 2020 Kaspersky threat report validated the analysis, indicating that unwanted adware apps top the malware found on mobile devices in the first quarter of the year, signifying 49.9% (Kaspersky b, 2020). The t-test, when using my smartphone to connect the UKZN Wi-Fi, the presence of regular advertisement pop-up alerts indicates a significant threat, is reported to be statistically not significant, p-value, $t = 0.187$, $p < 0.852$.

Question 6.4 deals with financial loss; where 57.81% strongly agreed that when using my smartphone to connect the UKZN Wi-Fi, financial loss due to data breach indicates a significant threat, while 25.26% of respondents agreed to this. Subsequently, 9.90% had a neutral view, 3.65% disagreed and 3.39% constituted a low percentage that strongly disagreed with the presence of financial loss as a severe threat. The t-test, when using my smartphone to connect the UKZN Wi-Fi, financial loss due to data breach indicates a significant threat is reported to be statistically significant, p-value, $t = 25.101$, $p < 0.001$. A past study reported that a group of Iranian hackers took intellectual property worth \$3.4 billion from multiple universities worldwide (Cohen, 2018) indicating a major financial threat.

According to the data gathered in question 6.5, 54.69% of respondents agreed that when using my smartphone to connect to the UKZN Wi-Fi, receiving strange text messages from unknown phone numbers indicates a significant threat. Another 26.56% strongly agreed with this view, 8.33% had a neutral view while 6.77% disagreed and 3.65% strongly disagreed with this view. The t-test, when using my smartphone to connect to the UKZN Wi-Fi, receiving strange text messages from unknown phone numbers indicates a significant threat is reported to be

statistically significant, p-value, $t = 18.883$, $p < 0.001$. In 2020, research indicated that smishing is used to send malicious links of dangerous websites and applications via texts to people (Mishra & Soni, 2020).

In question 6.6, many respondents, 39.84%, agreed that when using my smartphone to connect the UKZN Wi-Fi, receiving strange calls from unknown phone numbers indicates a significant threat, with 25.52% strongly agreeing. 17.45% had a neutral view, 10.68% disagreed, and 6.51% strongly disagreed. The t-test, when using my smartphone to connect the UKZN Wi-Fi, receiving strange calls from unknown phone numbers indicates a significant threat is reported to be statistically significant, p-value, $t = 11.380$, $p < 0.001$.

From the gathered data in question 6.7, a majority, 83.59%, of respondents strongly agreed that when using my smartphone to connect to the UKZN Wi-Fi, receiving strange emails from unknown sources indicates a significant threat. Another 11.46% agreed, 3.65% had a neutral view, while 0.78% disagreed and 0.52% strongly disagreed. The t-test, when using my smartphone to connect to the UKZN Wi-Fi, receiving strange emails from unknown sources indicates a significant threat is reported to be statistically significant, p-value, $t = 57.647$, $p < 0.001$. A 2019 study by Chapman supported this finding, which reported a phishing attack aimed at students is a scholarship fraud via email that requested both personal and banking details of the victim (Chapman, 2019).

The findings from question 6.8 establish that when using my smartphone to connect to the UKZN Wi-Fi, the presence of unknown mobile applications indicates a significant threat. Many respondents, 66.41% agreed to this, 14.06% strongly agreed and 9.90% held a neutral view. However, 6.51% of respondents disagreed with the statement, and 3.13% strongly disagreed. The t-test, when using my smartphone to connect to the UKZN Wi-Fi shows the presence of unknown mobile applications that indicates a significant threat reported to be statistically significant, p-value, $t = 18.503$, $p < 0.001$.

Figure 4.3 (Question 7) shows that most respondents, 53.13%, agreed that the lack of understanding of the UKZN online security guideline might result in a significant problem for UKZN. The number of respondents that strongly agreed is 22.92%, 13.80% had a neutral view, 5.73% strongly disagreed, and 4.43% disagreed. Past research indicated that a potential reason for individuals' failure to protect themselves online could be the lack of knowledge concerning

privacy consequences (Gerber et al., 2019). The t-test, the lack of understanding of the UKZN online security guideline might result in a significant problem for UKZN is reported to be statistically significant, p-value, $t = 16.010$, $p < 0.001$.

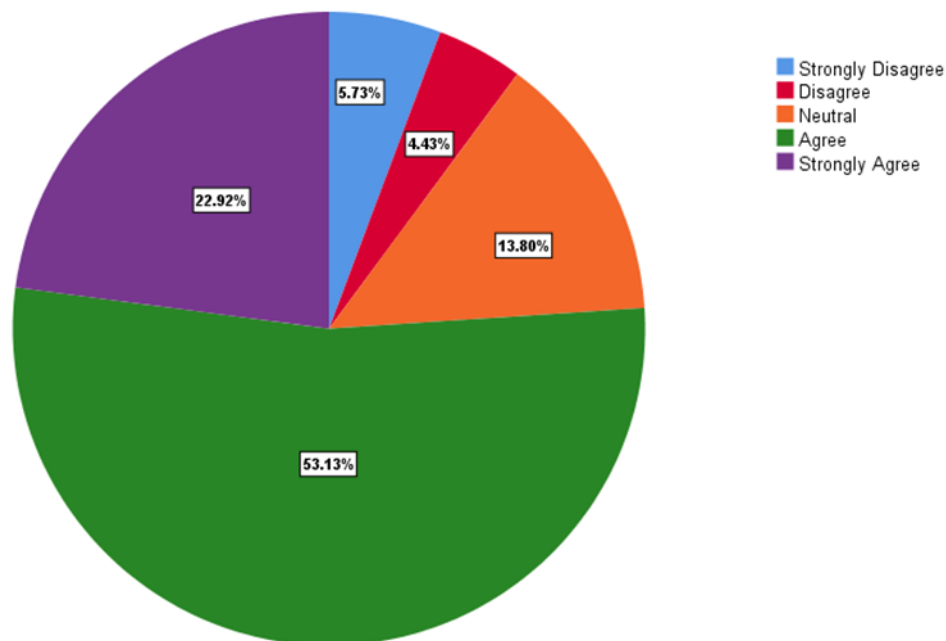


Figure 4.3 Lack of Understanding of Security Guideline.

Question 8 shows that many respondents, 69.01%, strongly agreed that UKZN would continually be susceptible to online threats if students do not implement UKZN online security measures on their smartphones, 21.35% agreed, 8.33% had a neutral view while 1.04% disagreed and 0.26% strongly disagreed with the question. The t-test result shows that UKZN would continually be susceptible to online threats if students do not implement UKZN online security measures on their smartphones which is statistically significant as shown by p-value, $t = 43.490$, $p < 0.001$.

Apart from the answers for question 9.1, most of the respondents, 51.56%, agreed that a disregard for UKZN online security guidelines by students could subject UKZN to a data breach, 25.26% had a neutral view, while 14.32% strongly agreed 5.73% strongly disagreed and the remaining 3.13% disagreed. A study conducted by Ogutcu (2016) reported that the exposure of organisational information systems to threats is related to smartphone users' security behaviours. The t-test shows a disregard for UKZN online security guidelines by students that could subject UKZN to a data breach. This is reported to be statistically significant, p-value, $t = 13.402$, $p < 0.001$.

Question 9.2 result indicates that 72.14% strongly agreed that students' disregard for UKZN online security guidelines could subject UKZN to financial loss. Furthermore, 26.56% agreed to this view, 1.30% had a neutral view which constituted a low percent. The t-test indicates a disregard for UKZN online security guidelines by students that could subject UKZN to financial loss and is reported to be statistically significant, p-value, $t = 69.316$, $p < 0.001$.

Question 9.3 shows that respondents 68.49% strongly agreed that a disregard for UKZN online security guidelines by students could subject UKZN to identity theft, 24.48% agreed to this view while 6.25% had a neutral perspective. Furthermore, 0.52% disagreed, and 0.26% strongly disagreed with the statement. The t-test shows a disregard for UKZN online security guidelines by students could subject UKZN to identity theft is reported to be statistically significant, p-value, $t = 48.063$, $p < 0.001$.

In question 9.4, most respondents 47.14% confirm that disregarding UKZN online security guidelines by students could subject UKZN to disruption of UKZN services, 26.30% had a neutral view while 13.28% strongly agreed with this view. In addition, 8.07% of the respondents disagreed and 5.21% strongly disagreed. The t-test shows a disregard for UKZN online security guidelines by students could subject UKZN to disruption of UKZN services is reported to be statistically significant, p-value, $t = 10.876$, $p < 0.001$.

Question 9.5 shows that a majority, 52.86% agreed, 20.57% had a neutral view, 15.36% strongly agreed that a disregard for UKZN online security guidelines by students could subject UKZN to compromised data in the online storage, Furthermore, 7.29% disagreed and 3.91% strongly disagreed with the above statement. The t-test indicates a disregard for UKZN online security guidelines by students that could subject UKZN to compromised data in the online storage. It is reported to be statistically significant, p-value, $t = 14.103$, $p < 0.001$.

Question 9.6 result, as indicated in Figure 4.4 below, establishes that students believe that a disregard for UKZN online security guidelines can subject UKZN to compromised student accounts. Many respondents, 71.88%, strongly agreed 22.40% agreed while 5.21% had a neutral view and 0.52% disagreed with the question. The t-test for students shows a disregard for UKZN online security guidelines by students which can lead to student accounts becoming compromised at UKZN. This is reported to be statistically significant, with a p-value, $t = 53.947$, $p < 0.001$.

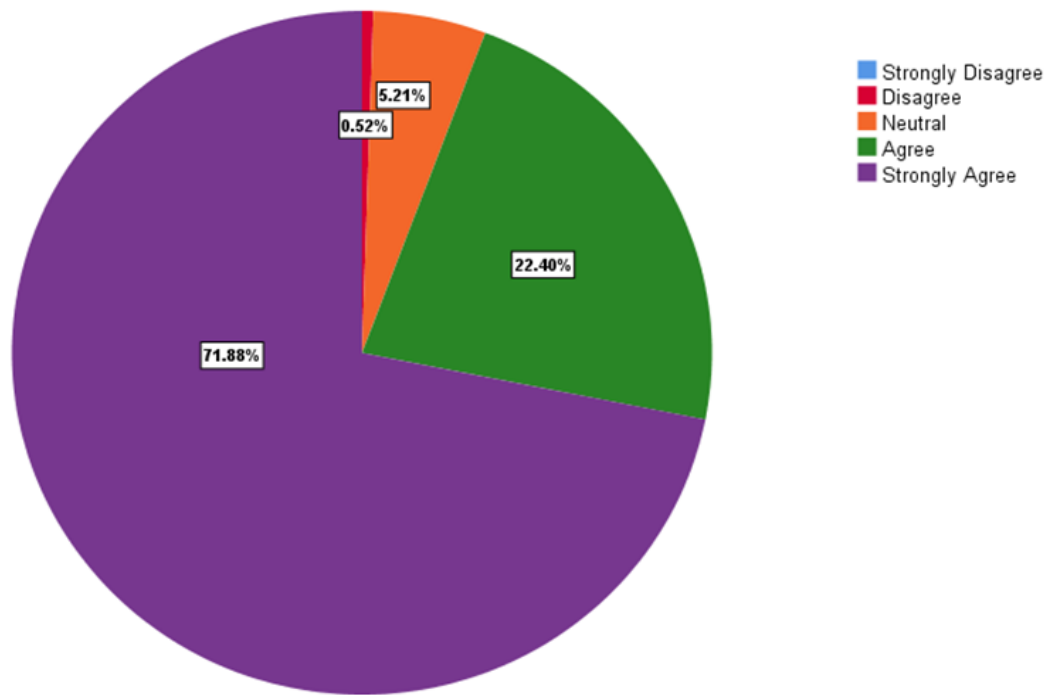


Figure 4.4 A Disregard for Online Security Guidelines can Compromise Student Accounts.

Question 9.7 shows that a majority of respondents, 69.53%, strongly agreed, 23.18% agreed that students believe a disregard for UKZN online security guidelines by them can subject UKZN to compromised staff accounts while 6.25% were of a neutral view. 0.78% of the respondents disagreed and 0.26% strongly disagreed. The t-test for students security behaviour shows a disregard for UKZN online security guidelines that can subject UKZN to compromised staff accounts and reported to be statistically significant, with a p-value, $t = 47.420$, $p < 0.001$.

Findings for question 9.8, revealed that most respondents, 51.82% agreed that a disregard for UKZN online security guidelines by students could subject UKZN to a compromised network, 33.85% strongly agreed, 10.42% had a neutral view, 2.86% disagreed and another 1.04% strongly disagreed. Concerning the derived percentage above, this result established that many university students agree that an individual's security actions can compromise the university's network. The t-test, a disregard for UKZN online security guidelines by students that could subject UKZN to a compromised network, is reported to be statistically significant, p-value, $t = 28.257$, $p < 0.001$.

In question 9.9, a significant number of respondents, 44.01%, agreed that a disregard for UKZN online security guidelines by me could subject UKZN to malicious software attacks. 27.08% strongly agreed, 17.45% had a neutral view, 7.81% disagreed, and the remaining 3.65%

strongly disagreed. The t-test shows a disregard for UKZN online security guidelines could subject UKZN to malicious software attacks and is reported to be statistically significant, p-value, $t = 15.811$, $p < 0.001$.

According to the data gathered in Table 4.4(Question 10.1), 65.63% of respondents strongly agreed that in the occurrence of a university-wide data breach, the UKZN ICS alerts students to fraudulent email through Microsoft Outlook, 14.06% agreed, 10.68% had a neutral view, but 5.99% disagreed and another 3.65% strongly disagreed. The t-test, in the occurrence of a university-wide data breach, the UKZN ICS alerts students to fraudulent email through Microsoft Outlook is reported to be statistically significant, p-value, $t = 23.316$, $p < 0.001$.

Table 4.4 The UKZN ICS Alerts Students to Fraudulent Emails.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	14	3.6	3.6	3.6
	Disagree	23	6.0	6.0	9.6
	Neutral	41	10.7	10.7	20.3
	Agree	54	14.1	14.1	34.4
	Strongly Agree	252	65.6	65.6	100.0
	Total	384	100.0	100.0	

Question 10.2 shows that 34.90% disagreed that in the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scams while 30.21% had a neutral view. Additionally, 27.34% strongly disagreed, 5.99% agreed and 1.56% of respondents strongly agreed with the above statement. The t-test, in the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scams is reported to be statistically significant, p-value, $t = -16.419$, $p < 0.001$.

In question 10.3, most respondents, 46.48%, disagreed that in the occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure students' smartphones. A neutral view was held by 27.15% of respondents, while 14.10% strongly disagreed, 10.18% agreed, and 2.09% strongly agreed. The t-test showed in Table 4.5 indicated that in the

occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure students' smartphones is statistically significant, p-value, $t = -12.784$, $p < 0.001$.

Table 4.5 T-Test for Response Efficacy Coping Appraisal.

Questions	t	Sig. (2-tailed)
10.1 In the occurrence of a university-wide data breach, the UKZN ICS alerts students to fraudulent email through Microsoft Outlook.	$t = 23.316$	$P < 0.000$
10.2 In the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scam.	$t = -16.419$	$P < 0.000$
10.3 In the occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure students' smartphones.	$t = -12.784$	$P < 0.000$

From the analysis of question 11, most respondents, 57.03%, disagreed that students constantly use UKZN information security guidelines to resolve online threats targeted at their smartphones. 14.32% had a neutral view. 13.80% strongly disagreed, 13.28% strongly disagreed, and the remaining 1.56% strongly agreed with the idea. The t-test, students constantly use UKZN information security guidelines to resolve online threats targeted at their smartphone, is statistically significant, with a p-value, $t = -14.464$, $p < 0.001$.

The findings of question 12 indicated that 54.69% of respondents disagreed that students utilise the UKZN ICS call service, which operates on weekdays, to resolve smartphone security problems, 18.49% strongly disagreed, 14.06% had a neutral view. At the same time, 9.90% agreed, and 2.86% strongly agreed. In the t-test, students utilise the UKZN ICS call service, which operates on weekdays to resolve smartphone security problems, is reported to be statistically significant, p-value, $t = -15.500$, $p < 0.001$.

According to the data gathered in question 13.1, 51.04% of respondents took a neutral view that in response to an online security threat targeted at students' smartphones, an anti-Virus

software is installed by the affected individual. In comparison, 30.21% disagreed, 10.42% strongly disagreed, 7.550% agreed, and 0.78% strongly agreed. Thus, many respondents had a neutral view about installing anti-virus on their smartphones. A study shows that most smartphones do not have pre-installed security software, yet people conduct tasks on these devices (Dawson and Wright, 2016). The t-test, in response to an online security threat targeted at students' smartphones, an anti-Virus software is installed by the affected individual is reported to be statistically significant, p-value, $t = -10.180$, $p < 0.001$.

In question 13.2, most respondents, 46.09%, agreed that in response to an online security threat targeted at students' smartphones, the affected individual uses multiple authentication methods to secure their email, with 23.18% strongly agreeing to this. In comparison, 18.75% had a neutral view, 9.64% disagreed, 2.34% strongly disagreed. Therefore, most respondents agree with the use of multiple authentications. Past research indicated that smartphones have little or no security indicator, making it easy to access malicious emails (David et al., 2017). The t-test, in response to an online security threat targeted at students' smartphones, the affected individual uses multiple authentication methods to secure their email is reported to be statistically significant, p-value, $t = 15.542$, $p < 0.001$.

Apparent from the gathered data in question 13.3 indicate that majority, 81.51% of respondents strongly agreed that in response to an online security threat targeted at students' smartphones, mobile applications used by UKZN are installed by the affected individual from recommended links, 16.67%, and 1.82% took a neutral view with the question. The t-test, in response to an online security threat targeted at students' smartphones, mobile applications used by UKZN are installed by the affected individual from recommended links is reported to be statistically significant, p-value, $t = 78.964$, $p < 0.001$.

Question 13.4 result establishes that in response to an online security threat targeted at students' smartphones, the affected individual pays attention to security messages for mobile application installation. Many respondents, 38.80% agreed, 29.95% had a neutral view, 16.93% strongly agreed. 11.98% disagreed, 2.34% strongly disagreed with this view. The t-test, in response to an online security threat targeted at students' smartphones, the affected individual pays attention to security messages for mobile application installation is reported to be statistically significant, p-value, $t = 11.153$, $p < 0.001$.

Evident from the gathered data in question 13.5, most respondents, 56.25%, agreed that in response to an online security threat targeted at students' smartphones, the affected individual changed passwords used for various platforms, 17.97% had a neutral view, while 15.89% strongly agreed. However, 7.29% disagreed, and another 2.60% of respondents strongly disagreed with this view. The t-test, in response to an online security threat targeted at students' smartphones, the affected individual change passwords used for various platforms is reported to be statistically significant, p-value, $t = 16.492$, $p < 0.001$.

In question 14, 53.39% of respondents agreed that it is easy for students to use the UKZN online security guideline to protect their smartphones against online threats. 19.53% had a neutral view, while 16.67% strongly agreed, 8.33% disagreed, and 2.08% strongly disagreed. The t-test, it is easy for students to use the UKZN online security guideline to protect their smartphone against online threats is reported to be statistically significant, p-value, $t = 16.076$, $p < 0.001$.

For question 15, most respondents, 70.83%, strongly agreed that it is easy for students to use UKZN online security guidelines if they follow an ICS technician's security instruction, with 24.74% agreeing. A few respondents, 3.13%, had a neutral view, and 1.30% disagreed. The t-test shows that it is easy for students to use UKZN online security guidelines if they follow an ICS technician's security instruction, which is statistically significant, p-value, $t = 53.278$, $p < 0.001$.

Question 16 findings indicate that 48.18% agreed that it is easy for students to take timely online protective measures on their smartphone, while 30.47% had a neutral view to this; subsequently, 10.16% strongly agreed, 9.13% disagreed, and 2.08% strongly disagreed that constituted a small percent. The t-test, it is easy for students to take timely online protective measures on their smartphone, is statistically significant, p-value, $t = 12.412$, $p < 0.001$.

For question 17, most respondents, 49.22%, agreed that it is easy for students to take adequate online security measures on their smartphones. In comparison, 29.55% had a neutral view, closely followed by 12.50% strongly agreeing. 6.25% disagreed, and another 2.08% strongly disagreed. The t-test shows that it is easy for students to take adequate online security measures on their smartphones and is reported to be statistically significant, p-value, $t = 14.605$, $p < 0.001$.

Apparent the result for question 18, the majority, 44.53% of respondents, stated that they possess the skill to protect themselves against online threats targeted at their smartphone, 28.39% constituted respondents had a neutral view, 14.06% strongly agree, 10.68% disagreed, and 2.34% strongly disagreed. Table 4.6 illustrates the t-test, students who possess the skill to protect themselves against online threats targeted at their smartphone analysis is statistically significant, p-value, $t = 11.952$, $p < 0.001$.

Table 4.6 T-Test for Self Efficacy Coping Appraisal.

Questions	t	Sig. (2-tailed)
14. It is easy for students to use the UKZN online security guideline to protect their smartphone against online threats.	$t = 16.076$	$P < 0.000$
15. It is easy for students to use UKZN online security guidelines if they follow an ICS technician's security instruction.	$t = 53.278$	$P < 0.000$
16. It is easy for students to take adequate online security measures on their smartphone.	$t = 12.412$	$P < 0.000$
17. It is easy for students to take adequate online security measures on their smartphone.	$t = 14.605$	$P < 0.000$
18. Students that possess the skill to protect themselves against online threats targeted at their smartphone.	$t = 11.952$	$P < 0.000$

Question 19 established that implementing security measures to protect a student's smartphone is not expensive as 53.13% of respondents disagreed with this question, 40.10% strongly disagreed. However, 5.21% had a neutral view, 1.04% agreed with the issue, and 0.52% strongly agreed. The t-test, which implements security measures to protect a student's smartphone is not expensive, is statistically significant, p-value, $t = -38.548$, $p < 0.001$.

From the gathered data in question 20, most respondents, 65.89%, indicated that implementing security measures to protect their smartphone takes less than five hours, while 18.49% utilise between five to ten hours. Another 4.69% use between fifteen to twenty hours, and a low

percent, 1.82%, takes more than twenty hours to implement the measures. In the t-test, the implementation of security measures to protect their smartphone takes less than five hours is statistically significant, p-value, $t = -28.868$, $p < 0.001$.

As seen in Figure 4.5 below, for question 21, most respondents, 80.47%, strongly agreed that the stress of implementing security measures on a student's smartphone discourages them from following UKZN security guidelines; 18.49% agreed. Fewer respondents, 0.78%, had a neutral view, while 0.26% disagreed with the influence of stress as the determinant of following security measures. The t-test, the stress of implementing security measures on a student's smartphone discourages them from following UKZN security guidelines, is reported to be statistically significant, p-value, $t = 79.164$, $p < 0.001$.

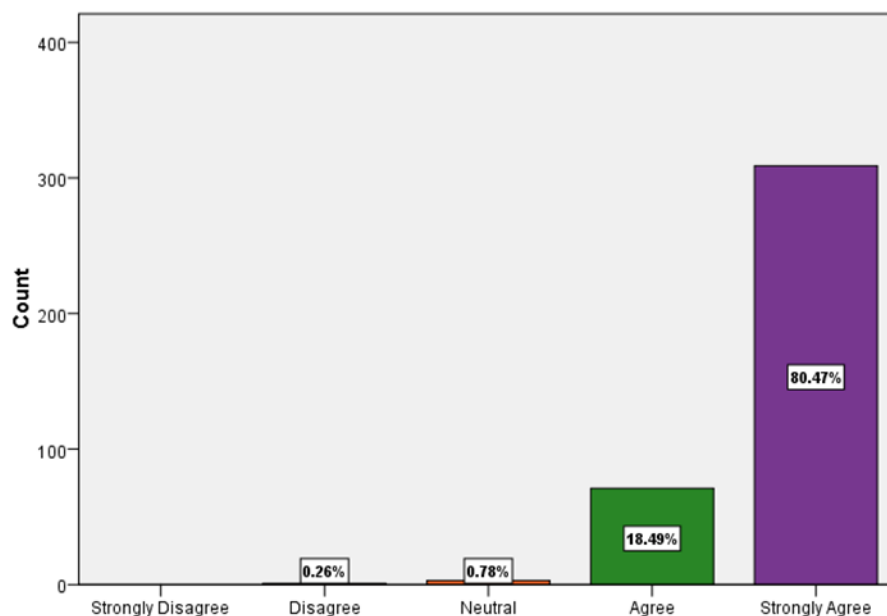


Figure 4.5 The Stress to Implement Security Measures Discourages Following UKZN Security Guidelines.

4.6 Protection Motivation Inferential Analysis

The ANOVA inferential test was used to analyse the study's data to answer the research questions and answer the research objectives stated in chapter one. The ANOVA test analyses the connection and effect between independent and dependent variables of a study (Pallant, 2016). The inference assesses how threat appraisal affects the coping appraisal of students. Research question one used sections 2 and 3 to analyse students' smartphone security behaviours. Research question two used the inferred security behaviours derived from research

question one to deduce threat rewards of students' security actions on UKZN information systems. However, the descriptive analysis of participants' opinions on threat rewards is derived from Section 2 of the questionnaire. Research question three used questions from Section 3 of the questionnaire to analyse a correlation between possessing security skills and security implementation.

4.6.1 Perceived Vulnerability analysis against Response Efficacy

For the ANOVA inferential analysis of research question one, “What are the factors influencing the security practices of UKZN smartphone users to counter security threats?” The outcome of the analysis helps to examine particular threat and coping appraisal factors to identify the factors influencing the security practices of students. The ANOVA test used perceived vulnerabilities data gathered for Section 2 of the questionnaire and analysed it against response efficacies data for Section 3. Both are subconstructs of threat appraisal and coping appraisal, respectively. The test examined if the perceived vulnerability assessment of students influences their response efficacy.

In the process of appraising a threat, the analysis investigates perceived vulnerability. Perceived vulnerability is the possibility that a harmful event will occur. The response efficacy assesses a person’s belief that adopting a specific behaviour response will divert a threat (Wu, 2020).

Inference test between questions 5(5.1 - 5.3) and 11

For research question one, the inferential tests between questions 5(5.1 - 5.3) and 11 analyses which perceived vulnerabilities influence students’ response efficacies.

Findings for questions 5.1 and 11 (Table 4.7) revealed the knowledge that UKZN may experience a data breach due to students’ disregard for UKZN online security guidelines. This has a significant influence $p < 0.024$ on students to use the UKZN security guidelines to protect their smartphones against online threats.

Table 4.7 Questions 5.1 and 11, The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	9.523	4	2.381	2.840	.024
Within Groups	317.717	379	.838		
Total	327.240	383			

For the analysis of questions 5.2 and 11 revealed that UKZN may experience a data loss due to students' disregard for UKZN online security guidelines and has no significant influence $p < 0.145$ on students to use UKZN security guidelines to protect their smartphones against threats.

The findings for 5.3 and 11 indicate, the awareness that UKZN may experience a disruption of services due to students' disregard for UKZN online security guidelines has no significant impact $p < 0.269$ on students to use the UKZN security guidelines to protect their smartphones against threats.

Inference test between questions 5(5.1 - 5.3) and 13.1

For research question one, the inferential tests between questions 5(5.1 - 5.3) and 13.1 indicated perceived vulnerabilities that influence students' response efficacies.

The findings from questions 5.1 and 13.1 indicate the knowledge that UKZN may experience a data breach due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.154$ on students to install anti-virus on their smartphones for protection against online threats.

From the result for questions 5.2 and 13.1, the awareness that UKZN may experience a data loss due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.763$ on students to install anti-virus on their smartphones for protection against online threats.

Findings for questions 5.3 and 13.1 indicated the knowledge that UKZN may experience a disruption of services due to students' disregard for the UKZN online security guidelines has

no significant influence $p < 0.183$ on students to install anti-virus on their smartphones for protection against online threats.

Inference test between questions 5(5.1 - 5.3) and 13.2

For research question one, the inferential tests between questions 5(5.1 - 5.3) and 13.2 revealed perceived vulnerabilities that influence students' response efficacies.

The analysis for questions 5.1 and 13.2 indicates the awareness that UKZN may experience a data breach due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.000$ on students to use multiple authentication methods to secure their emails against online threats.

The analysis of questions 5.2 and 13.2 revealed the knowledge that UKZN may experience a data loss due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.000$ on students to use multiple authentication methods to secure their emails against online threats.

The findings for questions 5.3 and 13.2, has shown the knowledge that UKZN may experience disruption of services due to students' disregard for the UKZN online security guidelines has no significant impact $p < 0.000$ on students to use multiple authentication methods to secure their emails against online threats.

Inference test between questions 5(5.1 - 5.3) and 13.3

For research question one, the inferential tests between questions 5(5.1 - 5.3) and 13.3 analyses indicate perceived vulnerabilities that influence students' response efficacies.

Questions 5.1 and 13.3 analysis indicated that the knowledge that UKZN may experience a data breach due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.614$ on students to install mobile applications from recommended links.

The findings from questions 5.2 and 13.3 indicate that the knowledge that UKZN may experience a data loss due to students' disregard for the UKZN online security guidelines has

no significant impact $p < 0.367$ on students to install mobile applications from recommended links.

In addition, findings for questions 5.3 and 13.3 revealed the knowledge that UKZN may experience disruption of services due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.253$ on students to install mobile applications from recommended links.

Inference test between questions 5(5.1 - 5.3) and 13.4

For research question one, the inferential tests between questions 5(5.1 - 5.3) and 13.4 analyses revealed perceived vulnerabilities that influence students' response efficacies.

The results for questions 5.1 and 13.4 indicate respondents' knowledge that UKZN may experience a data breach due to student disregard for the UKZN online security guidelines has no significant influence $p < 0.107$ on students to pay attention to security messages for mobile application installation.

Questions 5.2 and 13.4 (Table 4.8) results inferred that UKZN may experience a data loss due to students' disregard for the UKZN online security guidelines has a significant impact $p < 0.042$ on students to pay attention to security messages for mobile application installation.

Table 4.8 Questions 5.2 and 13.4 The Impact of Threat appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9.565	4	2.391	2.510	.042
Within Groups	361.058	379	.953		
Total	370.622	383			

The outcome for questions 5.3 and 13.4 show the knowledge that UKZN may experience disruption of services due to students' disregard for the UKZN online security guidelines has a significant influence $p < 0.011$ on students to pay attention to security messages for mobile application installation.

Inference test between questions 5(5.1 - 5.3) and 13.5

The inferential tests between questions 5(5.1 - 5.3) and 13.5 analyses which perceived vulnerabilities exploit students' responses for research question one. These inferential tests analyses research question one.

Questions 5.1 and 13.5 analysis shows that UKZN may experience a data breach due to students disregard for the UKZN online security guidelines has no significant influence $p < 0.000$ on students to change passwords used for multiple platforms in the event of threats occurrence.

According to questions 5.2 and 13.5, the knowledge that UKZN may experience a data loss due to students disregard for the UKZN online security guidelines has no significant influence $p < 0.120$ on students to change passwords used for multiple platforms in the event of threats occurrence.

Findings for questions 5.3 and 13.5 indicate that UKZN may experience disruption of services due to students' disregard for the UKZN online security guidelines has no significant influence $p < 0.000$ on students to change passwords used for various platforms in the event of threats occurrence.

4.6.2 Perceived Severity analysed against Self Efficacy

For the inferential analysis of research question one, "What are the factors influencing the security practices of UKZN smartphone users to counter security threats?" The outcome of the analysis helped to examine the perceived severity and self-efficacy factors to derive the influence of these factors on the security practices of students. The ANOVA test used perceived severity data gathered for Section 2 of the questionnaire and analysed it against self-efficacy data for Section 3. Both are subconstructs of the threat and coping appraisal respectively. The test examined if perceived severity influences students' self-efficacy.

In the process of appraising a threat, the analysis investigates perceived severity, which is the personal assessment of a person of the severe consequence that comes from a threat. In contrast, self-efficacy assesses a person's belief that they possess the capabilities and competence to do things or make choices by showing specific coping behaviours (Wu, 2020).

Inference test between questions 6(6.1 – 6.8) and 14

For research question one, the inferential tests between questions 6(6.1 – 6.8) and 14 analyses, indicate perceived severities influence students' self-efficacy.

Findings for Questions 6.1 and 14 indicate that a data breach may lead to a significant problem for UKZN has no significant influence $p < 0.130$ on students to use the UKZN online security guideline to protect their smartphone against online threats.

Evident Findings for questions 6.2 and 14 (Table 4.9) revealed the occurrence of an unknown change in a student's account password threat has a significant influence $p < 0.021$ on students to use the UKZN online security guideline to protect their smartphone against online threats.

Table 4.9 Questions 6.2 and 14 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9.389	4	2.347	2.926	.021
Within Groups	304.087	379	.802		
Total	313.477	383			

The results for questions 6.3 and 14 indicate that the presence of regular advertisement pop-up alerts has no significant influence $p < 0.079$ on students to use the UKZN online security guideline to protect their smartphones against online threats.

Questions 6.4 and 14, revealed that a financial loss due to a data breach is a significant problem although it has no significant influence $p < 0.082$ on students to use the UKZN online security guideline to protect their smartphone against online threats.

Furthermore, analyses of questions 6.5 and 14 revealed that receiving strange text messages from unknown phone numbers has no significant influence $p < 0.252$ on students to use the UKZN online security guideline to protect their smartphones against online threats.

Questions 6.6 and 14 indicate that receiving strange calls from unknown phone numbers has no significant influence $p < 0.123$ on students using the UKZN online security guideline to protect their smartphones against online threats.

The outcome from questions 6.7 and 14 indicates that receiving strange emails from unknown sources has no significant impact $p < 0.278$ on students in using the UKZN online security guideline to protect their smartphones against online threats.

The result of questions 6.8 and 14 shows that the presence of unknown mobile applications has no significant influence $p < 0.179$ on students to use the UKZN online security guideline to protect their smartphones against online threats.

Inference test between questions 6(6.1 – 6.8) and 15

For research question one, the inferential tests between questions 6(6.1 – 6.8) and 15 analyses which perceived severities influence students' self-efficacy.

The result for questions 6.1 and 15 shows that the knowledge that a data breach may lead to a significant problem for UKZN has no significant influence $p < 0.462$ on students to seek and follow an ICS technician's security instruction to protect their smartphones against online threats.

Findings for questions 6.2 and 15 indicate that an unknown change in a student's account password has no significant influence $p < 0.946$ on students seeking and following an ICS technician's security instruction to protect their smartphone against online threats.

The analysis of questions 6.3 and 15, revealed that the presence of regular advertisement pop-up alerts has no significant impact $p < 0.421$ on students seeking and following an ICS technician's security instruction to protect their smartphone against online threats.

The findings of questions 6.4 and 15 show that any financial loss due to a data breach is a major problem although it has no significant influence $p < 0.452$ on students seeking and following an ICS technician's security instruction to protect their smartphone against online threats.

For questions 6.5 and 15 (Table 4.10), the result illustrated that receiving strange text messages from unknown phone numbers significantly influenced $p < 0.012$ students to seek and follow an ICS technician's security instruction to protect their smartphone against online threats.

Table 4.10 Questions 6.2 and 15 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.734	4	1.183	3.286	.012
Within Groups	136.506	379	.360		
Total	141.240	383			

The answer to questions 6.6 and 15 analysis indicates that receiving strange calls from unknown phone numbers has a significant influence $p < 0.004$ on students to seek and follow an ICS technician's security instruction to protect their smartphones against online threats.

According to questions 6.7 and 15 (Table 4.11) result, receiving strange emails from unknown sources significantly influences $p < 0.005$ students to seek and follow an ICS technician's security instruction to protect their smartphones against online threats.

Table 4.11 Questions 6.7 and 15 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.342	4	1.335	3.724	.005
Within Groups	135.898	379	.359		
Total	141.240	383			

According to findings for questions 6.8 and 15, indicate the presence of unknown mobile applications that have no significant influence $p < 0.358$ on students to seek and follow an ICS technician's security instruction to protect their smartphones against online threats.

Inference test between questions 7 and 15

For research question one, the inferential tests between questions 7 and 15 analyses if a perceived severity influences a particular self-efficacy of students.

According to questions 7 and 15 (Table 4.12) analysis, students that do not understand online security guidelines are significantly influenced $p < 0.019$, by their lack of knowledge to seek the assistance of ICS technicians to resolve threat-related issues targeted at their smartphones. Past research confirms that individuals' intent to conduct secure behaviour when using technology varies based on personal security awareness, knowledge and actions (Zwilling et al., 2020).

Table 4.12 Questions 7 and 15 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.301	4	1.075	2.976	.019
Within Groups	136.938	379	.361		
Total	141.240	383			

Inference test between questions 8 and 15

For research question one, the inferential tests between questions 8 and 15 analyses if a perceived severity influences a particular self-efficacy of students.

Questions 8 and 15 analysis indicate that the knowledge of UKZN's continual online threat susceptibility due to lack of security implementation has no significant impact $p < 0.302$ on students to seek the assistance of ICS technicians to resolve threat-related issues targeted at their smartphones.

Inference test between questions 6(6.1 – 6.8) and 16

For research question one, the inferential tests between questions 6(6.1 – 6.8) and 16 analyses which perceived severities influence students' self-efficacy.

According to the findings for questions 6.1 and 16 (Table 4.13), the knowledge that a data breach may pose a problem for UKZN significantly influences $p < 0.033$ students to take timely online protective actions on their smartphones to protect themselves against online threats.

Table 4.13 Questions 6.1 and 16 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6.612	3	2.204	2.945	.033
Within Groups	284.347	380	.748		
Total	290.958	383			

The result from questions 6.2 and 16 indicate that an unknown change in a student's account password has a significant influence, $p < 0.006$, on students to take timely online protective measures on their smartphones to protect themselves against online threats.

According to questions 6.3 and 16 findings, the presence of regular advertisement pop-up alerts has no significant impact $p < 0.00$ on students taking timely online protective measures on their smartphones to protect themselves against online threats.

Questions 6.4 and 16 result show that the awareness that financial loss due to a data breach is a significant problem has no significant influence $p < 0.000$ on students to take timely online protective measures on their smartphones to protect themselves against online threats.

The analysis of questions 6.5 and 16 (Table 4.14) indicated that receiving strange text messages from unknown phone numbers has a significant influence $p < 0.001$ on students taking timely online protective measures on their smartphones to protect themselves against online threats.

Table 4.14 Questions 6.5 and 16 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	14.296	4	3.574	4.896	.001
Within Groups	276.662	379	.730		
Total	290.958	383			

The outcome of questions 6.6 and 16, receiving strange calls from unknown phone numbers, has no significant influence $p < 0.000$ on students to take timely online protective measures on their smartphones to protect themselves against online threats.

The result for questions 6.7 and 16 indicated that receiving strange emails from unknown sources has no significant impact $p < 0.129$ on students taking timely online protective measures on their smartphones to protect themselves against online threats.

Questions 6.8 and 16 (Table 4.15) analysis indicated that the presence of unknown mobile applications has a significant influence $p < 0.001$ on students taking timely online protective measures on their smartphones to protect themselves against online threats.

Table 4.15 Questions 6.8 and 16 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13.173	4	3.293	4.493	.001
Within Groups	277.785	379	.733		
Total	370.622	383			

Inference test between questions 6(6.1 – 6.8) and 17

For research question one, the inferential tests between questions 6(6.1 – 6.8) and 17 analyses which perceived severities influence students' self-efficacy.

From questions 6.1 and 17 results, the knowledge that a data breach may be a problem for UKZN has no significant influence $p < 0.111$ on students to take adequate online protective measures on their smartphones to protect themselves against online threats.

The findings from questions 6.2 and 17 (Table 4.16) indicate that an unknown change in a student's account password has a significant influence $p < 0.001$ on students taking adequate online protective measures on their smartphones to protect themselves against online threats.

Table 4.16 Questions 6.2 and 17 The Impact of Threat Appraisal on Coping Appraisal.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13.223	4	3.306	4.684	.001
Within Groups	267.462	379	.706		
Total	280.685	383			

According to questions 6.3 and 17 findings, the presence of regular advertisement pop-up alerts threat has no significant impact $p < 0.000$ on students to take adequate online protective measures on their smartphones to protect themselves against online threats.

The analysis for questions 6.4 and 17 indicates that the awareness that financial loss due to a data breach is a significant problem has no significant influence, $p < 0.000$ on students to take adequate online protective measures on their smartphones to protect themselves against online threats.

Evident from questions 6.5 and 17 findings, receiving strange text messages from unknown phone numbers has no significant influence $p < 0.000$ on students to take adequate online protective measures on their smartphones to protect themselves against online threats.

The findings of questions 6.6 and 17, receiving strange calls from unknown phone numbers, have no significant influence $p < 0.000$ on students taking adequate online protective measures on their smartphones to protect themselves against online threats.

Questions 6.7 and 17 findings indicate that receiving strange emails from unknown sources has no significant impact $p < 0.000$ on students taking adequate online protective measures on their smartphones to protect themselves against online threats. The past report affirms that cybercriminals target victims' security judgment in certain situations rather than the security measures taken. Hence, such people can fall victim to phishing attacks like spam (Broadhurst et al., 2018).

The results between questions 6.8 and 17 indicate that the presence of unknown mobile applications has no significant influence $p < 0.000$ on students taking adequate online protective measures on their smartphones to protect themselves against online threats.

4.6.3 Inference test for Self Efficacy

The inferential test between questions 18 and 17 analyses students' self-efficacy. For the inferential analysis of research question three, "Does possessing good security skills by students ensure taking the right security measures?" The analysis outcome helped evaluate the possible influence of security skills on implementing security measures. The inferential test

assesses coping appraisal based on students' self-efficacy. Questions 18 and 17 analysis indicated that students who possess good security skills are not influenced $p < 0.000$ by their ability to take security measures.

4.7 Answers for main research questions

The answers to the three research questions of this study are explained using the earlier findings since it is vital to offer solutions to the problem statements and fulfilling the research objectives.

4.7.1 The answer for research question one

The first research question, "What are the factors influencing the security practices of UKZN smartphone users to counter security threats?" is answered by using findings from the inferential analysis of data gathered for Sections 2 and 3 of the research questionnaire (Appendix B). Before the inferential analysis, the descriptive analysis used percentages to note students' opinions on threat and coping appraisal. The researcher then used inferential analysis to analyse threat appraisal factors against coping appraisal factors to discover which factors influence the security practices of UKZN students. The following factors of influence were derived:

- The awareness of a possible data breach influences students to use UKZN information security guidelines.
- The knowledge of potential disruption of UKZN services influences students to pay attention to security messages when installing a mobile application.
- Strange text messages from unknown phone numbers influence students to seek an ICS technician's assistance because it is easy to follow the security instruction, they provide from the UKZN online security guideline.
- The occurrence of strange calls from unknown phone numbers influences students to seek the assistance of an ICS technician because it is easy to follow the security instruction, they provide from the UKZN online security guideline.
- Receiving strange emails from unknown sources influences students to seek the assistance of an ICS technician because it is easy to follow the security instruction, they provide from the UKZN online security guideline.

- A lack of understanding of the UKZN online security guideline influences students to seek the assistance of an ICS technician because it is easy to follow the security instruction, they provide from the UKZN online security guideline.
- The occurrence of a data breach influences students to take timely online protective measures on their smartphones.
- An unknown change in a student's account password influences students to take timely online protective measures on their smartphones. The response to online threats can take the form of the use of strong passwords (Van der Kleij & Leukfeldt, 2019).
- Receiving strange text messages from unknown phone numbers influences students to take timely online protective measures on their smartphones. A past report by Phishlabs exposed the harm of text message attacks, indicating that Short Message Service attacks are primarily successful because many people access and read their text without expecting to open malicious messages (Phishlabs, 2019).
- Unknown mobile applications influence students to take timely online protective measures on their smartphones.
- An unknown change in a student's account password influences students to take adequate online security measures on their smartphones.

The above correlational findings indicate the eleven factors influence UKZN students to take security measures to protect themselves against online threats targeted at their smartphones. The result answers research question one of this study.

4.7.2 The answer for research question two

The second research question is "How are security practices of UKZN smartphone users affecting the university's information systems?" Based on the security practices derived from the influence factors in research question one, the researcher assessed each security practice and the consequential effects on UKZN's information systems. Meaning, research question two used the inferential analysis of data gathered for Sections 2 and 3 of the research questionnaire to derive its findings. The descriptive analysis used percentages to identify students' views on threat rewards from Section 2 of the questionnaire before the inferential analysis.

The above result in research question one indicated that students rarely use the UKZN information security guidelines to handle online threats. The guidelines are also used in the

case of a data breach, which leaves other attack instances unresolved, and exposes UKZN information systems. The result also indicated that students pay attention to security messages when installing a mobile application; this is good security behaviour that leaves less space for phishing attacks. Though, students do not always download applications from recommended links which still leaves opportunities for malicious attacks.

A reoccurring practice observed is that students seek an ICS technician's assistance because it is easy to follow technicians' security instructions. The expert solution helps handle threats better, especially when some students lack technical skills to address online threats targeted at their smartphones. It is good to seek ICS technicians' help. Still, the continual dependency on expert assistance makes most students personally less capable of handling security threats directed at their smartphones in real-time, leading to less timely threat resolution while opening the UKZN network to online threats coming from such smartphones.

In contrast, students are likely to take timely online protective measures on their smartphone when faced with the following threats: an unknown change in a student's account password, receiving strange text messages, the presence of unknown mobile applications, and the occurrence of a data breach. The ability to take timely protective measures in these situations mentioned above reduces the potential spread of malicious attacks over UKZN's information systems. In addition, an unknown change in a student's account password makes students take adequate online security measures on their smartphones, indicating that sufficient measures are not applied to every online threat. The lack of consistent practice of conducting security measures for every noticeable threat will continually expose UKZN's information systems to many online threats.

The personal security behaviour discussed earlier indicates that students' security practices are inconsistent and might lead UKZN to experience: a data breach, financial loss, identity theft, disruption of UKZN services, compromised data in the UKZN online storage, compromised student and staff accounts, compromised university network and malicious software attacks. A data breach will expose important information such as patent research work to hackers, and the outcome may lead to financial loss. A 2019 study supports the above findings on a data breach. It indicated that the University of Australia experienced a data breach that affected both staff and students. The stolen data of about 200,000 was taken from 19 years to the day of theft (Martin, 2019).

The study shows that the impact of a data breach is costly to a university, among other possible outcomes of students' security behaviours. Identity theft is also a problem that can arise through compromised student accounts, which may also affect staff accounts. A compromise on the university's network will affect data in the UKZN online storage, and such data may include personal information, academic, medical, and financial records. Exposing vital data can lead to financial loss, corporate espionage, patent research work, damage to the university's reputation and many other issues.

4.7.3 The answer for research question three

The third research question is, "Does possessing good security skills by students ensure taking the right security measures?" The findings established that students who possess good security skills to protect themselves against online threats are not influenced by their security skills to implement security measures. However, they can easily take suitable actions. In the descriptive analysis, students also agreed that the stress of implementing security measures discourages them from using the UKZN security guidelines to resolve threat issues by themselves. Although it takes less than five hours to implement security on a smartphone. Therefore, students' security implementation or the lack thereof is a personal choice that can adversely affect the smartphone owners and the university's information systems.

4.8 Conclusion

The research findings discussed the results of the study. The descriptive analysis of all questions was discussed first, along with the T-Tests. The inferential analysis of correlations between threat and coping appraisal variables was conducted. Is addressed in the first chapter; the findings were then used to answer the three research questions to fulfil the study's aim. The fifth chapter uses the research findings this chapter to conclude the study. Chapter five also explains the limitations encountered during the research and offers recommendations to improve the security practices of students.

CHAPTER 5

Conclusion

5.1 Introduction

Chapter five summarises the study and reassesses the research questions. The chapter critically assesses smartphone users' security practices at UKZN Westville Campus and their effects on the institutional information systems. This chapter proposes recommendations to enable students to form better security practices and assist the university in creating better security guidelines and support mechanisms against online threats. The chapter concludes by providing future research suggestions to mitigate existing literature gaps discovered in this study.

5.2 Dissertation Conclusion

This research aimed to assess the factors influencing student's smartphone users' security practices at the UKZN Westville Campus. First, in examining student smartphone users' security practices while utilising the university's wireless network, the researcher had to identify factors influencing users' security practices. Next, the researcher assessed if these smartphone users' security practices could lead to cyberattacks on the university's information systems. The third aim was to discover if students' possession of good security skills ensures suitable security measures. Each chapter enabled the completion of the study.

Chapter One of this study introduced the research. It also included the background of the study, problem statement, and objectives to develop the research. The rationale behind the study and structure of the subsequent chapters was discussed.

Chapter Two focused on reviewing some literature on students' security practices regarding using smartphones at universities and institutional information systems. The influence of technology on daily activities and education was assessed and insights regarding smartphone security practices were explored. Examined also were the flaws of security practices that can lead to data breaches and other threats, leaving both students and the university's information systems vulnerable. Several theoretical frameworks were assessed to select the most appropriate to conduct the study. The Protection Motivation theory and its six constructs of discussed and used in the research.

Chapter Three explained the research methodology: research design, research instrument, the research sample population, sample size, ethical considerations, data collection, measurements, data analysis and quality control.

Chapter Four explained the analysis of collected data using the descriptive and inferential methods to find numerical values to answer the research questions of this study. The outcome of the analysis was interpreted to answer the three research questions of the study and find possible solutions to the research problem.

5.3 Limitations and Future Research

The study's sample size is small. Therefore, the findings of this study cannot form a worldwide insight into the research problem. More research should be conducted using a bigger sample size to derive a broader insight into the issue.

The literature examined indicates gaps in the research area that can be explored in the future. The literature analysed revealed that many studies focused on using smartphones for learning while a few discussed cybersecurity problems related to the student smartphone user's security practices on campus and how it can enable threats to affect both individuals and the university. These threats include but are not limited to phishing, malware, a Man-in-the-middle attack, a Denial-of-service attack and many others.

5.4 Recommendations

The study offers recommendations to UKZN to mitigate security practice problems discovered during this research. The findings of this research will empower the UKZN Information Communication Services to understand how the university can improve methods of protecting UKZN information systems and make known the necessity of security training of smartphone users with access to the university's information systems. In addition, this research will also enlighten smartphone users on the campus of online threats that may occur due to their smartphone security practices and encourage these individuals to take timely security measures.

5.4.1 Recommendation for UKZN ICS

Based on this study's findings, for question 10.1, the ICS department can implement free online security training to increase security awareness and improve students' online protection skills and behaviour. Gauging people's security awareness is vital to create an appropriate security training program to prevent cyber victimisation (Broadhurst et al., 2018). The ICS already provides free computer literacy training for new students. Hence an online security training can also be established alongside the existing training. The training will empower students that do not understand the UKZN online security guideline or have prior protective security skills to respond competently to online threats by themselves with little need for technical assistance.

The university should encourage students to seek technical assistance at ICS walk-in centres if needed to protect students against online threats like data breaches targeted at their smartphones. For example, some institutions recommend using official email to secure communication to reduce the possibility of phishing attacks (Clark et al., 2018). The UKZN ICS department provides physical and telephonic services for students. However, the walk-in centres provide technical support for smartphones. This service will assist students that do not have good security skills to protect their smartphones against online threats.

The UKZN ICS should always encourage students to learn and practice protective online security skills. A study from recent years states that training students on how phishing works and information gathering works help to gauge threats (Salahdine & Kaabouch, 2019). Since the inferential findings for research question two indicate that many students rely on ICS technicians' assistance for specific security measures and conduct some other protective actions by themselves. An example for students asks for help to handle email breach issues. A significant dependency on ICS support may be harmful should there be a need for students' immediate online security resolve. The outcome of practical security training will benefit both students and the university alike as students are likely to commit security mistakes. In addition, students will depend less on ICS technicians for assistance to resolve threats targeted at their smartphones.

5.4.2 Recommendation for UKZN Students

Findings from question 15 in the previous chapter indicate the need for essential security training and encouragement for students that use smartphones connected to the university's Wi-Fi to learn good security practices and implement the measures timely without relying

solely on the ICS technicians for assistance. The training will also enable students to decrease the possibility of exposing themselves to numerous online threats. The mitigated risk helps reduce online threats to the university's information systems. The research findings of this study explained that people are a significant reason why security breaches occur due to inconsistent security behaviour, making people the most accessible element to exploit in a security system. Past research supports the aforementioned findings, stating that behavioural disconnect also exists with how people treat the security on their Personal Computers (PC) compared to smartphones. More security measures are implemented on the PC with the belief that smartphones are less vulnerable than PCs (Kithome, 2017).

Standard online security guidelines for mobile devices such as smartphones, tablets and laptops should be created, published, and sent to all students. In addition, electronic copies, or links of the updated versions of the security guidelines should be sent at timely intervals as a self-help guide to protect smartphones users against online threats. The above action is vital because knowledge of online security guidelines is missing among most UKZN students, as the finding from question 7 indicated.

Most students stated that they do not always use UKZN information security guidelines to resolve online threats targeted at their smartphones. The findings from the inference between questions 6 and 14 indicated this practice. In line with this issue, UKZN ICS can foster informative discussions and interactive security training online and offline for students about best smartphone security practices. Likewise, to recommend security tips and measures to counter online attacks and encourage conformity among students because malicious attacks keep evolving. Past research states that institutions recommend using official email to secure communication to reduce the possibility of phishing attacks (Clark et al., 2018).

The avoidance of downloading mobile applications from unknown sources should always be encouraged. Downloading applications from unknown sources can be a gateway for hackers to access a smartphone without the owner's permission (Sarang, 2018). Most but not all students in this study stated that they use the university recommended sites to download mobile applications; this finding was indicated in question 13.3. However, it is good to encourage all students to follow the same practice because vulnerability due to mobile downloads from malicious sources may result in unrestricted access to critical information on students' smartphones and the UKZN network.

Students should similarly be encouraged to avoid accessing suspicious websites. The findings for question 4 indicated that most students spend about five hours or less on the university Wi-Fi daily, which leaves enough time for students to explore none recommended websites, including malicious ones. Moreover, visiting malicious websites such as free movie download sites expose smartphones to phishing attacks, and such attacks enable more malicious attacks by hackers. A 2018 study supported this finding that people's use of smartphones could cause online security risks due to frequent random visits to safe and unsafe websites (Amro, 2018).

Students should be encouraged to take the necessary time to engage in the right security actions regardless of how busy their schedules might be. The more time a threat is left unattended, the more damage may occur. There will be a higher likelihood of both personal and university-wide threats occurring in such a situation.

5.6 Conclusion

Most students use their smartphones to browse the internet while connected to the university's Wi-Fi for less than five hours a day, leaving enough time for a threat to occur. Many students do not know what to do in the face of online threats due to the lack of understanding of the university's online security guidelines, which leaves the university's information systems exposed to threats. Hence such students may rely on ICS assistance to resolve specific issues such as an unknown change in student account password. Equally, numerous students are unaware that the university ICS staff provide physical and telephonic technical support weekly for students experiencing security-related issues targeted at smartphones. The lack of awareness of support services leaves many less-skilled students alone to protect themselves against online threats. Students are also in the habit of visiting random websites, and such websites may enable malicious attacks on their smartphones and the university's information systems. The behaviours mentioned above indicate inconsistencies in the way students handle online security threats targeted at their smartphones. The continual exposure of the university's information systems to such threats may lead to a data breach, data and financial loss, reputation damage, identity theft and many other damages. Finally, a good knowledge of the university's online security guidelines and having the necessary security skills has no significant impact on a student's behaviour when responding to online threats. Most students find the process of conducting security measures stressful.

REFERENCES

- Accenture. (2017). *Cyber Threatscape Report*. Retrieved 2 April, 2019 from <https://www.accenture.com/gb-en/event-black-hat-usa-2017>
- Accenture. (2019). *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection*. Retrieved 21 March, 2020 from <https://www.accenture.com/ acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf>
- Accenture. (2020a). *Cyber Threatscape Report*. Retrieved 14 December, 2020 from <https://www.accenture.com/za-en/insights/security/cyber-threatscape-report>
- Accenture. (2020b). *Insight Into The Cyberthreat Landscape in South Africa*. Retrieved 9 December, 2020 from <https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa>
- Afifi-Sabet, K. (2019). Dozens of 'innocent' apps are being infected through the development supply chain. Retrieved 12 August, 2019 from <https://www.itpro.co.uk/malware/33227/millions-hit-by-android-simbad-operation-sheep-campaigns>
- Ahvanooey, M. T., Li, Q., Rabbani, M., & Rajput, A. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *International Journal of Advanced Computer Science and Applications*, 8, 30 doi:10.14569/IJACSA.2017.081005
- Aiken, M., Davidson, J., & Amann, P. (2016). *Youth Pathways into Cybercrime*.
- Aini, Q., Zuliana, S. R., & Santoso, N. P. K. L. (2018). Management Measurement Scale As A Reference To Determine Interval In A Variable. *Aptisi Transactions on Management (ATM)*, 2(1). doi:10.33050/atm.v2i1.775
- Al Dhahri, S., Al Sarti, M., & Abdul Aziz, A. (2017). Information Security Management System. *International Journal of Computer Applications* 158(7), 0975 – 8887
- Ali, S., Islam, N., Rauf, A., Ud Din, I., Guizani, M., & Rodrigues, J. J. P. C. (2018). Privacy and Security Issues in Online Social Networks. *Future Internet* 2018 10(12), 114. doi:10.3390/fi10120114
- Almarabeh, H. (2019). The Impact of Cyber Threats on Social Networking Sites *International Journal of Advanced Research in Computer Science* 10, 1-9. doi:10.26483/ijarcs.v10i2.6384
- Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one* 12(3).
- Amro, B. (2018). Phishing Techniques in Mobile Devices. *Journal of Computer and Communications* 6, 27-35. doi:10.4236/jcc.2018.62003
- Anh, H. N. (2016). *Smartphone Industry: The New Era of Competition and Strategy*. Centria University of Applied Sciences,
- Argun, U., & Daglar, M. (2016). Examination of Routine Activities Theory by the property crime. *International Journal of Human Sciences* 13(1). doi:10.14687/ijhs.v13i1.3665
- Atas, H., & Celik., B. (2019). Smartphone Use of University Students: Patterns, Purposes, and Situations. *Malaysian Online Journal of Educational Technology* 7, 54-70. doi:10.17220/mojet.2019.02.004
- Aurigemma, S., Mattson, T., & Leonard, L. N. K. (2016). Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transactions on Replication Research* 5(3), 1–21. doi:10.17705/1attr.00035
- Avast. (2019). ICE under fire, SimBad the epic malware. Retrieved 23 January, 2020 from <https://blog.avast.com/ice-privacy-concerns-and-box-data-leaks>
- Baktha, K. (2017). Mobile Application Development: All the Steps and Guidelines for Successful Creation of Mobile App: Case Study. *International Journal of Computer Science and Mobile Computing* 6(9), 15-20.
- Ballantyne, N., Wong, Y., & Morgan, G. (2017). Human Services and the Fourth Industrial Revolution: From huslTa 1987 to huslTa 2016. *Journal of Technology in Human Services*, 35, 1-7 doi:10.1080/15228835.2017.1277900

- Barth, S., De Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics* 41, 55–69.
- Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems* 28, 34–49.
- Bjorck, F. (2004). *Institutional theory: a new perspective for research into IS/IT security*. Paper presented at the Proceedings of the 37th Hawaii International Conference on System Sciences, Big Island, Hawaii, USA.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, 48(7), 953–977. doi:<https://doi.org/10.1177/0093650218800915>
- Booth, A., Noyes, J., Flemming, K., Gerhardus, A., Wahlster, P., Van der Wilt, G. J., Mozygemba, K., Refolo, P., Sacchini, D., Tummers, M., & , & Rehfuess, E. (Eds.). (2016). *Guidance on choosing qualitative evidence synthesis methods for use in health technology assessments of complex interventions*: Integrate-HTA.
- Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros Macias, B., & Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. *SSRN Electronic Journal* doi:10.2139/ssrn.3176319
- Brook, C. (2017). Critical Moodle Vulnerability Could Lead to Server Compromise. *Threat Post*. Retrieved 2 February, 2020 from <https://threatpost.com/critical-moodle-vulnerability-could-lead-to-server-compromise/124446/>
- Bruceb. (2017). Security Warning: Do Not Click On Links In Email Messages! Retrieved 29 March, 2021 from <https://www.bruceb.com/2017/11/security-warning-do-not-click-on-links-in-email-messages/>
- Canadian Security. (2017). University of the Fraser Valley investigating breach of student information. *Canadian Security Magazine* Retrieved 18 June, 2020 from <https://www.canadiansecuritymag.com/university-of-the-fraser-valley-investigating-breach-of-student-information/>
- Cecere, G., Le Guel, F., & Lefrere, V. (2018). *Economics of free mobile applications: Personal data as a monetization strategy*. Paper presented at the 16th Conference of IAOS OECD Headquarters, Paris, France.
- Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2018). Hacking, protection and the consequences of hacking. *Communications - Scientific Letters of the University of Zilina* 20, 83-87. doi:10.26552/com.C.2018.2.83-87
- Chapman, J. (2019). *How safe is your data? Cyber-security in higher education*.
- Chaputula, A., & Mutula, S. (2018). Factors impacting library-related uses of mobile phones by students in public universities in Malawi. *South African Journal of Libraries and Information Science*, 84 (1). doi:10.7553/84-1-1757
- Chauhan, R., & Upamannyu, N. (2017). Assessing the Moderating Relationship for Mobile Learning Apps: A study of students in college context. *Prestige International Journal of Management & IT-Sanchayan*, 6, 116-140. doi:10.37922/PIJMIT.2017.V06i01.009
- Chawdhry, A. A., Poullet, K., Douglas, D. M., & Compimizzi, J. (2016). *Downloading Mobile Applications – Are Students Protecting Themselves?* . Paper presented at the Information Systems Applied Research, Las Vegas, Nevada USA.
- Check Point. (2019). *Cyber Attack Trends: 2019 Mid-Year Report*. Retrieved 23 May, 2020 from <https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/>
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. doi:10.1002/widm.1211
- Clark, J., Oorschot, P., Ruoti, S., Seamons, K., & Zappala, D. (2018). Securing Email. Retrieved 5 May, 2021 from <https://arxiv.org/pdf/1804.07706v1.pdf>

- Clubb, A., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies* 28. doi:10.1080/1478601X.2015.1050590
- Cohen, J. (2018). Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies. *American Association for the Advancement of Science. AAA Science Magazine*. Retrieved 15 April, 2021 from <https://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and>
- Coleman, L., & Purcell, B. M. (2015). Data Breaches in Higher Education *Journal of Business Cases and Applications*, 15.
- Conetta, C. (2019). Individual Differences in Cyber Security. *McNair Research Journal SJSU*, 15.
- Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4 ed.).
- Croasdell, D. T., Elste, J. R., & Hill, A. (2018). *Cyber Clinics: Re-imagining Cyber Security Awareness*. Paper presented at the 51st Hawaii International Conference on System Sciences 2018, Hawaii, USA.
- Da Veiga, A., & Swartz, P. (2017). Personal Information and Regulatory Requirements for Direct Marketing: A South African Insurance Industry Experiment *South African Institute of Electrical Engineers*, 108(2).
- Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security* 48, 281.
- David, N. J., Kadobayashi, Y., & Fall, D. (2017). UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App. *Asia Joint Conference on Information Security 2017* doi:10.1109/AsiaJCIS.2017.19
- Davis, F., Bagozzi, R., & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science* 35, 982-1003 doi:10.1287/mnsc.35.8.982
- De Bruyn, M. (2014). The Protection Of Personal Information (POPI) Act - Impact On South Africa. *International Business & Economics Research Journal (IBER)*, 13. doi:10.19030/iber.v13i6.8922
- De Prá Carvalho, A., Da Cunha, S. K., De Lima, L. F., & Carstens, D. D. (2017). The role and contributions of sociological institutional theory to the socio-technical approach to innovation theory. *RAI Revista de Administração e Inovação*, 14(3), 250-259
- Deloitte. (2018). *Elevating cybersecurity on the higher education leadership agenda: Deloitte Insights*. Retrieved 23 December, 2019 from <https://www2.deloitte.com/us/en/insights/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html>
- Deloitte. (2019). *Tech Trends 2019: Beyond the digital frontier*. Retrieved 6 April, 2019 from <https://www2.deloitte.com/lu/en/pages/technology/articles/tech-trends-2019-beyond-digital-frontier.html>
- Dias, L., & Victor, A. (2017). Teaching and Learning with Mobile Devices in the 21st Century Digital World: Benefits and Challenges. *European Journal of Multidisciplinary Studies*, 2 (5).
- Diaz, A., Sherman, A., & Joshi, A. (2019). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *Cryptologia*, 44(1), 1-15. doi:10.1080/01611194.2019.1623343.
- Edwards, B. (2018). The Golden Age of PDAs. *PC Magazine* Retrieved 31 July, 2019 from <https://www.pcmag.com/feature/364985/the-golden-age-of-pdas>
- El Hajjar, S. T. (2018). Statistical Analysis: Internal-Consistency Reliability and Construct Validity *International Journal of Quantitative and Qualitative Research Methods* 6(1), 27-38.
- European Insurance and Occupation Pension Authority. (2018). *Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies*. Retrieved from
- Faklaris, C., Dabbish, L., & Hong, J. I. (2019). *A Self-Report Measure of End-User Security Attitudes (SA-6)*. Paper presented at the Fifteenth Symposium on Usable Privacy and Security. USENIX.

- Fleming, J., & Zegwaard, K. E. (2018). Methodologies, methods and ethical considerations for conducting research in work-integrated learning. *International Journal of Work-Integrated Learning, Special Issue, 2018*, 19 (3), 205-213.
- Gartner. (2019). Mobile OSs and Device Security: A Comparison of Platforms. Retrieved 3 March, 2021 from <https://www.gartner.com/en/documents/3913286/mobile-oss-and-device-security-a-comparison-of-platforms>
- George, D., & Mallery, P. (2016). *IBM SPSS Statistics 23 Step by Step: A Simple Guide and Reference* (14th ed.).
- Gerber, N., Zimmermann, V., & Volkamer, M. (2019). *Why Johnny Fails to Protect his Privacy*. Paper presented at the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden.
- Godwin-Jones, R. (2017). Smartphones and language learning. *Language Learning & Technology*, 21 (2), 3–17.
- Google. (2019). *Android Security & Privacy 2018 Year in Review*. Retrieved 30 May, 2021 from <https://source.android.com/security/reports/Google Android Security 2018 Report Final.pdf>
- Gyorodi, R., Zmaranda, D., Georgian, V., & Györödi, C. (2017). A Comparative Study between Applications Developed for Android and iOS. *International Journal of Advanced Computer Science and Applications*, 8. doi:10.14569/IJACSA.2017.081123
- Hagger, M. (2019). *The Reasoned Action Approach and the Theories of Reasoned Action and Planned Behavior*.
- Holicza, P., & Kadena, E. (2018). Smart and Secure? Millennials on Mobile Devices. *Interdisciplinary Description of Complex Systems*, 16, 376-383 doi:10.7906/indexs.16.3.10
- Holt, T., Van Wilsem, J., Weijer, S., & Leukfeldt, E. (2018). Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review* 38. doi:10.1177/0894439318805067
- IBM. (2019). *Cost of a Data Breach Report 2019: Ponemon*. Retrieved 18 June, 2020 from <https://www.ibm.com/downloads/cas/RDEQK07R>
- Internet Society. (2017). Internet for Education in Africa. Helping Policy Makers to Meet the Global Education Agenda Sustainable Development Goal 4. In *Internet Society — Internet for Education in Africa*.
- Jackson, S. (2016). *Research Methods and Statistics: A Critical Thinking Approach* (5 ed.).
- Jason, A. (2017). *Mobile Device Use in Student Learning Process with Use of Mobile Devices*. Lahti University of Applied Sciences,
- Joint Information Systems Committee. (2018). The cyber threat to Universities: Assessing the cyber security threat to UK Universities. Retrieved 12 August, 2020 from <https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities>
- Jurcut, A., Niculcea, T., Ranaweera, P., & Le Khac, N. (2020). Security Considerations for Internet of Things: A Survey. *SN Computer Science* 1(193). doi:10.1007/s42979-020-00201-3
- Kabir, S. M. (2016). *Methods of Data Collection*.
- Kadir, A. F. A., Stakhanova, N., & Ghorbani, A. A. (2018). Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges. *Journal of Cyber Security and Mobility*, 73 1–52. doi:10.13052/jcsm2245-1439.732
- Kandeh, A. T., Botha, R. A., & Fitcher, L. A. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *South African Journal of Information Management*, 20(1). doi:10.4102/sajim.v20i1.917
- Kaspersky. (2019). Mobile Malware Threats. Retrieved 10 August, 2020 from <https://usa.kaspersky.com/resource-center/threats/mobile-malware>
- Kaur, P., Stoltzfus, J., & Yellapu, V. (2018). Descriptive statistics. *International Journey of Academic Medicine*, 4, 60-63.

- Kausar, F., Aljumah, S., Alzaydi, S., & Alroba, R. (2019). Traffic Analysis Attack for Identifying Users' Online Activities. *IT Professional*, 21(2), 50-57. doi:10.1109/MITP.2018.2876988
- Kim, T. K., & Park, J. H. (2019). More about the basic assumptions of t-test: normality and sample size. *Korean Journal of Anesthesiology* 72 331-335.
- Kithome, A. (2017). Managing Threats of Cyber-Attacks on Mobile Devices. Munich. *GRIN Verlag*.
- Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, 2019, 11.
- KPMG. (2018). *Cyber Insurance – How Insuretechs Can Unlock The Opportunity*. Retrieved 29 March, 2021 from <https://assets.kpmg/content/dam/kpmg/za/pdf/2017/12/17383MC-cyber-insurance.pdf>
- Kranenbarg, M. W. (2018). *Cyber-offenders versus traditional offenders. An empirical comparison*. Vrije Universiteit Amsterdam, Retrieved 2 June, 2021 from <https://research.vu.nl/en/publications/cyber-offenders-versus-traditional-offenders-an-empirical-compari>
- Langkos, S. (2014). *Chapter 3 - Research Methodology: Data collection method and Research tools*.
- Leukfeldt, E. (2017). *Research agenda. The human factor in cybercrime and cybersecurity*.
- Lewis, M., & Zaheer, H. (2018). Predictors of Problematic Smartphone Use: An Examination of the Integrative Pathways Model and the Role of Age, Gender, Impulsiveness, Excessive Reassurance Seeking, Extraversion, and Depression. *Behavioral Sciences*, 8(74). doi:10.3390/bs8080074
- Lieberman, M. (2019). Students Are Using Mobile Even If You Aren't. Retrieved 23 January, 2020 from <https://www.insidehighered.com/digital-learning/article/2019/02/27/mobile-devices-transform-classroom-experiences-and>
- Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017). *Descriptive analysis in education: A guide for researchers. Descriptive analysis in education: A guide for researchers. (NCEE 2017-4023)*.
- Losoncz, P., Vackova, M., & Necas, P. (2019). *The Security of the WI-FI Networks in University Environment*.
- Lukacs, A. (2017). To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection. *Masaryk University Journal of Law and Technology*, 11, 85-214. doi:10.5817/MUJLT2017-2-1
- Maimon, D., Becker, M., Patil, S., & Katz, J. (2017). *Self-Protective Behaviors Over Public WiFi Networks*. Paper presented at the USENIX. The Laser Workshop 2017.
- Majid, U. (2018). Research Fundamentals: Study Design, Population, and Sample Size. *Undergraduate Research in Natural and Clinical Science and Technology (URN CST) Journal* 2. doi:10.26685/urncst.16
- Martin, L. (2019). Australian National University hit by huge data breach. *The Guardian Australia*. Retrieved 23 December, 2019 from <https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach>
- Martin, M., Nathan, S., Morris, A., & Harvey, E. (2018). A Review of Behavioural Research on Data Security. *2018 European Journal of Privacy Law & Technology*, 16.
- Mayisela, T. (2013). The potential use of mobile technology: enhancing accessibility and communication in a blended learning course. *South African Journal of Education*, 33(1).
- McAfee. (2020). *McAfee Labs Covid 19 Threats Report*. Retrieved 13 November, 2020 from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf>
- Mills, A. M., & Sahi, N. (2019). *An Empirical Study of Home User Intentions towards Computer Security*. Paper presented at the 52nd Hawaii International Conference on System Sciences, Hawaii.
- Miró-Llinares, F. (2014). *Routine Activity Theory*.
- Mishra, P., Pandey, C., Singh, U., & Gupta, A. (2018). Scales of Measurement and Presentation of Statistical Data. *Annals of Cardiac Anaesthesia*, 21, 419-422. doi:10.4103/aca.ACA_131_18

- Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems* 108. doi:10.1016/j.future.2020.03.021
- Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty*.
- Mohajan, H. K. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University*, 17 (4), 56-82.
- Mohamed, I. A. H. (2017). Some Issues In The Institutional Theory: A Critical Analysis. *International Journal of Scientific and Technology Research*, 6(9).
- Momani, A., Jamous, M., & Hilles, S. M. (2017). Technology Acceptance Theories: Review and Classification. *International Journal of Cyber Behavior, Psychology and Learning*, 7, 1-14. doi:10.4018/IJCBPL.2017040101
- Mshana, J. A. (2015). Cybercrime: An Empirical Study of its Impact in the Society- A Case Study of Tanzania. *Huria: Journal of the Open University of Tanzania*, 19(1).
- Mueni, P. (2019). How to check your UKZN application status. Retrieved 30 November, 2021 from <https://briefly.co.za/34075-how-check-ukzn-application-status.html>
- Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *South African Journal of Information Management*, 20(1). doi: 10.4102/sajim.v20i1.980
- Mwambakulu, M., & Chikumba, P. (2021). Smartphone usage patterns in public universities in Malawi: student perspectives. *South African Journal of Libraries and Information Science*, 86, 26-37. doi:10.7553/86-2-1907
- Nagarjun, P. M. D., & Ahamad, S. S. (2018). Review of Mobile Security Problems and Defensive Methods. *International Journal of Applied Engineering Research* 13(12), 10256-10259.
- Nayak, K. J. (2018). Relationship among smartphone usage, addiction, academic performance and the moderating role of gender: A study of higher education students in India. *Computers & Education*, 123, 164-173
- Ngesi, N., Landa, N., Madikiza, N., Cekiso, M. P., Tshotsho, B., & Walters, L. M. (2018). Use of mobile phones as supplementary teaching and learning tools to learners in South Africa. *Reading & Writing - Journal of the Reading Association of South Africa*.
- Nguyen, Q. A., Hens, L., MacAlister, C., Johnson, L., Lebel, B., Tan, S. B., Nguyen, H. M., Nguyen, T. N., & Lebel, L. (2018). Theory of Reasoned Action as a Framework for Communicating Climate Risk: A Case Study of School children in the Mekong Delta in Vietnam. *Sustainability* 2018 10. doi:10.3390/su10062019
- Norton. (2020). Android vs. iOS: Which is more secure? Norton Life Lock. Mobile. Retrieved 18 January, 2021 from <https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html>
- Nurse, J. (2018). *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*: Oxford University Press.
- O'Hagan, T. (2017). Mobility in Education: can mobile devices support teaching and learning in South Africa? Retrieved 27 July, 2020 from <https://hsf.org.za/publications/focus/focus-68/%2811%29%20T.%20OHagan.pdf>
- Oakley, M., Himmelweit, S. M., Leinster, P., & Casado, M. R. (2020). Protection Motivation Theory: A Proposed Theoretical Extension and Moving beyond Rationality—The Case of Flooding. *Water* 2020, 12, 1848. doi:10.3390/w12071848
- Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-89.
- Palaniappan, G., Sangeetha, S., Rajendran, B., Sanjay, Goyal, S., & Bindhumadhava, B. S. (2020). Malicious Domain Detection Using Machine Learning On Domain Name Features, Host-Based Features and Web-Based Features. *Procedia Computer Science*, 171, 654-661.
- Pallant, J. (2016). *SPSS Survival Manual: A Step By Step Guide To Data Analysis Using IBM SPSS* (6 ed.).

- Parveen, H., & Showkat, N. (2017). Research Ethics. Retrieved from https://www.researchgate.net/publication/318912804_Research_Ethics
- Phillips, W. (2016). Research Tools: Interview and Questionnaires. Research Methodology in Education. Retrieved 9 April, 2021 from <https://lled500.trubox.ca/2016/225>
- Phishlabs. (2019). *2019 Phishing Trends and Intelligence Report. The Growing Social Engineering Threat*. Retrieved 27 March, 2021 from <https://info.phishlabs.com/blog/2019-phishing-trends-intelligence-report-the-evolving-threat>
- Polyakov, A. (2017). What Cyberthreats Do Higher Education Institutions Face? . *Forbes* Retrieved 29 July, 2020 from <https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/?sh=4fccf10b640d>
- Ponemon. (2017). *The Data Breach: Business & Financial Impact Report. Study of Marketers, IT Practitioners and Consumers in the United Kingdom*: Ponemon Institute.
- Rajotiya, R. N. (2019). *Advances in Wireless Technologies: A Survey*. Paper presented at the Chandigarh-4th International conference on Science, Technology & Management (ICSTM-2018), Chandigarh.
- Republic of South Africa. (2013). *Protection of Personal Information Act 2013*. Republic of South Africa Government Gazette 2013.
- Republic of South Africa. (2015). *National Development Plan 2030: Our Future-make it work*: Republic of South Africa.
- Republic of South Africa. (2021). Protection of Personal Information Act. Retrieved 29 March, 2021 from <https://popia.co.za/category/information-security/>
- Research ICT Africa. (2016). *Developing Smart Public Wi-Fi in South Africa: Research ICT Africa*.
- Research ICT Africa. (2020). *Digital Futures: South Africa's Digital Readiness for the 'Fourth Industrial Revolution'*. Research ICT Africa.
- Riasat, R., Sakeena, M., Wang, C., Hannan Sadiq, A., & Wang, Y. (2017). A Survey on Android Malware Detection Techniques. *DEStech Transactions on Computer Science and Engineering*. doi:10.12783/dtcse/wcne2016/5088
- Rivadeneira, F., & Rodriguez, G. (2018). Bring your own device: a survey of threats and security management models. *International Journal of Electronic Business*, 14(146). doi:10.1504/IJEB.2018.10016225
- Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 9(1), 93-114. doi:10.1080/00223980.1975.9915803
- Rossmo, D. K., & Summers, L. (2015). *Routine Activity Theory in Crime Investigation*: London: Palgrave Macmillan.
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet* doi:10.3390/fi11040089
- Sarang, R. (2018). Are Fake Apps Taking Over Your Phone? Retrieved 15 February, 2019 from <https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/fake-apps-taking-over-phone/m>
- Saunders, M., Lewis, M., & Thornhill, A. (2016). *Research methods for business students* (7 ed.).
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (4 ed.).
- Schober, P., Boer, C., & Schwarte, L. (2018). Correlation Coefficients: Appropriate Use and Interpretation. *Anesthesia & Analgesia*, 126(5), 1763-1768. doi:10.1213/ANE.0000000000002864
- Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems* 32(2), 314-341. doi:10.1080/07421222.2015.1063315
- Shanks, G., & Bekmamedova, N. (2018). Case study research in information systems. In *Research methods: information, systems, and contexts*.
- Shillair, R. (2020). Protection Motivation Theory. 1-3. doi:10.1002/9781119011071.iemp0188


- Shouran, Z., Priyambodo, T., & Ashari, A. (2019). Information System Security: Human Aspects. *International Journal of Scientific and Technology Research*, 8(111).
- Siani, A. (2017). BYOD strategies in higher education: current knowledge, students' perspectives, and challenges. *New Directions in the Teaching of Physical Sciences*, 12(1).
- Siew, F., Ng, S. F., Che-Hassan, N. S. I., Hassan, C., Mohammad-Nor, N. H., Ain, N., & Abdul-Malek, N. A. (2017). The Relationship Between Smartphone Use and Academic Performance: A Case of Students in a Malaysian Tertiary Institution. *Malaysian Online Journal of Educational Technology*.
- Singh, A. S., & Masuku, M. (2014). Sampling Techniques and Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Commerce and Management*, 2(1-22).
- Singh, M. M., Wai-Chan, C., & Zulkefli, Z. (2017). Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. *International Journal of Advanced Computer Science and Applications*, 8. doi:10.14569/IJACSA.2017.080208
- Smith, R. (2018). IBM created the world's first smartphone 25 years ago. Retrieved 28 March, 2021 from <https://www.weforum.org/agenda/2018/03/remembering-first-smartphone-simon-ibm/>
- Sowells, J. (2018). Malicious Mobile Applications: An Introduction. Retrieved 13 June, 2019 from <https://hackercombat.com/knowledge-base/malicious-mobile-applications-an-introduction/>
- Statista. (2021a). *Annual number of global mobile app downloads 2016-2020*. Retrieved 28 March, 2021 from <https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/>
- Statista. (2021b). *Social media - Statistics & Facts*. Retrieved 28 March, 2021 from <https://www.statista.com/topics/1164/social-networks/>
- Statista. (2021c). *South Africa mobile internet user penetration 2015-2025*. Retrieved 27 March, 2021 from <https://www.statista.com/statistics/972866/south-africa-mobile-internet-penetration/>
- Sun, J. C. Y., Yu, S. J., Lin, S. S. J., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, 59, 249-257. doi:10.1016/j.chb.2016.02.004
- Symantec. (2018). *Internet Security Threat Report*. Retrieved 13 October, 2019 from <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape>
- Taber, K. (2017). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, 1-24. doi:10.1007/s11165-016-9602-2
- Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. doi:10.1007/s10639-020-10330-0
- Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)* 5.
- Talal, M., Zaidan, A., Bahaa, B., Albahri, O. S., Alsalem, M., Albahri, A. S., Alamoodi, A., Kiah, L. M., Jumaah, F., & Alaa, M. (2019). Comprehensive review and analysis of anti-malware apps for smartphones. *Telecommunication Systems*. doi:10.1007/s11235-019-00575-7
- Thirumoorthy, G. (2020). *A Comparative Study on the Recent Smart Mobile Phone Processors*.
- Thompson, S. A., & Warzel, C. (2019). Twelve Million Phones, One Dataset, Zero Privacy. The Privacy Project. *New York Times*. Retrieved 23 December, 2019 from <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>
- Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Comput. Surv* 51(2).
- University of KwaZulu-Natal. (2018). Phishing and Spam Awareness. Retrieved 26 December, 2019 from https://ics.ukzn.ac.za/wp-content/uploads/2018/03/Phishing_4.pdf

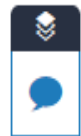
- University of KwaZulu-Natal. (2020). *Student Registration Report*. Retrieved 16 June, 2020 from <https://ii.ukzn.ac.za/Report/StudentRegistrations>
- University of KwaZulu-Natal. (n.d). Student Support. Retrieved 30 November, 2021 from <https://ics.ukzn.ac.za/student-support/>
- Van Bavel, R., Rodriguez 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. doi:10.1016/j.ijhcs.2018.11.003
- Van den Berg, J., & Van der Lingen, E. (2019). An Empirical Study of the Factors Affecting the Adoption of Mobile Enterprise Applications. *South African Journal of Industrial Engineering* 30(1), 124-146. doi:10.7166/30-1-1992
- Van der Kleij, R., & Leukfeldt, E. (2019). *Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security*. Paper presented at the Advances in Intelligent Systems and Computing, AHFE International Conference on Human Factors in Cybersecurity, Washington D.C., USA.
- Van Niekerk, B., & Maharaj, M. (2017). Mobile Malware Implications for IT Management. *Alternation Interdisciplinary Journal for the Study of the Arts and Humanities in Southern Africa*, 232-252. doi:10.29086/2519-5476/2017/sp20a12
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49, 190–198. doi:10.1016/j.im.2012.04.002
- Verizon. (2019). *Incident Preparedness and Response Report: Taming the data beast breach*. Paper presented at the RSA Conference.
- Wang, C., & Wang, S. (2014). User Behavior Research of Information Security Technology Based on TAM. *International Journal of Security and Its Applications*, 8, 203-210. doi:10.14257/ijisia.2014.8.2.21
- Weems, C. F., Ahmed, I., Richard III, G. G., Russell, J. D., & Neill, E. L. (2018). Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior. *PloS one*, 13(12).
- Weichbroth, P., & Lysik, L. (2020). Mobile Security: Threats and Best Practices. *Mobile Information Systems*, 1-15. doi:10.1155/2020/8828078
- Winder, D. (2019). New Android App Malware Infects 250 Million Downloads - Here's What You Need To Know. *Forbes*. Retrieved 25 September, 2020 from <https://www.forbes.com/sites/daveywinder/2019/03/13/new-android-app-malware-infects-250-million-downloads-heres-what-you-need-to-know/?sh=2fabe67060fd>
- Xiao, X., Fu, P., Li, Q., Hu, G., & Jiang, Y. (2017). Modelling and validation of SMS worm propagation over social networks. *Journal of Computational Science*, 21, 132-139.
- Yoon, C., Hwang, J., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, 23(4), 407-415.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Çetin, F., & Basim, N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*. doi:10.1080/08874417.2020.1712269

APPENDIX

Turnitin report

The Turnitin index is 5%

 Oluwafisayo Kaka | Mcom (IS&T) - Thesis - Oluwafisayo Kaka - 208513240




5



Security Practices of Smartphone Users at UKZN Westville Campus and Its Effects on the Institutional Information Systems

By
Oluwafisayo Kaka
208513240

 A dissertation submitted in fulfilment of the requirements for the degree of
Master of Commerce

Questionnaire



Respondent number: _____

Voluntary Questionnaire

Security Practices of Smartphone Users at UKZN Westville Campus and Its Effects on the Institutional Information Systems

Researcher: Ohlwafisayo Kaka

Supervisor: Mr Karunakaran Naidoo

School of Management, Information Systems & Technology and Governance

Faculty

Discipline Information Systems & Technology

University of KwaZulu-Natal, Durban, South Africa

- Please complete this voluntary questionnaire on the Security Practices of Smartphone Users at UKZN Westville Campus and Its Effects on the Institutional Information Systems.
- Please be forthright in your answers.
- Complete the questionnaire by pen and please do not revise your initial answers.
- Please indicate your response to the questions by ticking (✓) in the appropriate boxes.
- Please sign the letter of informed consent, permitting the researcher to use your responses for this research project.

Section 1: Biography

1. Gender
Male ☐
Female ☐
2. Age: 18 – 24 ☐ 25 – 34 ☐ 35 – 44 ☐ 45 or older ☐
3. I am a
Undergraduate student ☐ Postgraduate student ☐

4. When using a smartphone connected to the UKZN network

	Less than 5 hours	5–10 hours	10 – 15 hours	15–20 hours	More than 20 hours
The average time that I spend online per day is					

Section 2

Threat Appraisal (RQ1 - Perceived Vulnerability)

5. When using a smartphone connected to the UKZN Wi-Fi, UKZN...

5.1. May experience data breach if I disregard UKZN online security guideline.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

5.2. May experience data loss if I disregard the UKZN online security guidelines.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

5.3. UKZN productivity can experience a disruption of services attack if I disregard the UKZN online security guidelines.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Threat Appraisal (RQ1 - Perceived Severity)

6. When using my smartphone to connect the UKZN Wi-Fi

6.1. A data breach may result in a significant problem for UKZN.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.2. An unknown change in my student account password indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.3. The presence of regular advertisement pop-up alerts indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.4. Financial loss due to data breach indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.5. Receiving strange text messages from unknown phone numbers indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.6. Receiving strange calls from unknown phone numbers indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.7.Receiving strange emails from unknown sources indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

6.8.The presence of unknown mobile applications indicates a significant threat.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

7. Lack of understanding for the UKZN online security guideline may result in a significant problem for UKZN.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

8. UKZN will continually be susceptible to online threats if I do not implement UKZN online security measures on my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Threat Appraisal (RQ2 - Reward)

9. I believe a disregard for UKZN online security guidelines by me can subject UKZN to...

9.1.A data breach.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.2.A Financial loss.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.3.Identity theft.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.4.Disruption of UKZN services.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.5.Compromised data in the online storage.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.6.Compromised student accounts

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.7.Compromised staff accounts.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.8. Compromised network.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

9.9. Malicious software attacks.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Section 3

Coping Appraisal (RQ1 - Response Efficacy)

10. In the occurrence of a university-wide data breach, the UKZN ICS

10.1. Alerts me to fraudulent email through Microsoft Outlook.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

10.2. Provides a fraudulent email quiz to help me become aware of email scams.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

10.3. Provides technical assistance to secure my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

11. I always use UKZN information security guidelines to resolve online threats targeted at my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

12. I utilise the UKZN ICS call service which operates on weekdays to resolve smartphone security problems.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

13. In response to an online security threat targeted at my smartphone, I

13.1. Install an anti-Virus software.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

13.2. Use multiple authentication methods to secure my email.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

13.3. Install mobile applications used by UKZN from recommended links.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

13.4. Pay attention to security messages for mobile application installation.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

13.5. Change passwords used for various platforms.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Coping Appraisal (RQ1 & RQ3 - Self-efficacy)

14. It is easy for me to use the UKZN online security guideline to protect my smartphone against online threats.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

15. It is easy for me to use UKZN online security guideline if I follow an ICS technician's security instruction.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

16. It is easy for me to take timely online protective measures on my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

17. It is easy for me to take adequate online security measures on my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

18. I possess the skill to protect myself against online threats targeted at my smartphone.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Coping Appraisal (RQ3 - Response Cost)

19. The implementation of security measures to protect my smartphone is expensive.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

20. The implementation of security measures to protect my smartphone takes

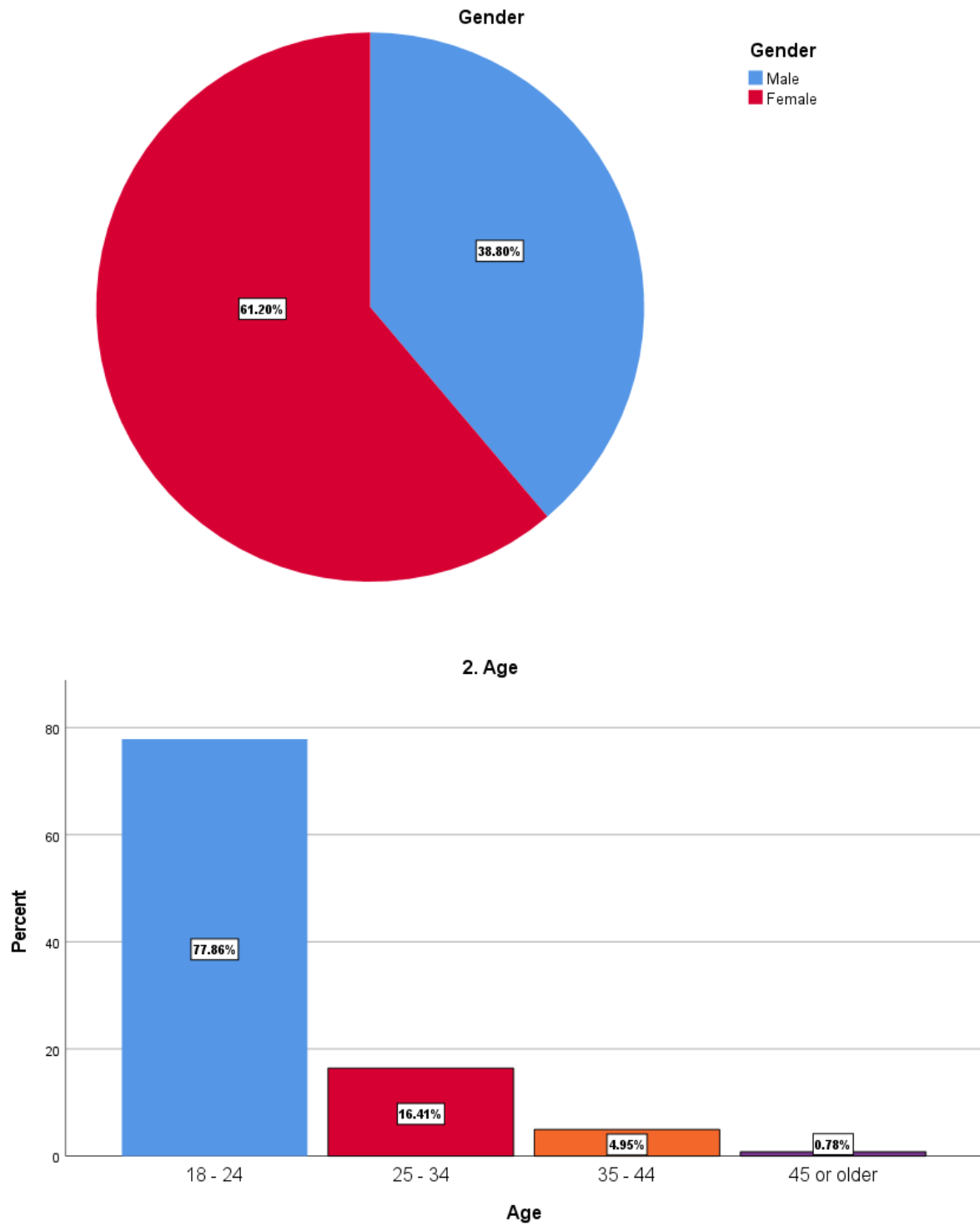
Less than 5 hours	5 – 10 hours	10 – 15 hours	15–20 hours	More than 20 hours

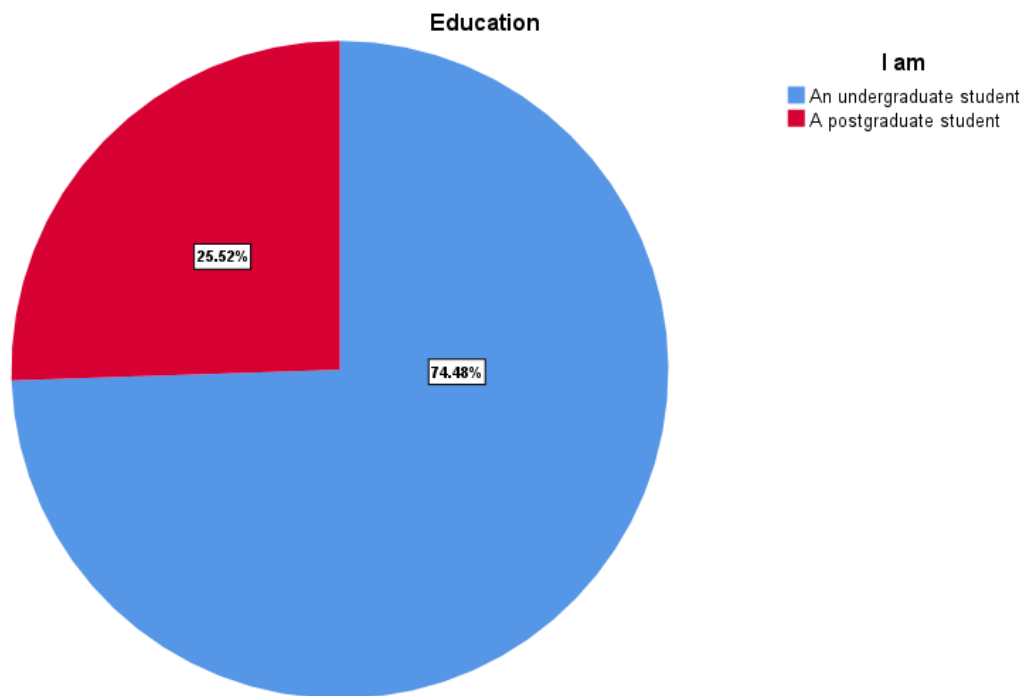
21. The stress to implement security measures on my smartphone discourages me from following UKZN security guidelines.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

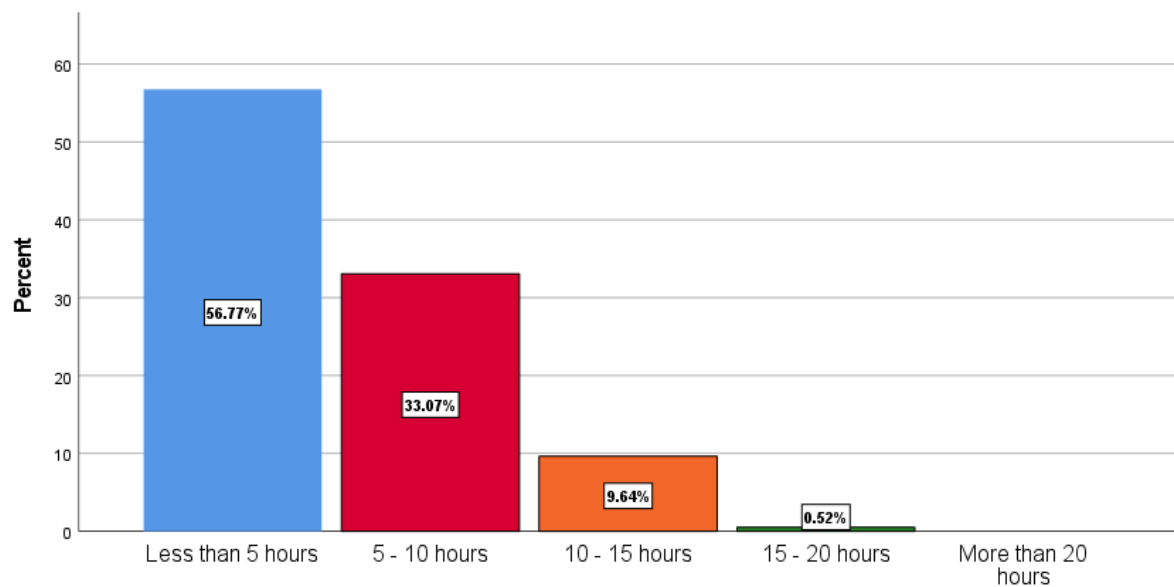
Thanks for participating

Tables and charts – data

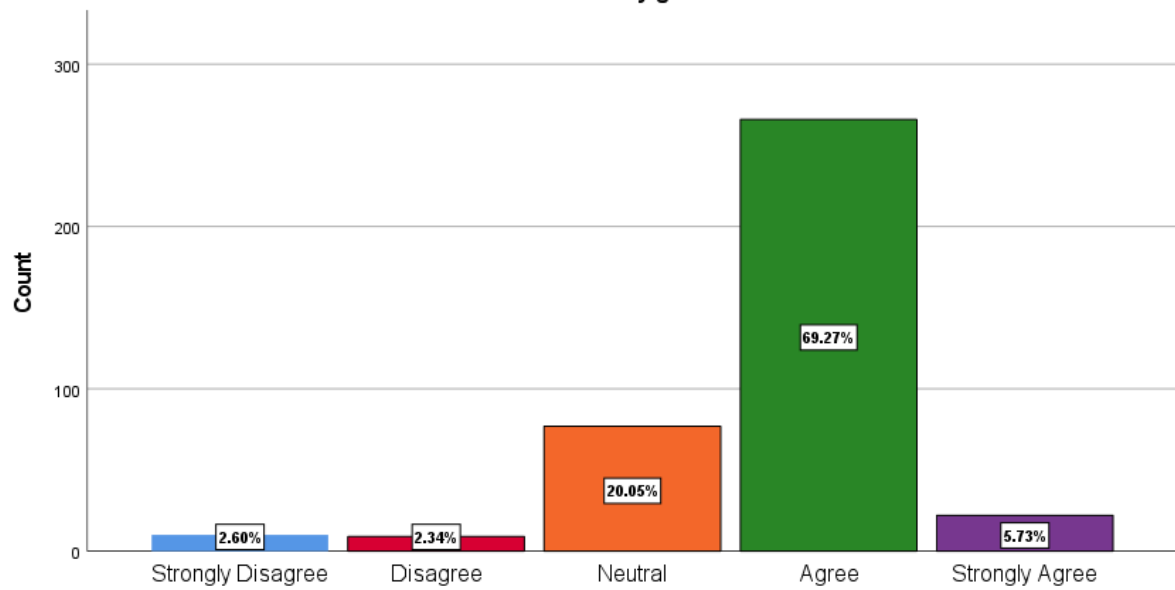




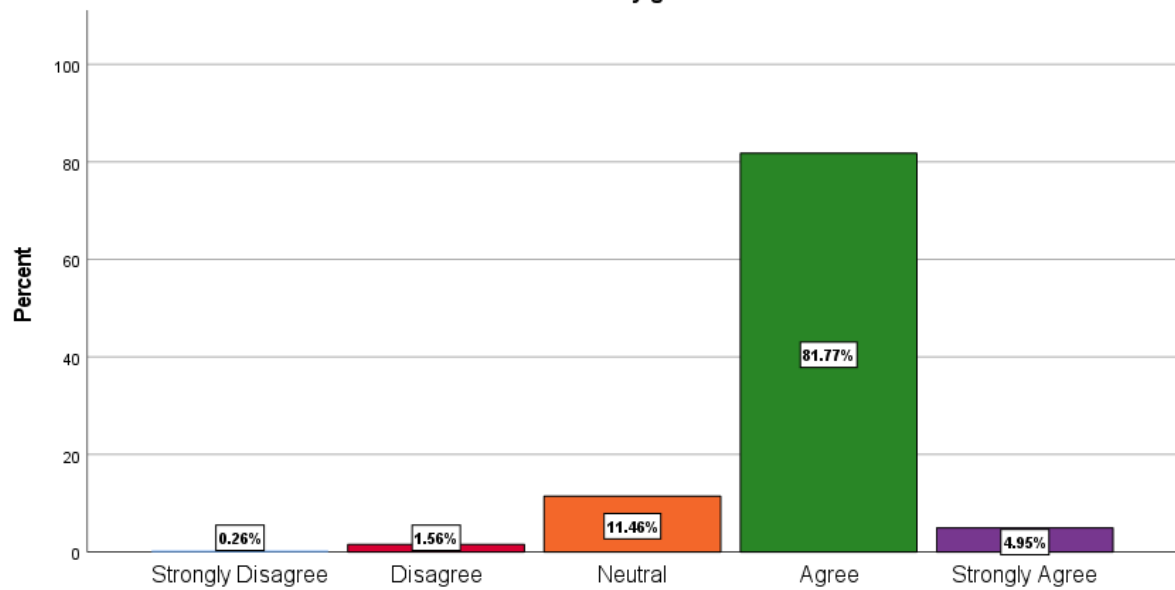
4. When using a smartphone connected to the UKZN network the average time that I spend online per day is



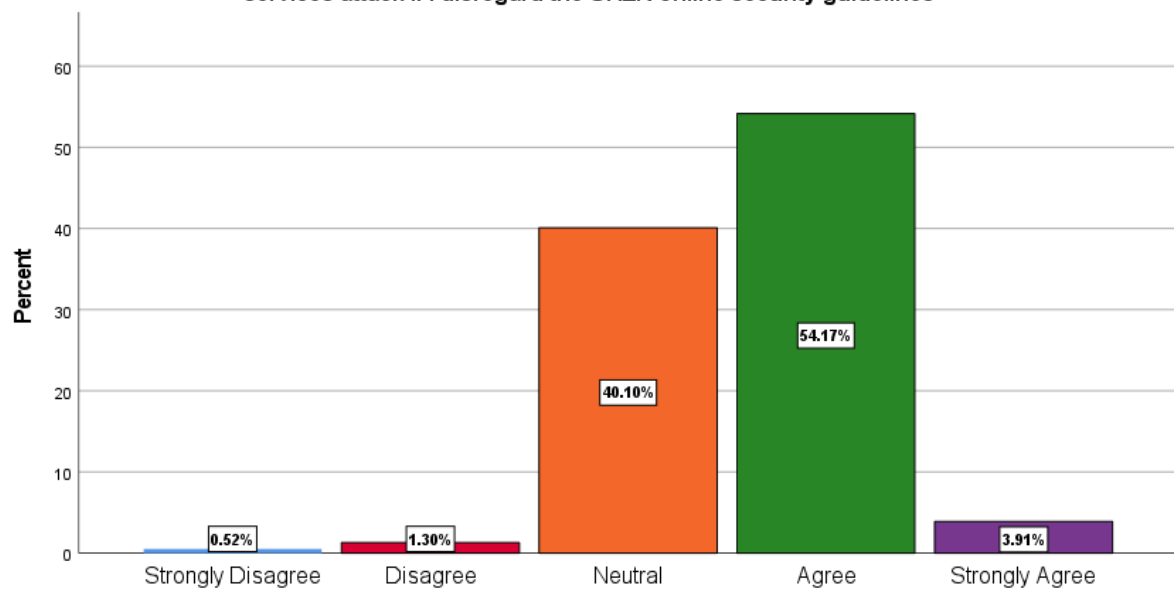
5.1 When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data breach if I disregard UKZN online security guideline



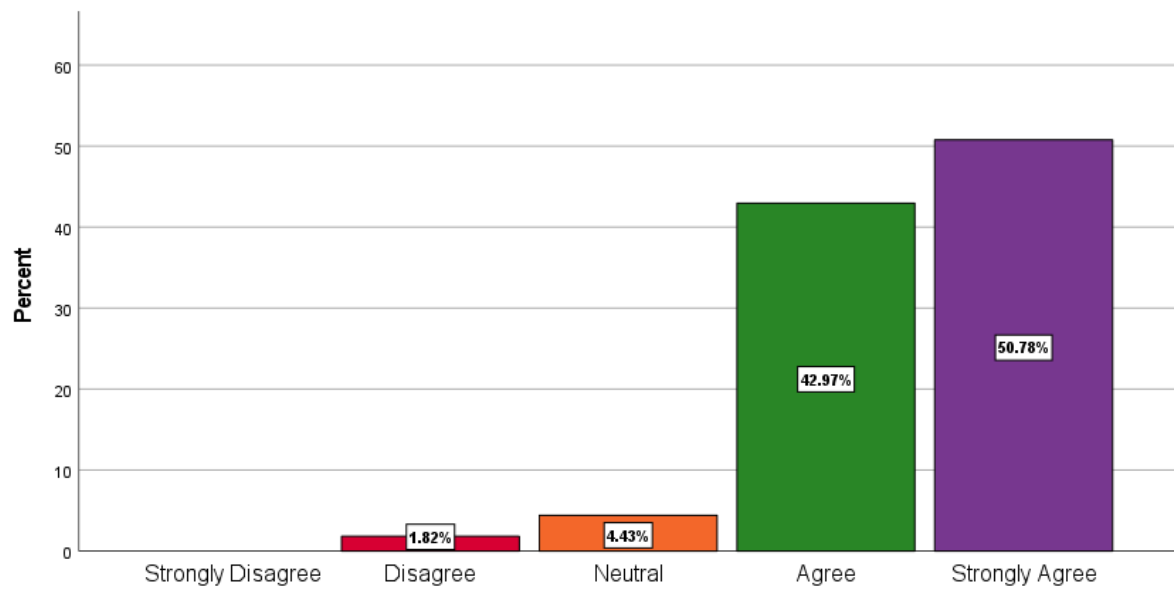
5.2 When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if I disregard the UKZN online security guidelines



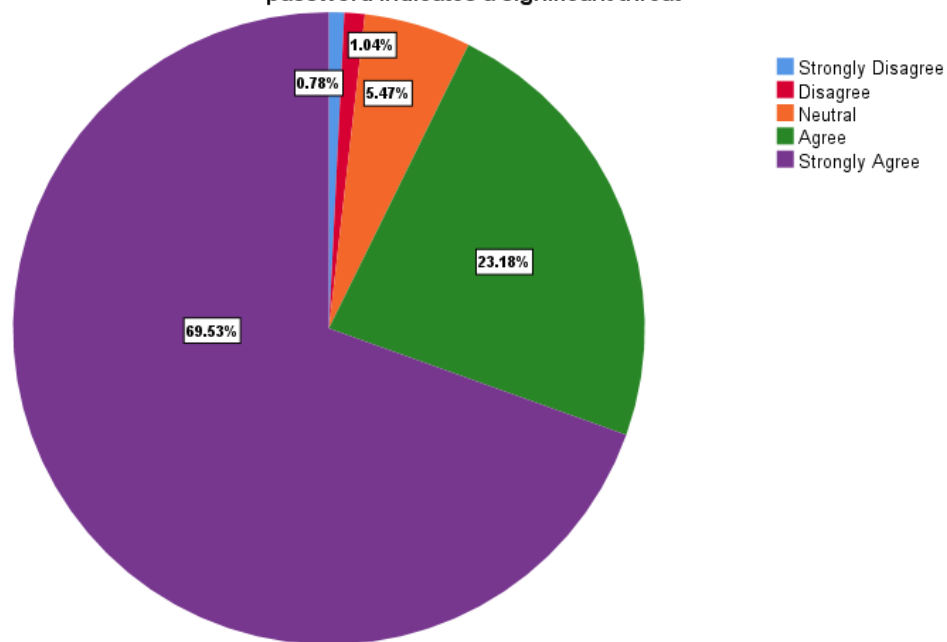
5.3 When using a smartphone connected to the UKZN Wi-Fi, UKZN productivity can experience a disruption of services attack if I disregard the UKZN online security guidelines



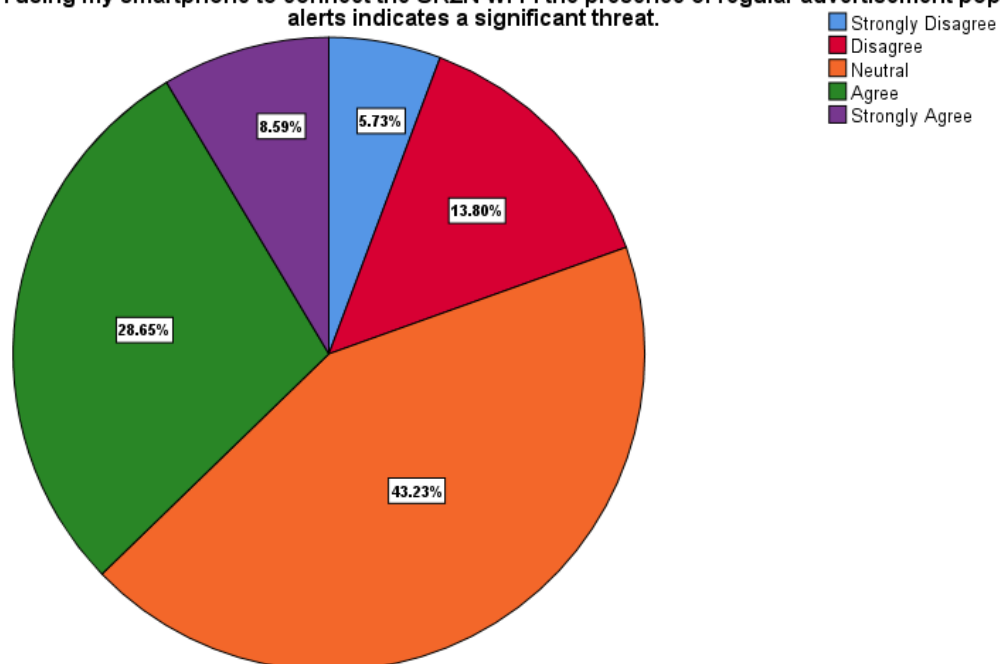
6.1 When using my smartphone to connect the UKZN Wi-Fi a data breach may result in a significant problem for UKZN.



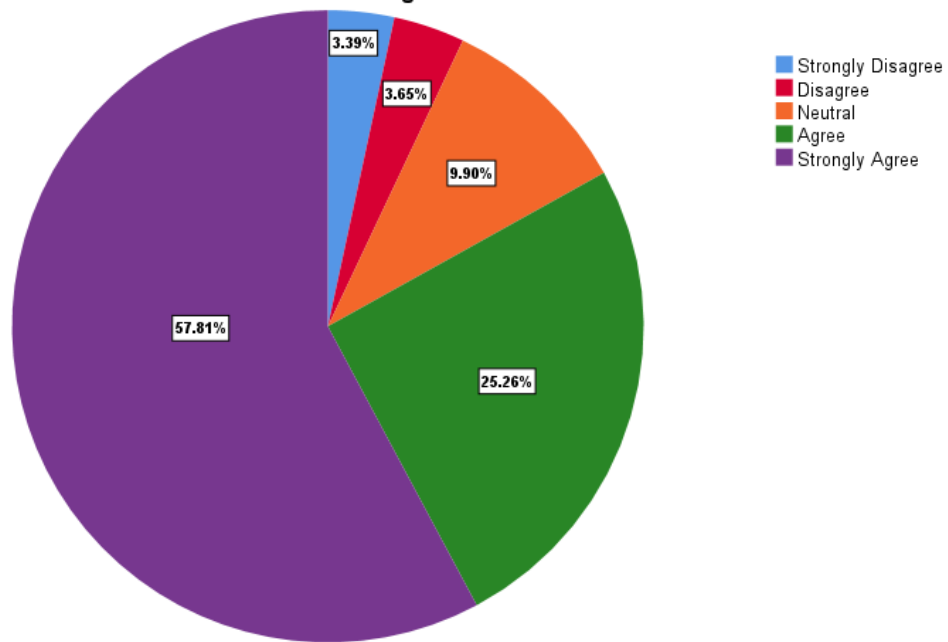
6.2 When using my smartphone to connect the UKZN Wi-Fi an unknown change in my student account password indicates a significant threat



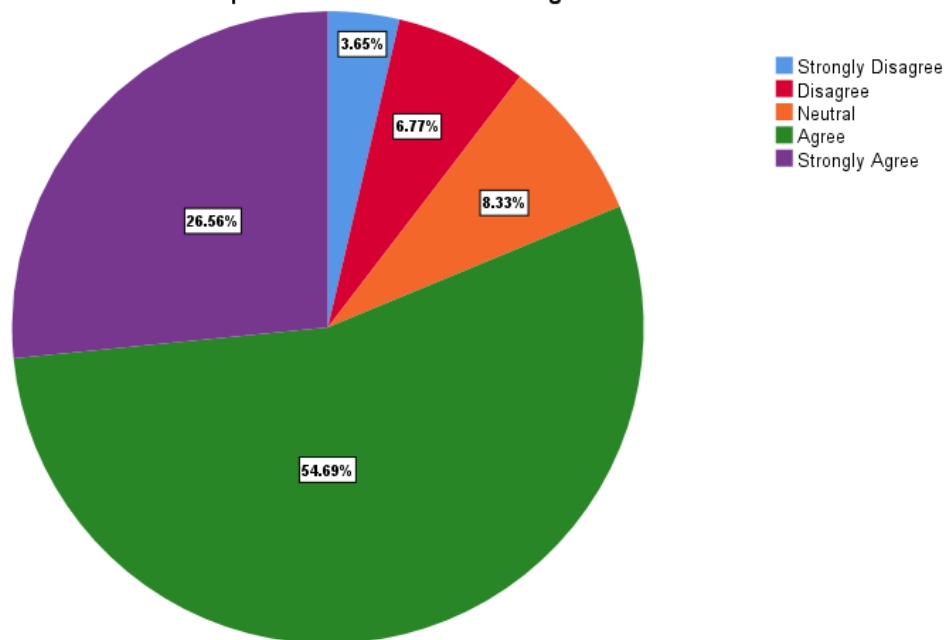
6.3 When using my smartphone to connect the UKZN Wi-Fi the presence of regular advertisement pop-up alerts indicates a significant threat.



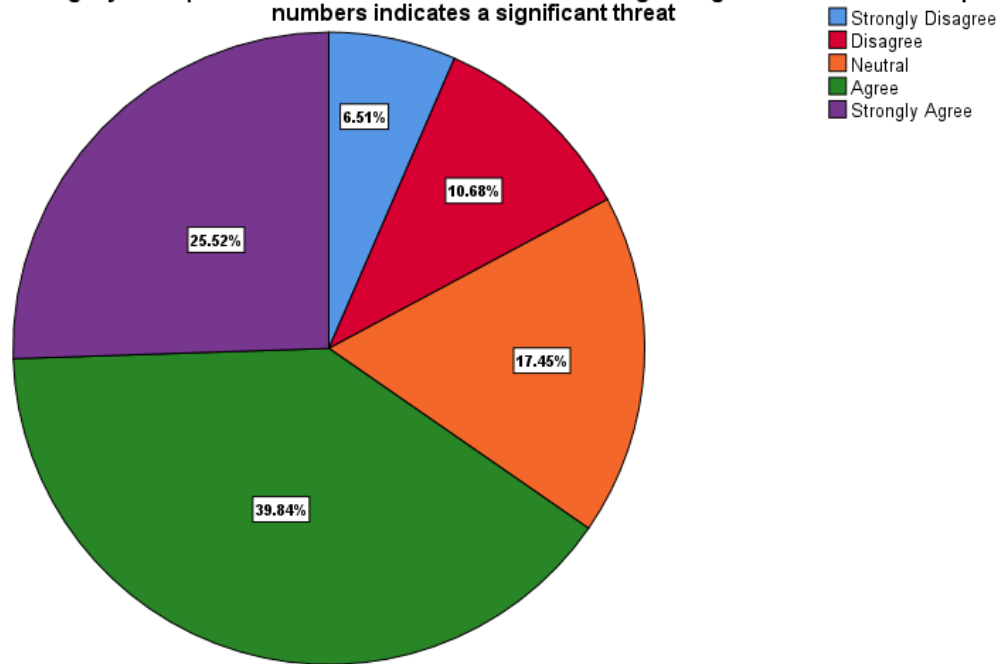
6.4 When using my smartphone to connect the UKZN Wi-Fi financial loss due to data breach indicates a significant threat



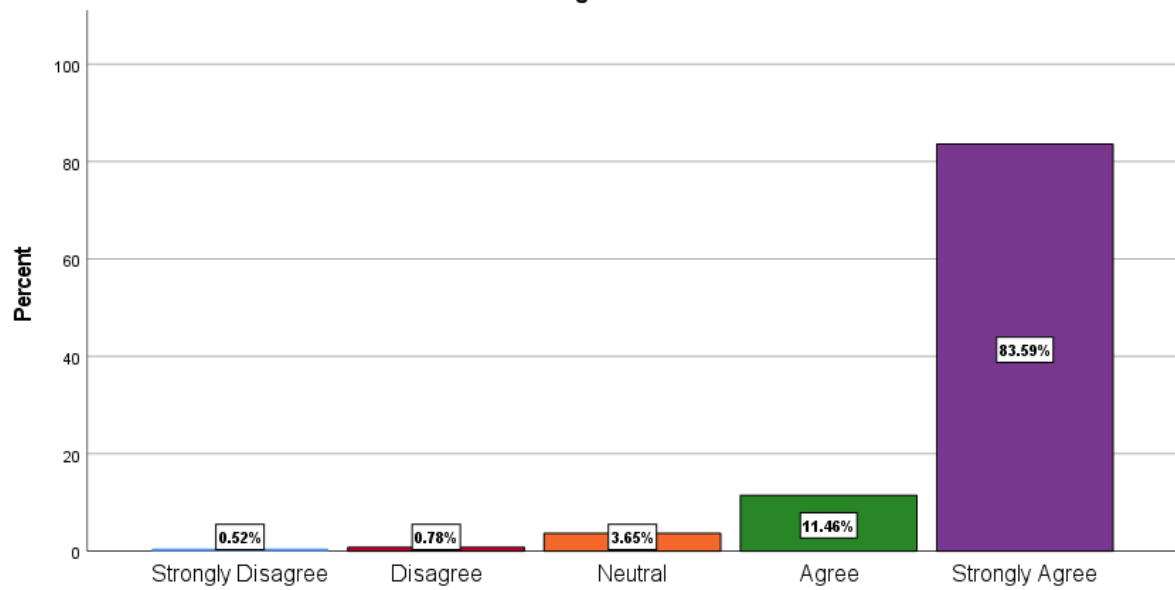
6.5 When using my smartphone to connect the UKZN Wi-Fi receiving strange text messages from unknown phone numbers indicates a significant threat.



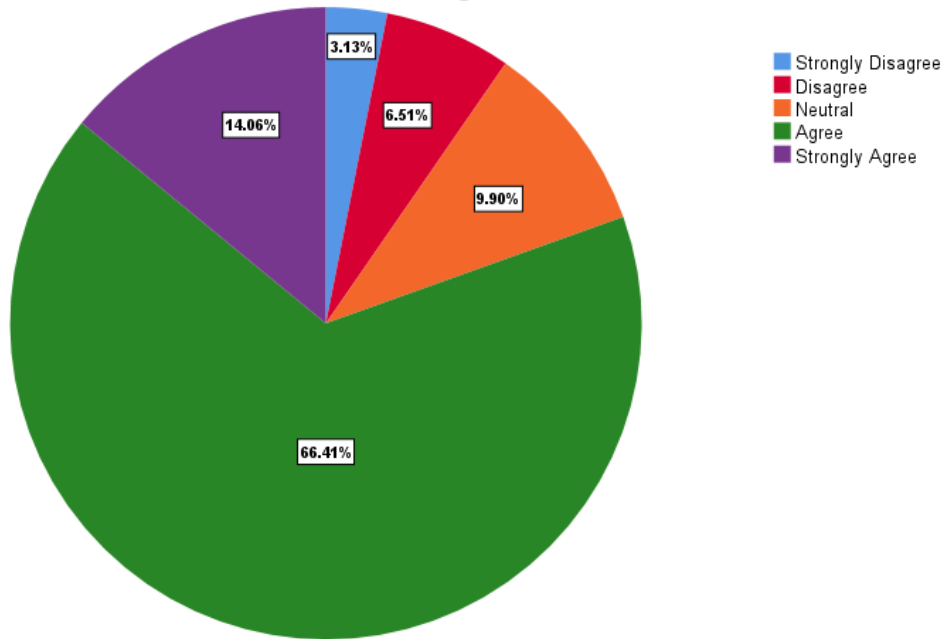
6.6 When using my smartphone to connect the UKZN Wi-Fi receiving strange calls from unknown phone numbers indicates a significant threat



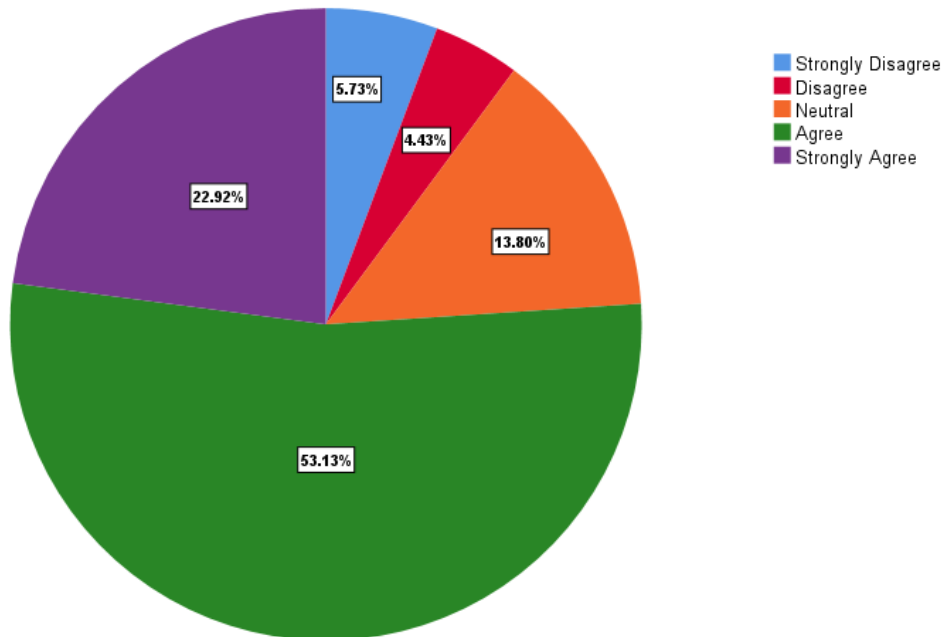
6.7 When using my smartphone to connect the UKZN Wi-Fi receiving strange emails from unknown sources indicates a significant threat.



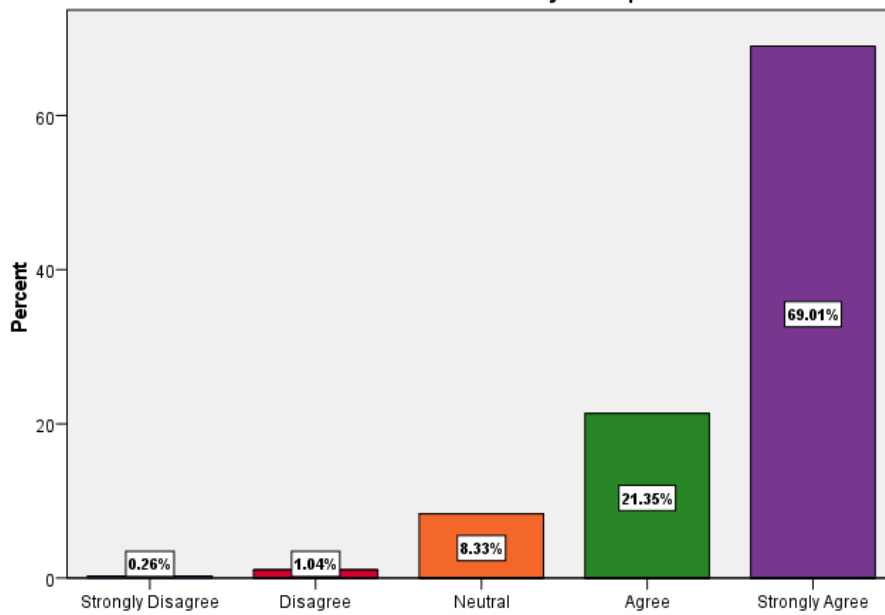
6.8 When using my smartphone to connect the UKZN Wi-Fi the presence of unknown mobile applications indicates a significant threat.



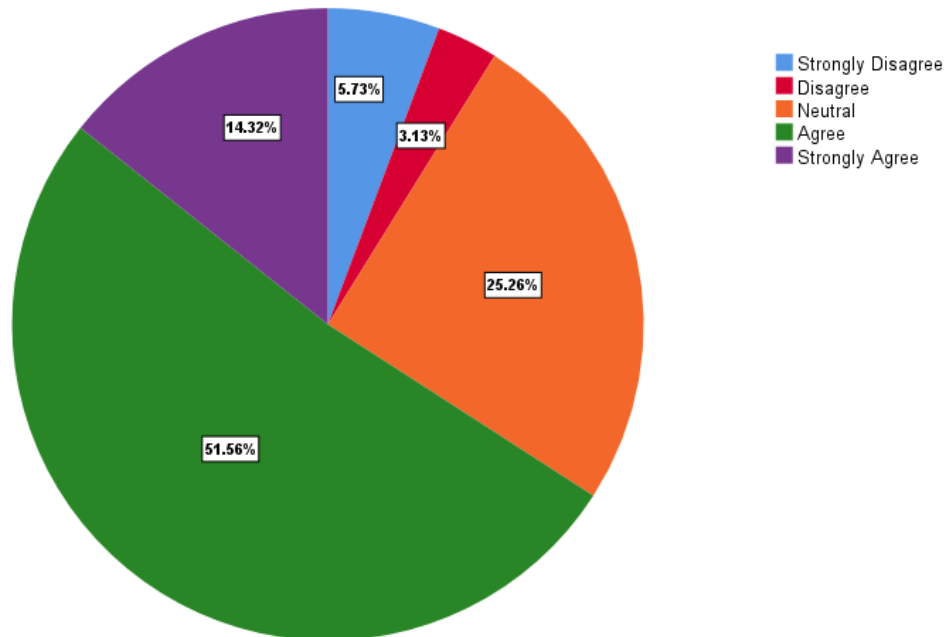
7. Lack of understanding for the UKZN online security guideline may result in a significant problem for UKZN



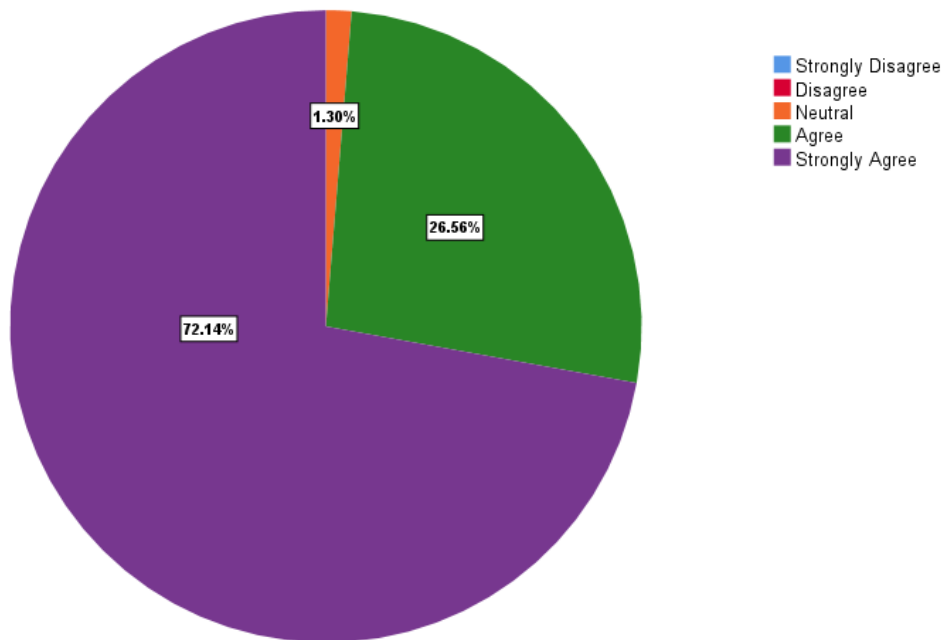
8. UKZN will continually be susceptible to online threats if I do not implement UKZN online security measures on my smartphone



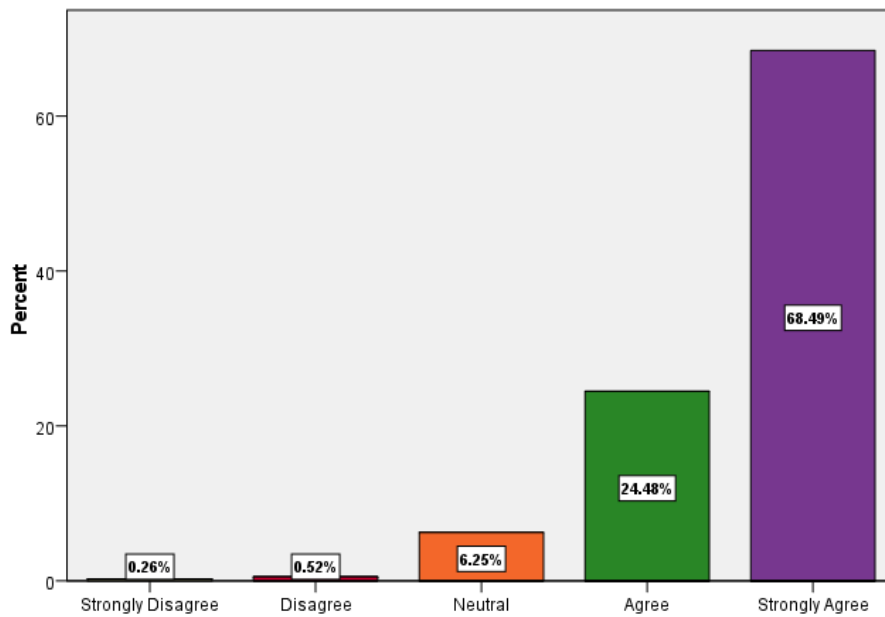
9.1 I believe a disregard for UKZN online security guidelines by me can subject UKZN to a data breach.



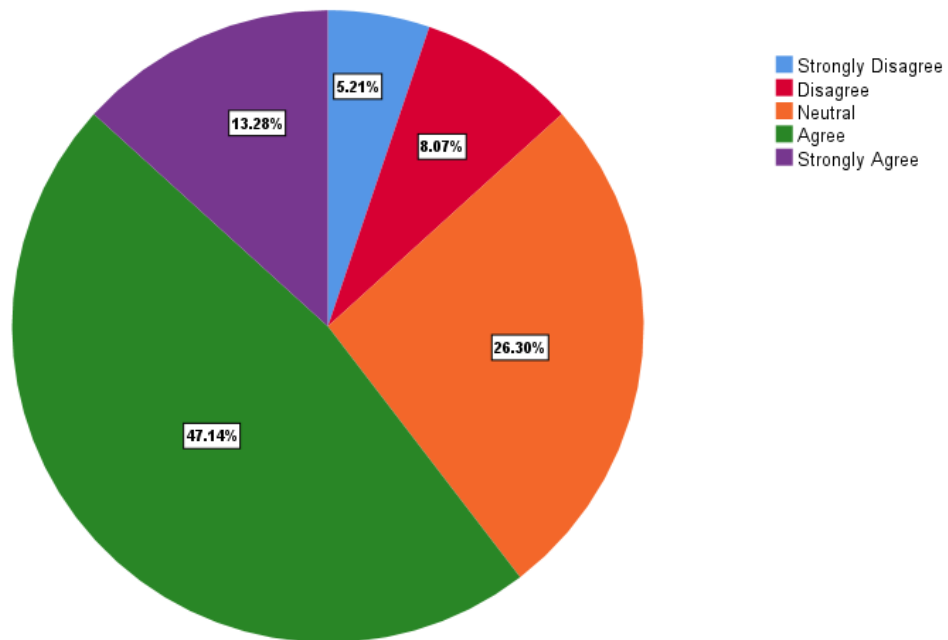
9.2 I believe a disregard for UKZN online security guidelines by me can subject UKZN to a financial loss.



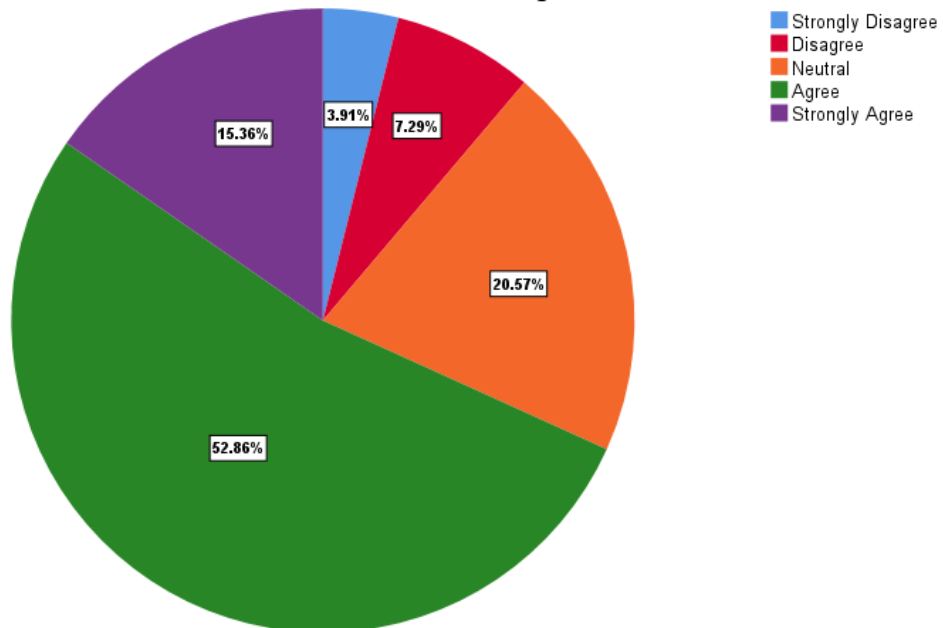
9.3 I believe a disregard for UKZN online security guidelines by me can subject UKZN to identity theft.



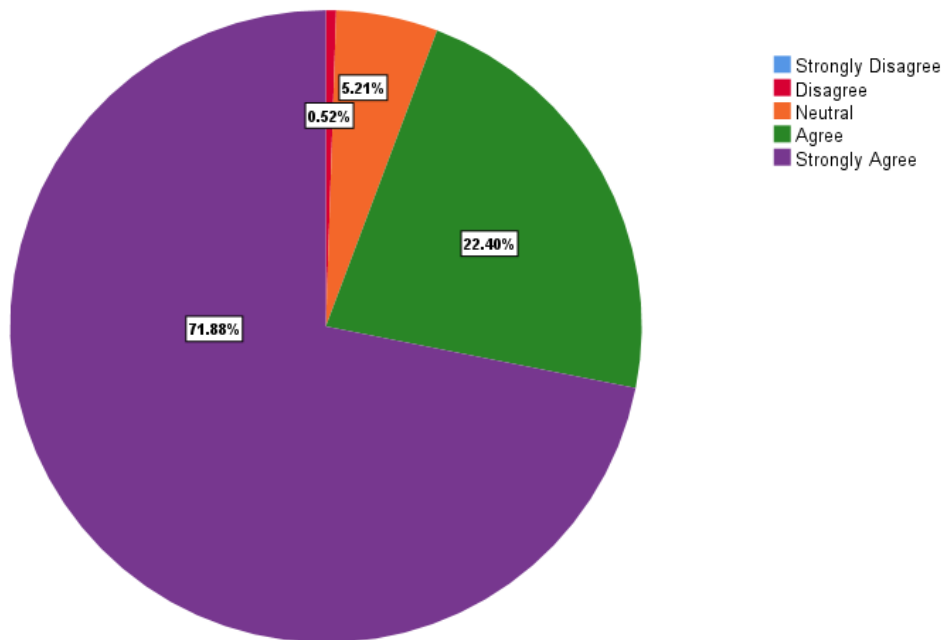
9.4 I believe a disregard for UKZN online security guidelines by me can subject UKZN to disruption of UKZN services.



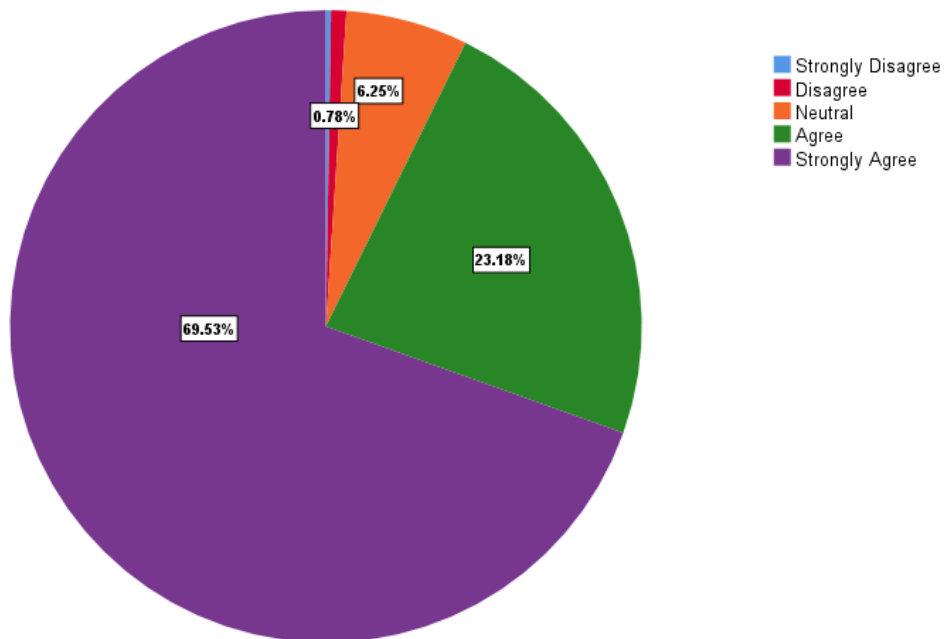
9.5 I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised data in the online storage.



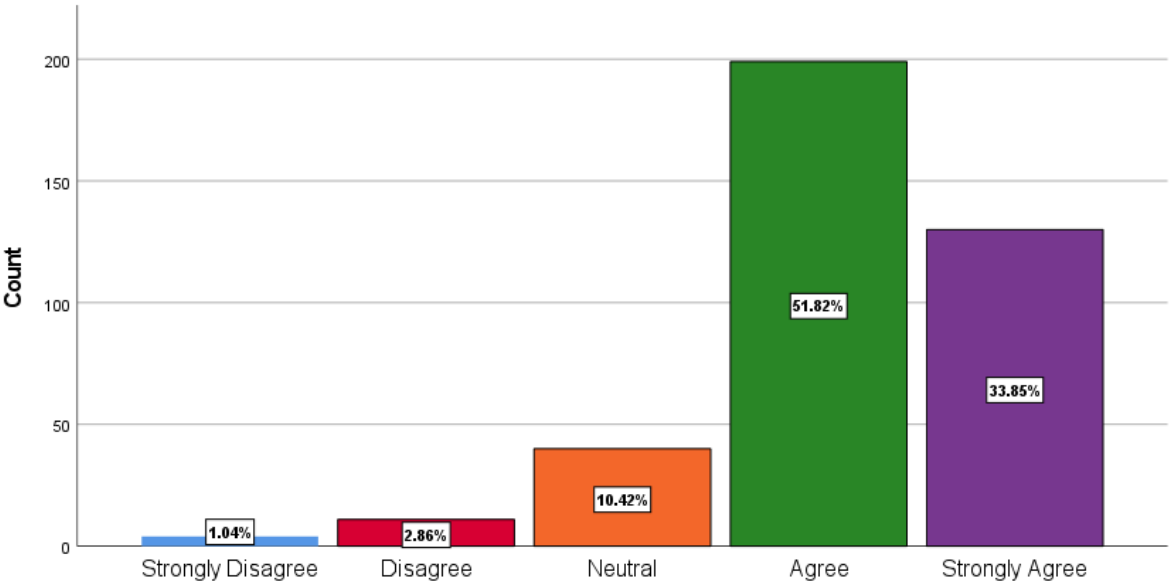
9.6 I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised student accounts.



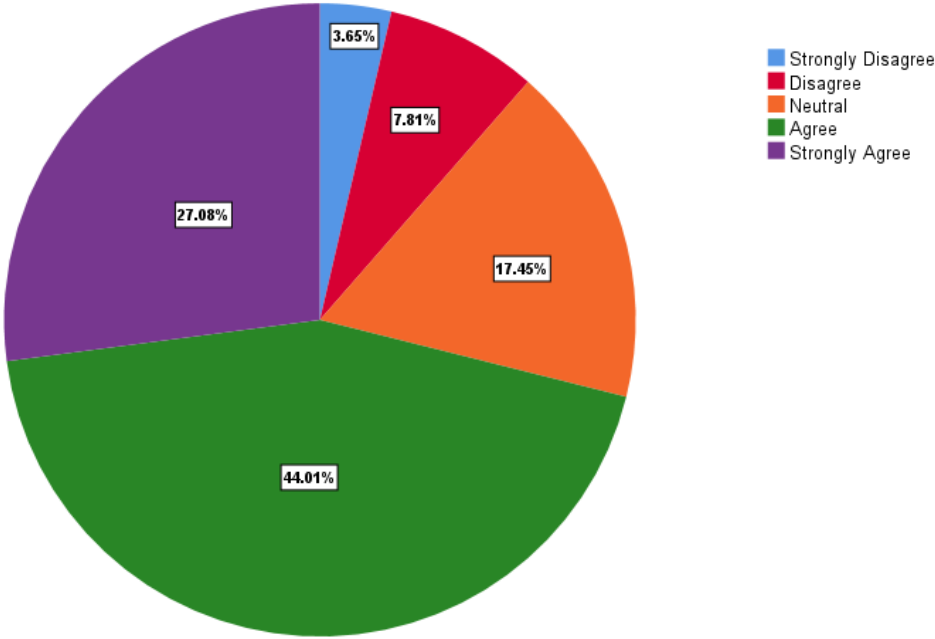
9.7 I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised staff accounts.



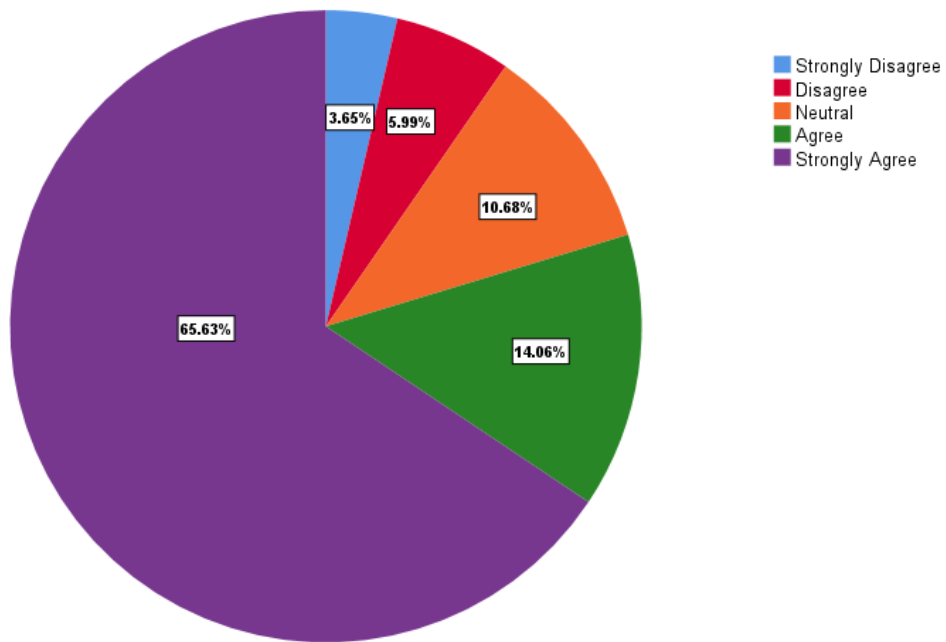
9.8 I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised network.



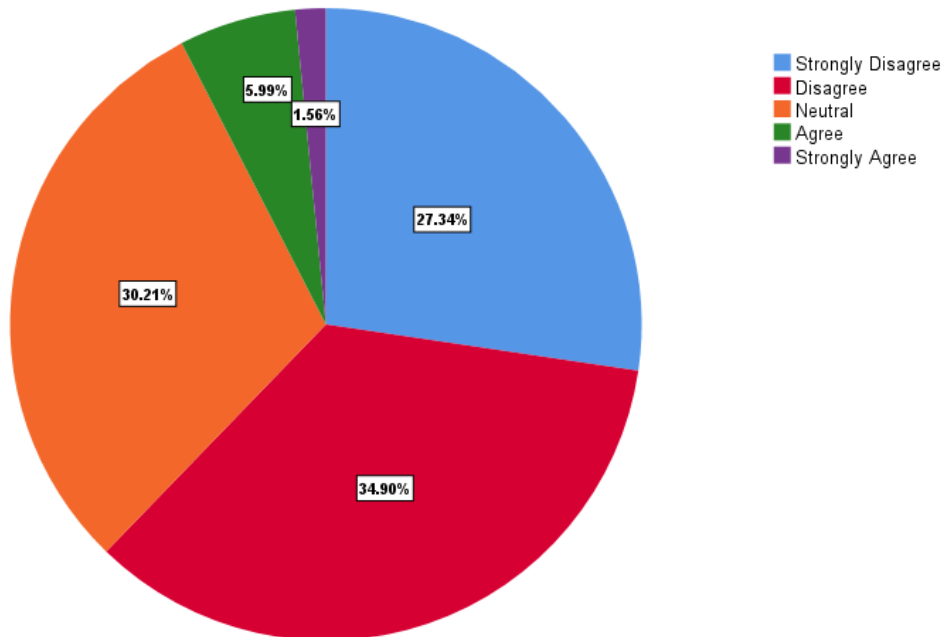
9.9 I believe a disregard for UKZN online security guidelines by me can subject UKZN to malicious software attacks.



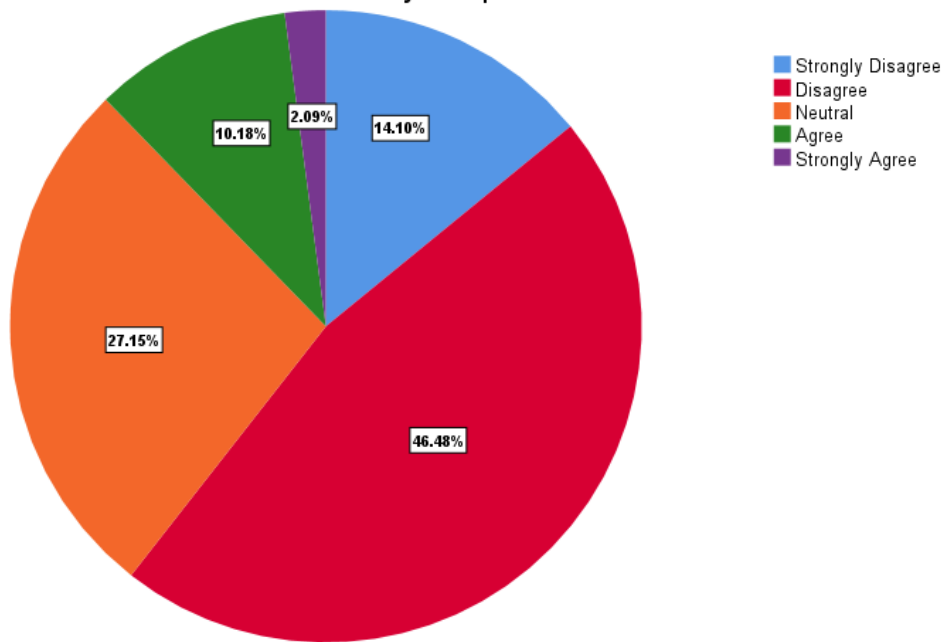
10.1 In the occurrence of a university-wide data breach, the UKZN ICS alerts me to fraudulent email through Microsoft Outlook.



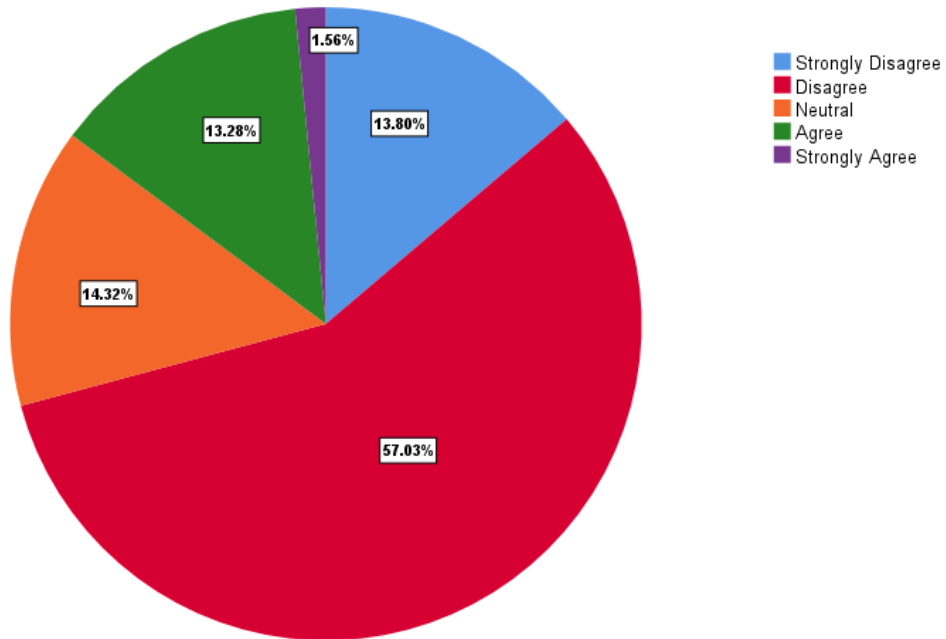
10.2 In the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scams.



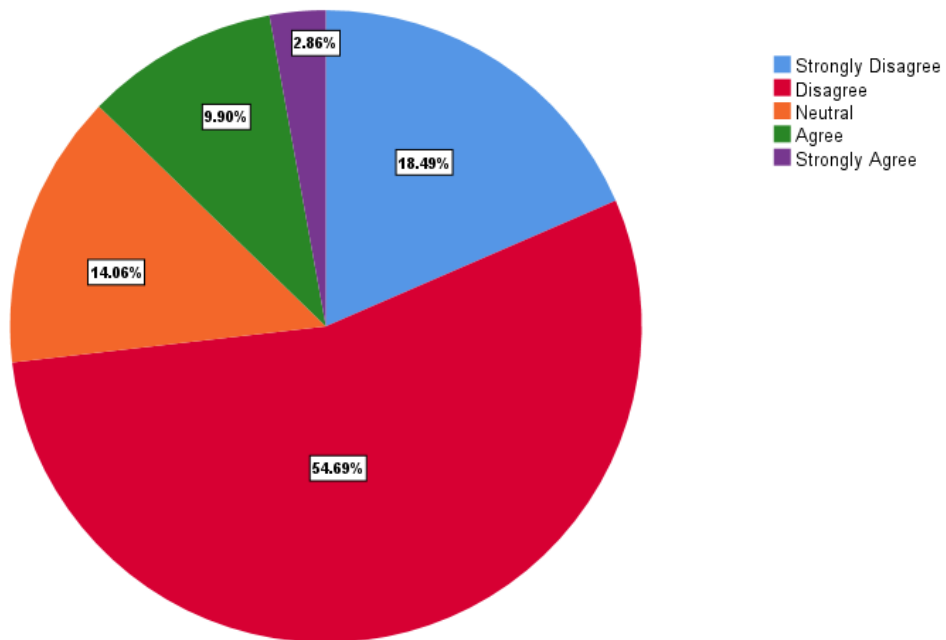
10.3 In the occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure my smartphone.



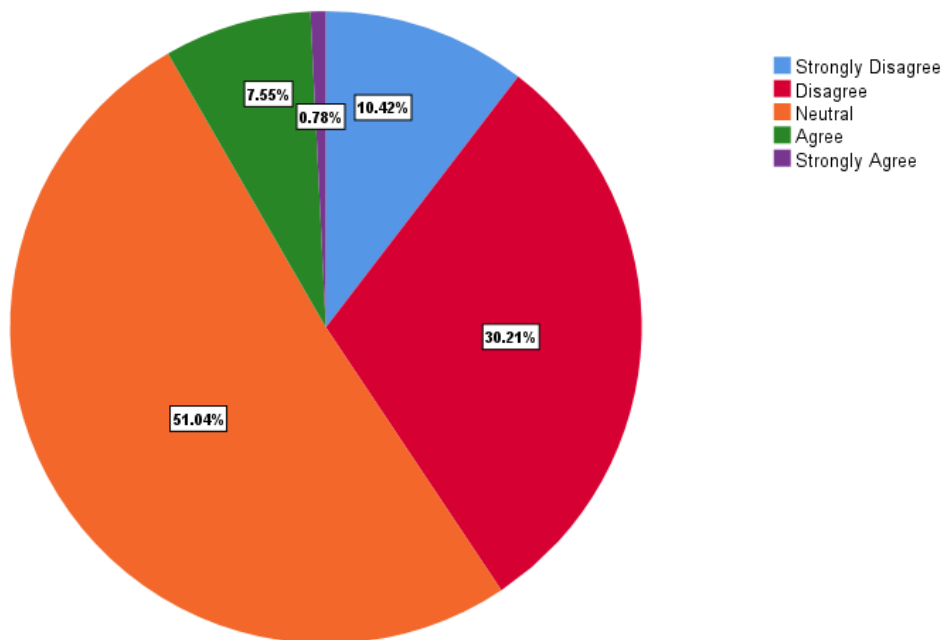
11. I always use UKZN information security guidelines to resolve online threats targeted at my smartphone.



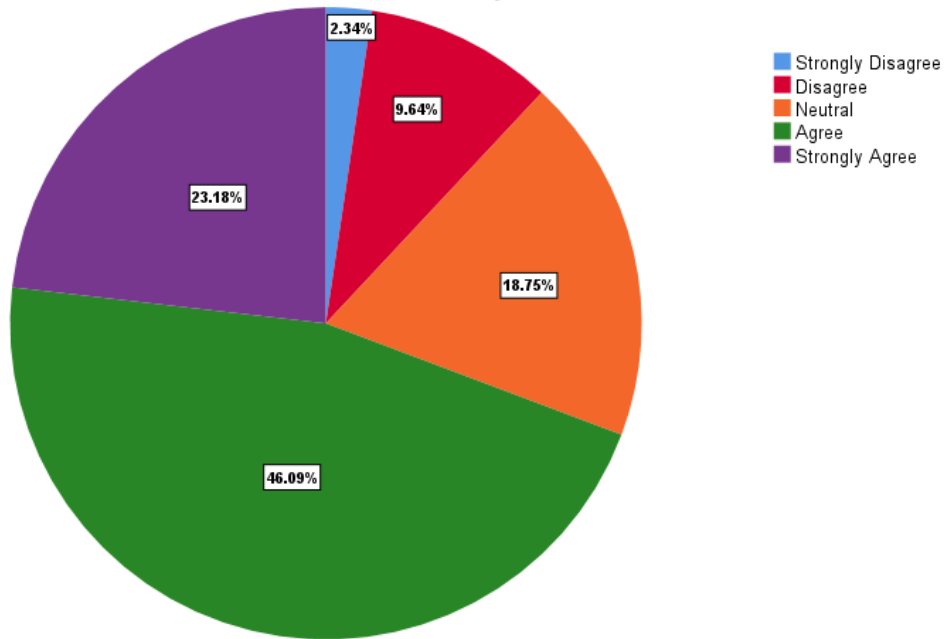
12. I utilise the UKZN ICS call service which operates on weekdays to resolve smartphone security problems.



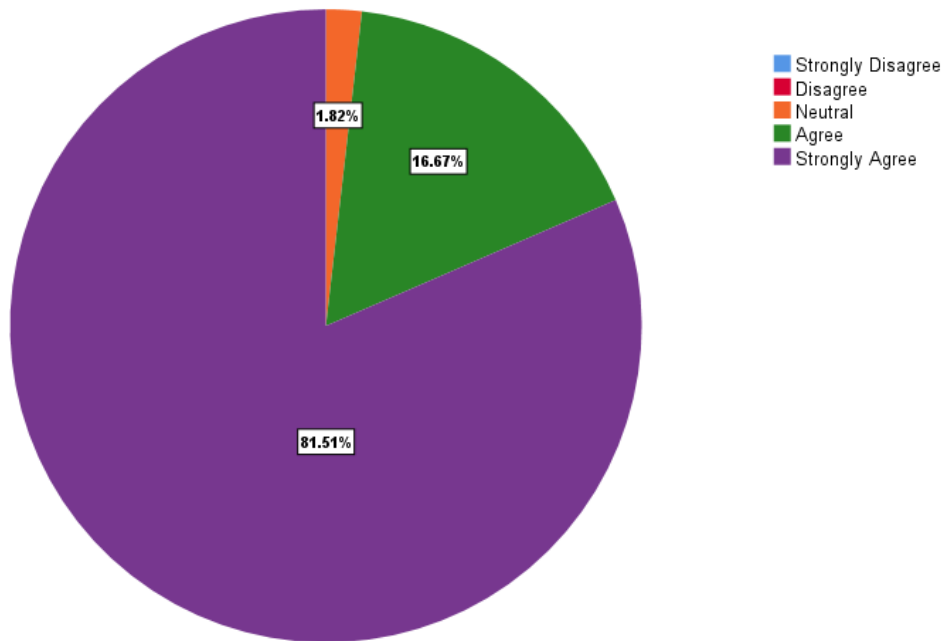
13.1 In response to an online security threat targeted at my smartphone, I install an anti-Virus software.



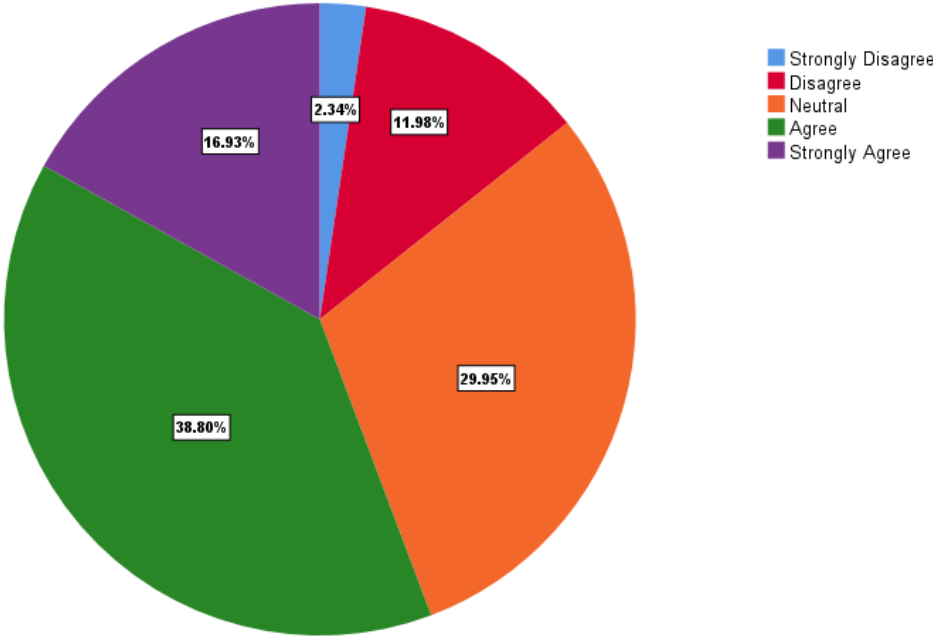
13.2 In response to an online security threat targeted at my smartphone, I use multiple authentication methods to secure my email.



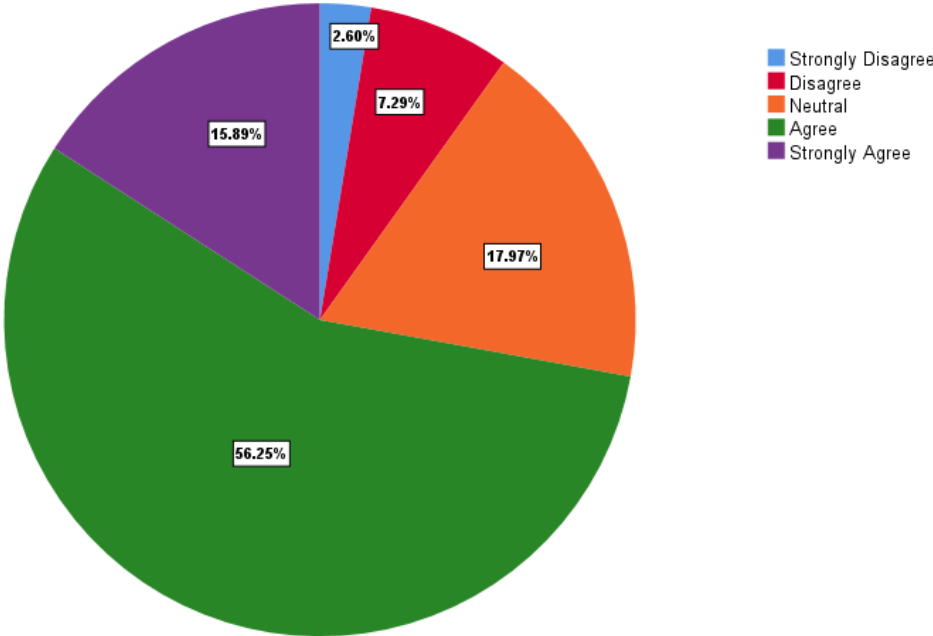
13.3 In response to an online security threat targeted at my smartphone, I install mobile applications used by UKZN from recommended links.



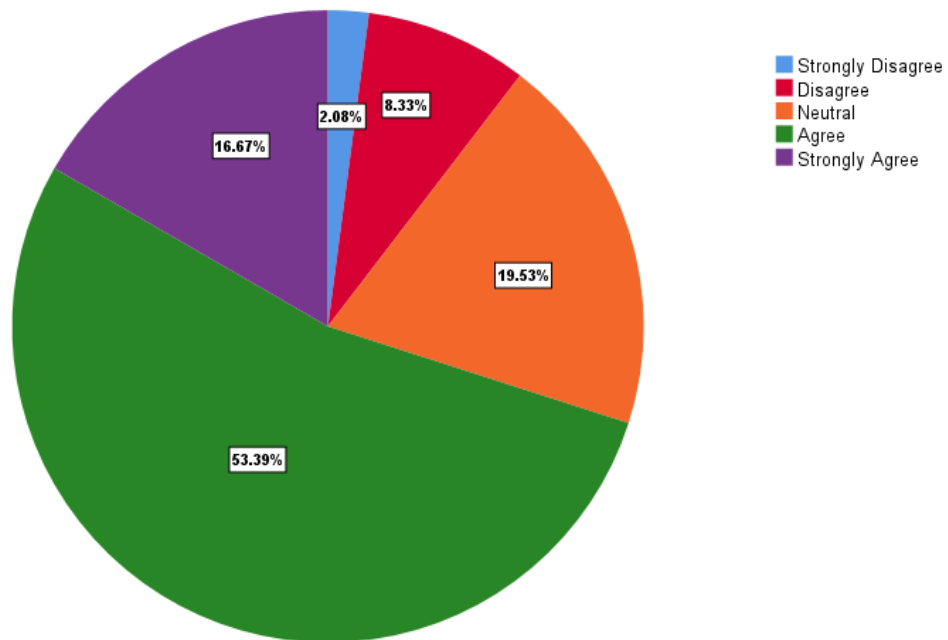
13.4 In response to an online security threat targeted at my smartphone, I pay attention to security messages for mobile application installation.



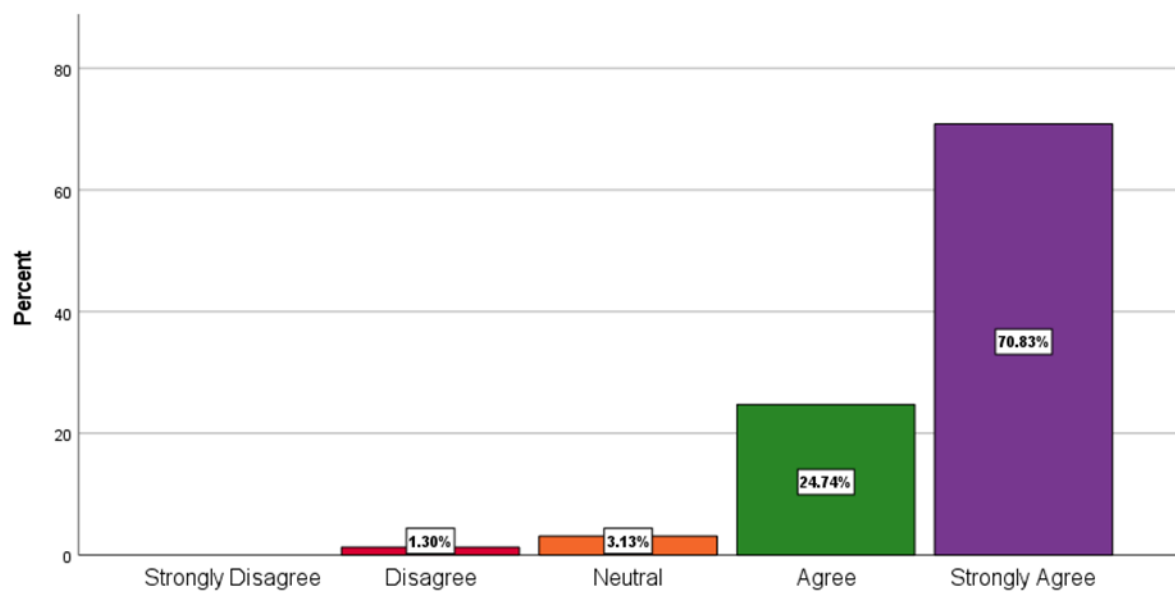
13.5 In response to an online security threat targeted at my smartphone, I change passwords used for various platforms.



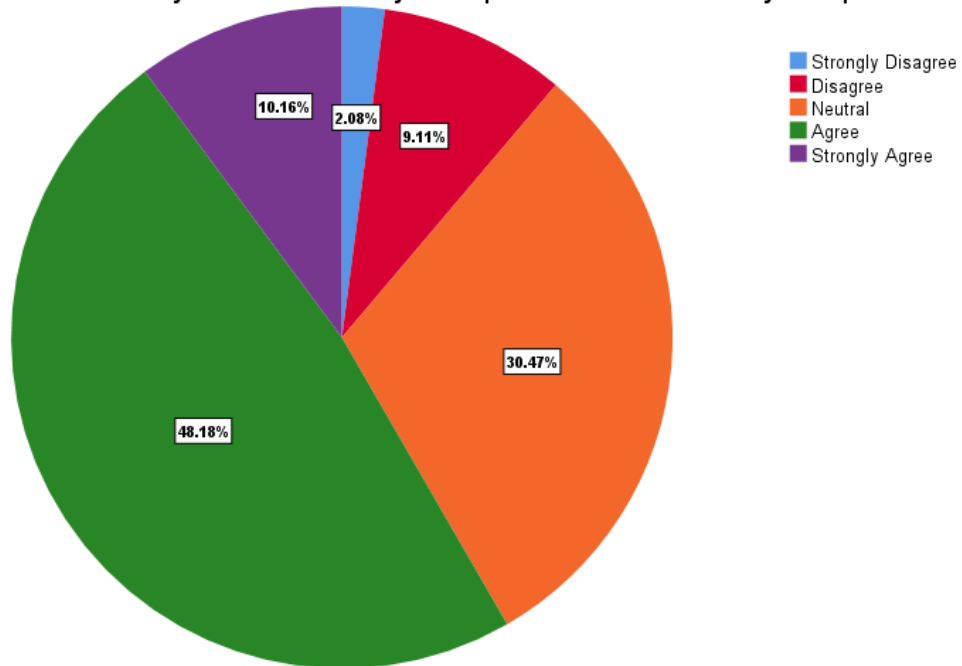
14. It is easy for me to use the UKZN online security guideline to protect my smartphone against online threats.



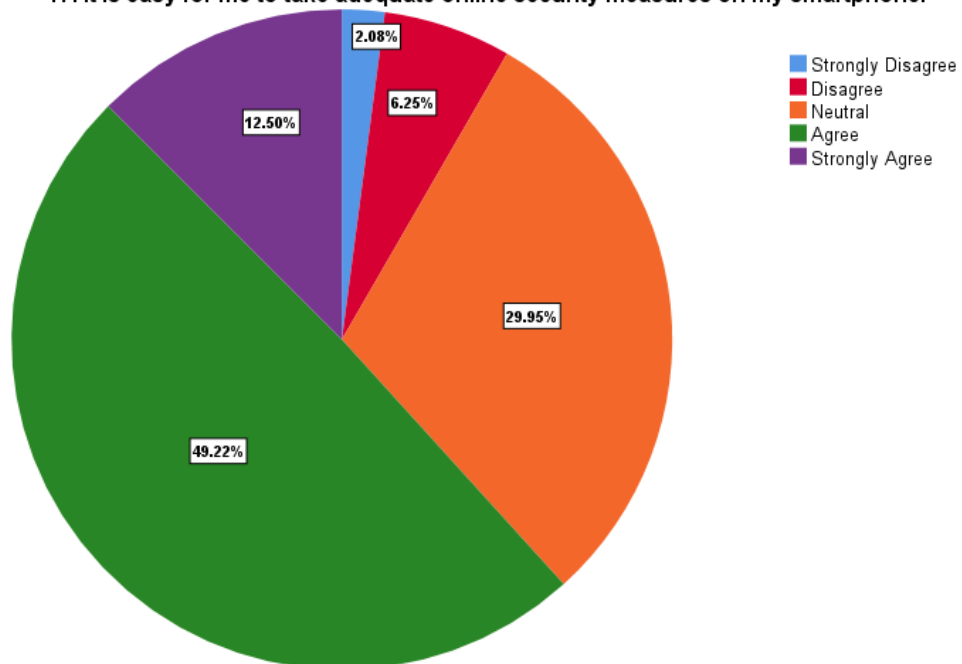
15. It is easy for me to use UKZN online security guideline if I follow an ICS technician's security instruction.



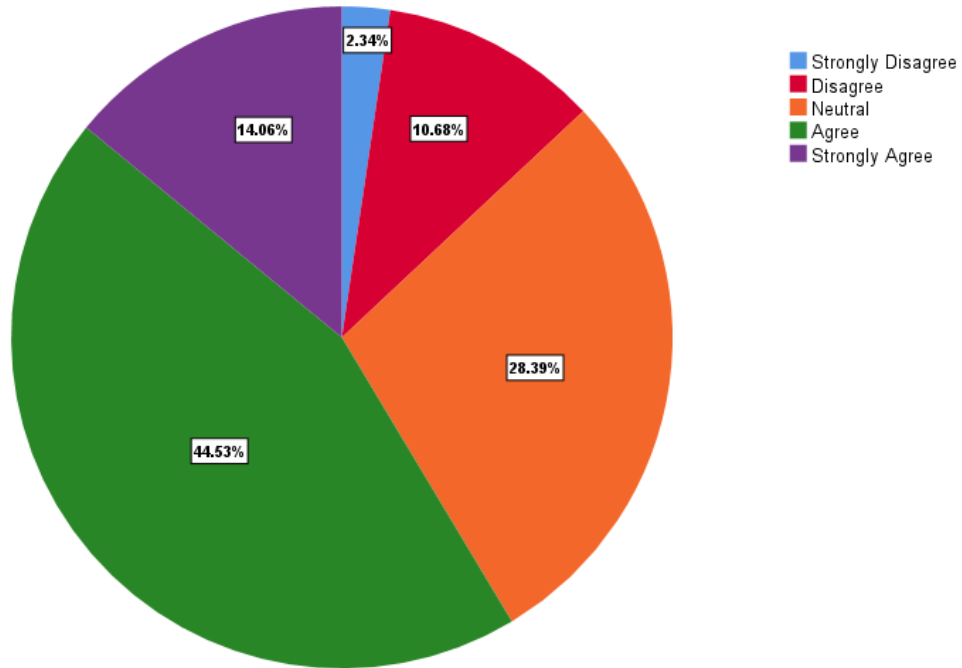
16. It is easy for me to take timely online protective measures on my smartphone.



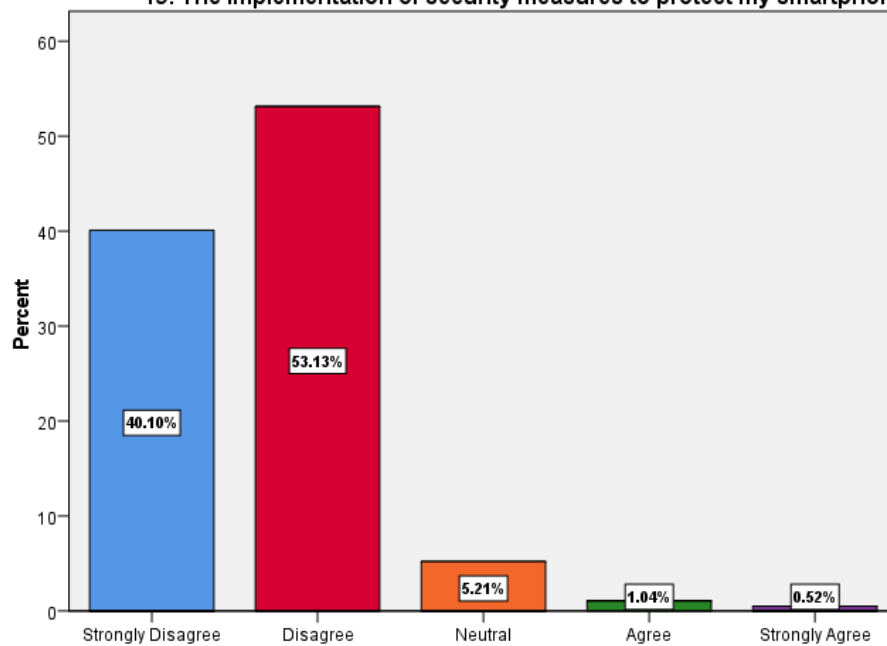
17. It is easy for me to take adequate online security measures on my smartphone.

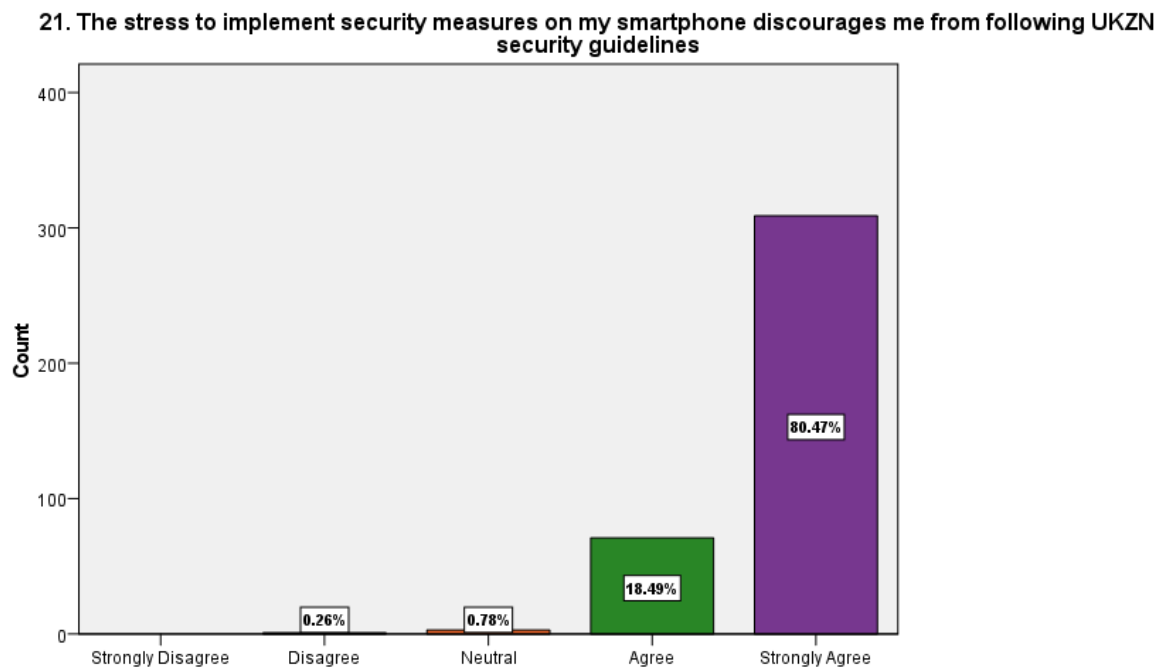
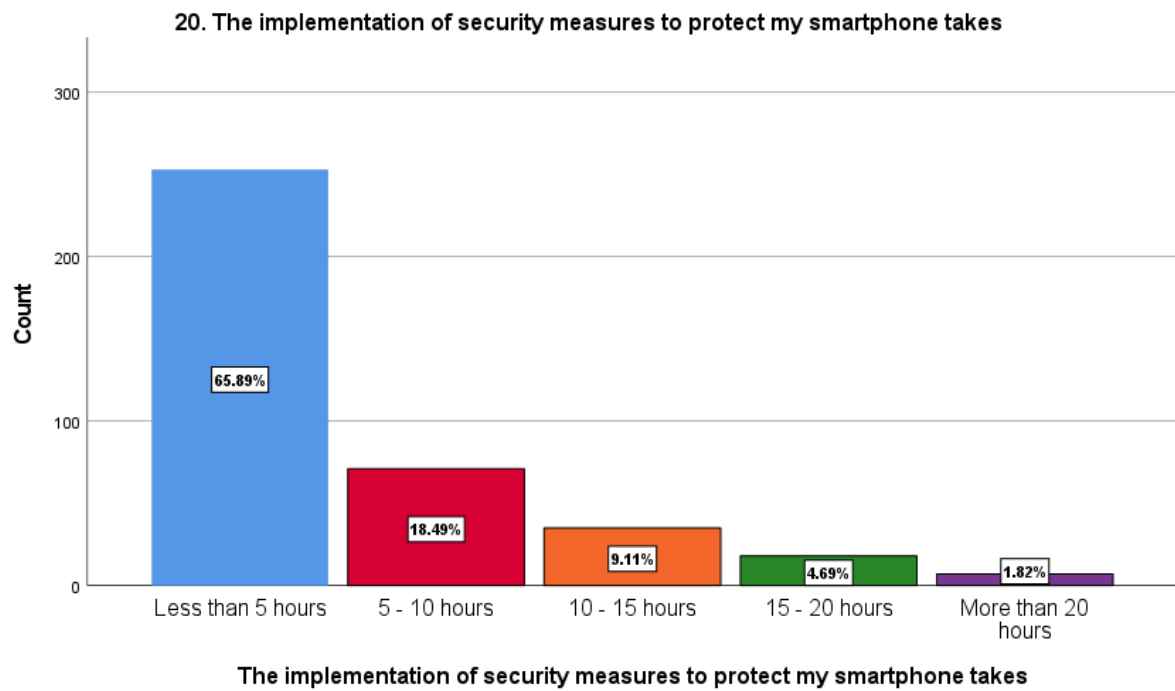


18. I possess the skill to protect myself against online threats targeted at my smartphone



19. The implementation of security measures to protect my smartphone is expensive.





1

One-Sample Test

Test Value = 1

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Gender	24.578	383	.000	.612	.56	.66

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
Gender	Cohen's d	.488	1.254	1.120 1.387
	Hedges' correction	.489	1.252	1.118 1.385

2

One-Sample Test

Test Value = 2

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Age	-23.596	383	.000	-.714	-.77	-.65

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
Age	Cohen's d	.593	-1.204	-1.335 -1.072
	Hedges' correction	.594	-1.202	-1.332 -1.070

3

One-Sample Test						
Test Value = 1						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I am	11.456	383	.000	.255	.21	.30

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I am	Cohen's d	.437	.585	.476	.693
	Hedges' correction	.437	.583	.475	.691

4

One-Sample Test						
Test Value = 3						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using a smartphone connected to the UKZN network the average time that I spend online per day is	-41.597	383	.000	-1.461	-1.53	-1.39

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
When using a smartphone connected to the UKZN network the average time that I spend online per day is	Cohen's d	.688	-2.123	-2.303	-1.942
	Hedges' correction	.690	-2.119	-2.298	-1.938

5.1

One-Sample Test

Test Value = 3						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data breach if I disregard UKZN online security guideline	19.975	383	.000	.732	.66	.80

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data breach if I disregard UKZN online security guideline	Cohen's d	.718	1.019	.896	1.142
	Hedges' correction	.719	1.017	.894	1.140

5.2

One-Sample Test

Test Value = 3						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if I disregard the UKZN online security guidelines	35.850	383	.000	.896	.85	.94

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN may experience data loss if I disregard the UKZN online security guidelines	Cohen's d	.490	1.829	1.665	1.993
	Hedges' correction	.491	1.826	1.662	1.989

5.3

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN productivity can experience a disruption of services attack if I disregard the UKZN online security guidelines	19.030	383	.000	.596	.53	.66

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using a smartphone connected to the UKZN Wi-Fi, UKZN productivity can experience a disruption of services attack if I disregard the UKZN online security guidelines	Cohen's d	.614	.849	1.092
	Hedges' correction	.615	.848	1.090

^a The denominator used in estimating the effect sizes

6.1

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi a data breach may result in a significant problem for UKZN.	41.980	383	.000	1.427	1.36	1.49

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi a data breach may result in a significant problem for UKZN.	Cohen's d	.666	1.960	2.323
	Hedges' correction	.667	1.956	2.319

6.2

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi an unknown change in my student account password indicates a significant threat	43.904	383	.000	1.596	1.52	1.67

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi an unknown change in my student account password indicates a significant threat	Cohen's d	.713	2.240	2.053
	Hedges' correction	.714	2.236	2.048

6.3

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi the presence of regular advertisement pop-up alerts indicates a significant threat.	.187	383	.852	.010	-.10	.12

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi the presence of regular advertisement pop-up alerts indicates a significant threat.	Cohen's d	1.093	.010	-.091
	Hedges' correction	1.096	.010	-.090

6.4

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi financial loss due to data breach indicates a significant threat	25.101	383	.000	1.305	1.20	1.41

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi financial loss due to data breach indicates a significant threat	Cohen's d	1.019	1.145	1.415
	Hedges' correction	1.021	1.143	1.413

6.5

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi receiving strange text messages from unknown phone numbers indicates a significant threat.	18.883	383	.000	.938	.84	1.04

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi receiving strange text messages from unknown phone numbers indicates a significant threat.	Cohen's d	.973	.842	1.084
	Hedges' correction	.975	.840	1.082

6.6

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	90% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi receiving strange calls from unknown phone numbers indicates a significant threat	11.380	383	.000	.672	.57	.77

6.7

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi receiving strange emails from unknown sources indicates a significant threat.	57.647	383	.000	1.768	1.71	1.83

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi receiving strange emails from unknown sources indicates a significant threat.	Cohen's d	.601	2.942	2.710 3.172
	Hedges' correction	.602	2.936	2.705 3.166

6.8

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi the presence of unknown mobile applications indicates a significant threat.	18.503	383	.000	.818	.73	.90

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
When using my smartphone to connect the UKZN Wi-Fi the presence of unknown mobile applications indicates a significant threat.	Cohen's d	.866	.823	1.064
	Hedges' correction	.868	.822	1.062

7

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Lack of understanding for the UKZN online security guideline may result in a significant problem for UKZN	16.010	383	.000	.831	.73	.93

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
Lack of understanding for the UKZN online security guideline may result in a significant problem for UKZN	Cohen's d	1.017	.701	.932
	Hedges' correction	1.019	.700	.930

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
UKZN will continually be susceptible to online threats if I do not implement UKZN online security measures on my smartphone	43.490	383	.000	1.578	1.51	1.65

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
UKZN will continually be susceptible to online threats if I do not implement UKZN online security measures on my smartphone	Cohen's d	.711	2.219	2.033	2.405
	Hedges' correction	.712	2.215	2.029	2.400

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to a data breach.	13.402	383	.000	.656	.56	.75

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to a data breach.	Cohen's d	.960	.684	.572	.795
	Hedges' correction	.961	.683	.571	.793

9.2

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to a financial loss.	69.316	383	.000	1.708	1.66	1.76

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to a financial loss.	Cohen's d	.483	3.267	3.806
	Hedges' correction	.484	3.261	3.799

9.3

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to identity theft.	48.063	383	.000	1.604	1.54	1.67

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to identity theft.	Cohen's d	.654	2.252	2.653
	Hedges' correction	.655	2.247	2.647

9.4

One-Sample Test

Test Value = 3						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to disruption of UKZN services.	10.876	383	.000	.552	.45	.65

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to disruption of UKZN services.	Cohen's d	.995	.555	.447	.662
	Hedges' correction	.997	.554	.446	.661

9.5

One-Sample Test

Test Value = 3						
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised data in the online storage.	14.103	383	.000	.685	.59	.78

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised data in the online storage.	Cohen's d	.952	.720	.607	.832
	Hedges' correction	.954	.718	.606	.830

9.6

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised student accounts.	53.947	383	.000	1.656	1.60	1.72

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised student accounts.	Cohen's d	.602	2.753	2.533 2.972
	Hedges' correction	.603	2.748	2.529 2.966

9.7

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised staff accounts.	47.420	383	.000	1.609	1.54	1.68

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised staff accounts.	Cohen's d	.665	2.420	2.221 2.618
	Hedges' correction	.666	2.415	2.217 2.613

9.8

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised network.	28.257	383	.000	1.146	1.07	1.23

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to compromised network.	Cohen's d	.795	1.442	1.299	1.584
	Hedges' correction	.796	1.439	1.296	1.581

9.9

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to malicious software attacks.	15.811	383	.000	.831	.73	.93

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I believe a disregard for UKZN online security guidelines by me can subject UKZN to malicious software attacks.	Cohen's d	1.030	.807	.691	.922
	Hedges' correction	1.032	.805	.690	.920

10.1

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS alerts me to fraudulent email through Microsoft Outlook.	23.316	383	.000	1.320	1.21	1.43

One-Sample Effect Sizes

			Point Estimate	95% Confidence Interval	
Standardizer ^a				Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS alerts me to fraudulent email through Microsoft Outlook.	Cohen's d	1.110	1.190	1.059	1.320
	Hedges' correction	1.112	1.188	1.057	1.318

10.2

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scams.	-16.419	383	.000	-.802	-.90	-.71

One-Sample Effect Sizes

			Point Estimate	95% Confidence Interval	
Standardizer ^a				Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS provides a fraudulent email quiz to help me become aware of email scams.	Cohen's d	.957	-.838	-.954	-.721
	Hedges' correction	.959	-.836	-.952	-.720

10.3

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure my smartphone.	-12.784	382	.000	-.603	-.70	-.51

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
In the occurrence of a university-wide data breach, the UKZN ICS provides technical assistance to secure my smartphone.	Cohen's d	.923	-.763	-.543
	Hedges' correction	.925	-.762	-.541

11

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I always use UKZN information security guidelines to resolve online threats targeted at my smartphone.	-14.464	383	.000	-.682	-.78	-.59

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
I always use UKZN information security guidelines to resolve online threats targeted at my smartphone.	Cohen's d	.924	-.851	-.625
	Hedges' correction	.926	-.849	-.624

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I utilise the UKZN ICS call service which operates on weekdays to resolve smartphone security problems.	-15.500	383	.000	-.760	-.86	-.66

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I utilise the UKZN ICS call service which operates on weekdays to resolve smartphone security problems.	Cohen's d	.961	-.791	-.905	-.676
	Hedges' correction	.963	-.789	-.903	-.675

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In response to an online security threat targeted at my smartphone, I install an anti-Virus software.	-10.180	383	.000	-.419	-.50	-.34

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
In response to an online security threat targeted at my smartphone, I install an anti-Virus software.	Cohen's d	.807	-.519	-.626	-.413
	Hedges' correction	.809	-.518	-.625	-.412

13.2

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In response to an online security threat targeted at my smartphone, I use multiple authentication methods to secure my email.	15.542	383	.000	.781	.68	.88

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
In response to an online security threat targeted at my smartphone, I use multiple authentication methods to secure my email.	Cohen's d	.985	.793	.678	.907
	Hedges' correction	.987	.792	.677	.906

13.3

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In response to an online security threat targeted at my smartphone, I install mobile applications used by UKZN from recommended links.	78.964	383	.000	1.797	1.75	1.84

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
In response to an online security threat targeted at my smartphone, I install mobile applications used by UKZN from recommended links.	Cohen's d	.446	4.030	3.727	4.331
	Hedges' correction	.447	4.022	3.720	4.323

13.4

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In response to an online security threat targeted at my smartphone, I pay attention to security messages for mobile application installation.	11.153	383	.000	.560	.46	.66

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
In response to an online security threat targeted at my smartphone, I pay attention to security messages for mobile application installation.	Cohen's d	.984	.569	.461	.677
	Hedges' correction	.986	.568	.460	.675

13.5

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
In response to an online security threat targeted at my smartphone, I change passwords used for various platforms.	16.492	382	.000	.757	.67	.85

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
In response to an online security threat targeted at my smartphone, I change passwords used for various platforms.	Cohen's d	.899	.843	.726	.959
	Hedges' correction	.900	.841	.724	.957

14

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
It is easy for me to use the UKZN online security guideline to protect my smartphone against online threats.	16.076	383	.000	.742	.65	.83

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
It is easy for me to use the UKZN online security guideline to protect my smartphone against online threats.	Cohen's d	.905	.820	.704
	Hedges' correction	.906	.819	.703

15

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
It is easy for me to use UKZN online security guideline if I follow an ICS technician's security instruction.	53.278	383	.000	1.651	1.59	1.71

One-Sample Effect Sizes

	Standardizer ^a	Point Estimate	95% Confidence Interval	
			Lower	Upper
It is easy for me to use UKZN online security guideline if I follow an ICS technician's security instruction.	Cohen's d	.607	2.719	2.501
	Hedges' correction	.608	2.713	2.497

16

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
It is easy for me to take timely online protective measures on my smartphone.	12.412	383	.000	.552	.46	.64

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
It is easy for me to take timely online protective measures on my smartphone.	Cohen's d	.872	.633	.523	.743
	Hedges' correction	.873	.632	.522	.741

17

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
It is easy for me to take adequate online security measures on my smartphone.	14.605	383	.000	.638	.55	.72

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
It is easy for me to take adequate online security measures on my smartphone.	Cohen's d	.856	.745	.632	.858
	Hedges' correction	.858	.744	.631	.856

18

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
I possess the skill to protect myself against online threats targeted at my smartphone	11.952	383	.000	.573	.48	.67

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
I possess the skill to protect myself against online threats targeted at my smartphone	Cohen's d	.939	.610	.501	.719
	Hedges' correction	.941	.609	.500	.717

19

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
The implementation of security measures to protect my smartphone is expensive.	-38.548	383	.000	-1.312	-1.38	-1.25

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
The implementation of security measures to protect my smartphone is expensive.	Cohen's d	.667	-1.967	-2.138	-1.795
	Hedges' correction	.669	-1.963	-2.134	-1.792

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
The implementation of security measures to protect my smartphone takes	-28.868	383	.000	-1.419	-1.52	-1.32

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
The implementation of security measures to protect my smartphone takes	Cohen's d	.963	-1.473	-1.617	-1.328
	Hedges' correction	.965	-1.470	-1.614	-1.326

One-Sample Test

Test Value = 3

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
The stress to implement security measures on my smartphone discourages me from following UKZN security guidelines	79.164	383	.000	1.792	1.75	1.84

One-Sample Effect Sizes

		Standardizer ^a	Point Estimate	95% Confidence Interval	
				Lower	Upper
The stress to implement security measures on my smartphone discourages me from following UKZN security guidelines	Cohen's d	.444	4.040	3.736	4.342
	Hedges' correction	.444	4.032	3.729	4.334

Case Processing Summary

		N	%
Cases	Valid	382	99.5
	Excluded^a	2	.5
	Total	384	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's	
Alpha	N of Items
.751	44

Ethical Clearance



07 April 2020

Miss Oluwafisayo Kaka (208513240)
School Of Man Info Tech & Gov
Westville Campus

Dear Miss Kaka,

Protocol reference number: HSSREC/00001150/2020

Project title: Security Practices of Smartphone Users at UKZN Westville Campus and Its Effects on the Institutional Information Systems

Degree: Masters

Approval Notification – Amendment Application

This letter serves to notify you that your application and request for an amendment received on 07 April 2020 has now been approved as follows:

- **Change in data collection method**

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

Best wishes for the successful completion of your research protocol.

Yours faithfully



Professor Dipane Hlalele (Chair)

/dd

Humanities & Social Sciences Research Ethics Committee
UKZN Research Ethics Office Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Tel: +27 31 260 8350 / 4557 / 3587
Website: <http://research.ukzn.ac.za/Research-Ethics/>

Founding Campuses: ■ Edgewood ■ Howard College ■ Medical School ■ Pietermaritzburg ■ Westville

INSPIRING GREATNESS