UNIVERSITY OF KWAZULU-NATAL

Gender responses towards online social engineering attacks amongst young adult students in South Africa

By
Happyness Nothando Ngwane
210527408

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

School of Management, IT and Governance
College of Law and Management Studies

Supervisor: Professor Manoj Sewak Maharaj

2019

DECLARATION

I, Happyness Nothando Ngwane 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 an 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.

Signature: 

Date: 06-August-2020

ACKNOWLEDGEMENTS

I would like to thank God for giving me the strength throughout challenging moments. You showed me Your grace and I have indeed experienced Your faithfulness. Professor Manoj Maharaj, I extend my heartfelt appreciation for your patience, guidance, and encouragement throughout my time as your student. It is both a privilege and honour to have been supervised by one of the greatest names in the academic domain. I would also like to thank Dr. N. Ajayi for all forms of assistance that he has assisted me with, especially during the early stages of this research journey. I would also like to express my thanks to Miss Debbie for her consistency in ensuring that all the admin aspects of the study are intact.

Most importantly, my mother, Nomsombuluko Ngwane, your unconditional support in all spheres of life has allowed me to be an exemplary to the "Ngwane" generations to come. I would also like to extend my sincerest gratitude to my daughter Zanokuhle, the long phone call conversations helped me to cheer up throughout the study. To my brother Jabulani Ngwane, thank you for always being my confidant.

A big thank you goes out to all my academic companions. To my dearest research friend, Temitayo Faloye, thank you for the persistent push and assistance. Bahige Ndamuso, we have been in this together from day one. Last, but not least, Victor Faniran, thank you for your willingness to assist whenever I needed a helping hand.

ABSTRACT

Online-based attacks have become prevalent and continue to be on the rise as technology advances. The complexity of the internet has posed a cybersecurity concern across various online channels. As a result, online social engineering has become an important information aspect of security in the usage of the internet. Young adults, mainly students, who have the necessary social engineering knowledge to protect their personally identifiable information (PII) are less likely to fall victim. Therefore, social engineering awareness is seen as an important defense mechanism that enables students to protect their PII. Due to the lack of social engineering awareness initiatives conducted in higher academic institutions, social engineers succeed in luring students.

This study applied the quantitative research approach through distributing 379 questionnaires to both female and male students. The questionnaire tested both male and female students on their social engineering knowledge, information security attitudes, social engineering perceptions and online behaviour. The results of this study showed that there is a gender difference in online behaviour in reacting to online social engineering. The male students' responses revealed that they have more social engineering knowledge compared to their female counterparts. The findings also provided an indication of the online behaviours that potentially increase the students' susceptibility. The findings validate the need for social engineering awareness initiatives that address students on how to improve their online social engineering identification and information security. The study concludes by recommending attainable solutions to increasing the awareness levels of social engineering knowledge.

TABLE OF CONTENTS

DECLARATION i
ACKNOWLEDGEMENTS ii
ABSTRACT iii
TABLE OF CONTENTS iv
LIST OF TABLES viii
LIST OF FIGURES x
LIST OF ABBREVIATIONS xi
CHAPTER 1: INTRODUCTION 1
1.1 Introduction 1
1.2 Background of the study 4
1.3 Research problem 4
1.4 Research questions 5
1.5 Research objectives 6
1.6 Significance of the study 6
1.7 Justification 6
1.8 Theoretical framework 6
1.8.1 Gender and International Security, Feminist Theory 7
1.8.2 Theory of Reasoned Action 8
1.9 Limitations of the study 10
1.10 Outline of the Dissertation 10
1.11 Conclusion 11
CHAPTER 2: LITERATURE REVIEW 12
2.1 Introduction 12
2.2.1 Phishing attacks 15
2.2.2 Identity theft 17
2.2.3 Online scams 19
2.2.4 Social engineering compliance mechanism 19
2.3 Information security principles 20
2.3.1 Confidentiality 23
2.3.2 Integrity 24
2.3.3 Availability 24
2.4 Gender 25
2.5 Online social engineering is human-dependent 28

2.6 Young adults 29
2.7 Conclusion 31
CHAPTER 3: RESEARCH METHODOLOGY 32
3.1 Introduction 32
3.2 Research Objectives 32
3.3 Research design 32
3.3.1 Research Structure 32
3.3.2 Nature of the study 33
3.3.3 Exploratory research design 34
3.3.4 Questionnaire design 35
3.4 Research approaches 36
3.4.1 Qualitative 36
3.4.2 Quantitative 37
3.5 Sampling 37
3.5.1 Sample design 37
3.5.2 Sample size 37
3.5.3 Sampling techniques 38
3.6 Study site 39
3.7 Target population 40
3.8 Data analysis 40
3.8.1 Reliability and validity 40
3.8.1.1 Reliability 40
3.8.1.2 Validity 41
3.9 Theoretical frameworks 41
3.9.1 The Gender and International Security Feminist framework 42
3.9.2 Theory of Reasoned Action 42
3.10 Ethical considerations 43
3.11 Summary of Chapter 3 44
CHAPTER 4: FINDINGS AND ANALYSIS 45
4.1 Introduction 45
4.2 Response rate 45
4.3 Consistency and reliability 45
4.4 Normality test 46
4.5 Descriptive statistics 46
4.5.1 Gender 46

4.5.2 Respondents' ages 47
4.5.3 Respondents' racial classification 47
4.5.4 Tertiary institution of respondents 48
4.5.5 Faculty 48
4.5.6 Awareness 49
4.6 Constructs used in this study 52
4.6.1 Attitude 52
4.6.2 Subjective norm 52
4.6.3 Behavioural intention 53
4.6.4 Behaviour 53
4.7 Cross-tabulations 53
4.7.1 Cross-tabulation between gender and phishing attack awareness 54
4.7.2 Cross-tabulation between gender and identity theft awareness 54
4.7.3 Cross-tabulation between gender and cyber-crime awareness 55
4.7.4 Cross-tabulation between gender and email spam awareness 56
4.7.5 Cross-tabulation between gender and malware awareness 57
4.7.6 Cross-tabulation between gender and receiving and responding to an email message 58
4.7.7 Cross-tabulation between gender and receiving and responding to an online link 59
4.7.8 Cross-tabulation between gender and receiving and responding to an online pop-up message 60
4.7.9 Cross-tabulation between gender and receiving and responding to a social media message 62
4.7.10 Cross-tabulation between gender and online security perceptions 63
4.7.11 Cross-tabulation between gender and information security-related principles 67
4.7.12 Cross-tabulations between gender and responding to a random email message 72
4.7.13 Cross-tabulations between gender and responding to an email from someone close 75
4.7.14 Cross-tabulation between gender and responding to a direct message on social media 78
4.7.15 Cross-tabulation between faculty and phishing awareness 81
4.7.16 Cross-tabulation between gender, ethnicity and online security concern 82
4.8 Summary of gender-dependent results 83
4.8.1 Awareness: 83
4.8.2 Receiving and responding to random SE messages 83
4.8.3 Online security perceptions 83

4.8.4 Information security-related principles 83
4.8.5 Responding to random email messages 83
4.8.6 Responding to random email messages from someone close 83
4.8.7 Responding to a social media direct message 83
4.9 Conclusion 84
CHAPTER 5: DISCUSSION OF RESULTS 85
5.1 Introduction 85
5.2 Alignment of the findings with the research objectives 85
5.3 Answering research objectives 85
5.3.1 Research Objective 1: 85
5.3.2 Research Objective 2: 87
5.3.3 Research Objective 3: 90
5.4 Adaptation of the Gender and International Security, Feminist Theory to the study 97
5.5 Adaptation of the Theory of Reasoned Action (TRA) to the study 98
5.6 Conclusion 99
CHAPTER 6: CONCLUSION 101
6.1 Introduction 101
6.2 Summary of the study 101
6.3 Conclusion of the study 102
6.4 Recommendations 104
6.5 Suggestions for future research 105
REFERENCES 107
APPENDICES 118
APPENDIX A: ETHICAL CLEARANCE 118
APPENDIX B: NEW ETHICAL CLEARANCE 119
APPENDIX C: QUESTIONNAIRE 120
APPENDIX D: RELIABILITY TEST 125
APPENDIX E: NORMALITY TESTS 129
APPENDIX F: DESCRIPTIVE STATISTICS 134
APPENDIX G: CROSS TABULATIONS AND CHI-SQUARE TESTS 137
APPENDIX H: LANGUAGE EDITTING CERTIFICATE 149

LIST OF TABLES

Table 4. 1: Reliability test results 46
Table 4. 2: Cross-tabulation between gender and phishing attack awareness 54
Table 4. 3: Cross-tabulation between gender and identity theft awareness 55
Table 4. 4: Cross-tabulation between gender and cyber-crime awareness 56
Table 4. 5: Cross-tabulation between gender and email spam awareness 57
Table 4.6: Cross-tabulation between gender and malware awareness 57
Table 4. 7: Cross-tabulation between gender and receiving an email message 59
Table 4. 8: Cross-tabulation between gender and responding to an email message 59
Table 4. 9: Cross-tabulation between gender and receiving an online link 60
Table 4. 10: Cross-tabulation between gender and responding to an online link 60
Table 4. 11: Cross-tabulation between gender and receiving an online pop-up message 61
Table 4. 12: Cross-tabulation between gender and responding to an online pop-up message 61
Table 4. 13: Cross-tabulation between gender and receiving a social media message 62
Table 4. 14: Cross-tabulation between gender and responding to a social media message 63
Table 4. 15: Cross-tabulation between gender and online security 64
Table 4. 16: Cross-tabulation between gender and necessity for online security 64
Table 4. 17: Cross-tabulation between gender and user control of online security 65
Table 4. 18: Cross-tabulation between gender and online security concern 65
Table 4. 19: Cross-tabulation between gender and online security concern when responding to an unknown source 66
Table 4. 20: Cross-tabulation between gender and online security concern when responding to a friend 67
Table 4. 21: Cross-tabulation between gender and perceptions of the importance of online privacy 68
Table 4. 22: Cross-tabulation between gender and online security concern 70
Table 4. 23: Cross-tabulation between gender and change of privacy settings on social network sites 71
Table 4. 24: Cross-tabulation between gender and online security learning 72
Table 4. 25: Cross-tabulation between gender and verifying the sender of a random email message 73
Table 4. 26: Cross-tabulation between gender and responding without verifying the sender of a random email message 74
Table 4. 27: Cross-tabulation between gender and responding after verifying the sender of a random email message 75
Table 4. 28: Cross-tabulation between gender and responding after verifying the sender of a random email message when something will be won 75
Table 4. 29: Cross-tabulation between gender and verifying if it is someone close 76
Table 4. 30: Cross-tabulation between gender and response without verifying that it is someone close 77
Table 4. 31: Cross-tabulation between gender and response after verifying if it is someone close 78
Table 4. 32: Cross-tabulation between gender and verifying the social media message sender 79
Table 4. 33: Cross-tabulation between gender and responding without verifying the social network sender 80

Table 4. 34: Cross-tabulation between gender and response after verifying the social network message sender when something will be won 81
Table 4. 35: Cross-tabulation between faculty and phishing awareness 82

LIST OF FIGURES

Fig. 1.1: Ontological model of a SE attack (Mouton, Malan, Leenen, & Venter, 2014, p. 2)...2
Fig. 1.2: The TRA model (Montano & Kasprzyk, 2015) 9
Fig. 2.1: CIA Triad (Mohanty, Ganguly, & Pattnaik, 2018) 23
Fig. 4. 1: Gender representation of respondents 47
Fig. 4. 2: Age range of respondents 47
Fig. 4. 3: Ethnicity of the respondents 48
Fig. 4. 4: Respondents' respective institutions 48
Fig. 4. 5: Faculty grouping of respondents 49
Fig. 4.6: Respondents' online attack awareness 51

LIST OF ABBREVIATIONS

CIA - Confidentiality, Integrity and Availability

ICT - Information and Communication Technology

IR - International Relations

OSE - Online Social Engineering

PII - Personally Identifiable Information

PMB - Pietermaritzburg

SPSS - Statistical Package for Social Sciences

STEM - Science, Technology, Engineering and Mathematics

TRA - Theory of Reasoned Action

UKZN - University of KwaZulu-Natal

SE - Social Engineering

SEA - Social Engineering Attacks

CHAPTER 1: INTRODUCTION

1.1 Introduction

The internet has grown rapidly, and has brought about changes in the ways in which people interact, browse for information, shop, and the way in which they spend their time (Curran, Fenton, & Freedman, 2016; Musingafi, Mapuranga, Chiwanza, & Zebron, 2015). Almost two thirds of adults participate on social network sites, as compared to 2005 where only 7% of adults were active users (Perrin, 2015). The internet's size, complexity and increasing number of connected devices has brought about the need for security for data storage and communication purposes (Cabaj, Grochowski, & Gawkowski, 2015). The frequent cyberattack events that currently occur on the internet are symbolic of the security weaknesses in the growing internet. Information security therefore becomes a challenge, since cloud technologies have introduced virtual connections of wireless networks subjecting online sites to greater cybersecurity vulnerabilities.

Technology is an essential aspect of modern society. The 'internet of things' (Cabaj et al., 2015) makes it possible for objects in our physical world to connect with the virtual world, allowing the objects to share information with members of that particular network, usually through the use of the same internet protocol (Halevi, Lewis, & Memon, 2013) connecting the internet (Drucker, 2015). The internet provides online social networking and social media platforms which create stimulating environments for internet users, enabling real time communication, socialisation and entrepreneurial activities. However, within the population of all internet users are malicious users, including social engineers, who exploit all possible vulnerabilities. Social engineering (SE), in the context of information security, is a term used when internet users are deceived and misled by attackers into exposing valuable personal and corporate information (Algarni, Xu, & Chan, 2016). Such information is then used by the attackers to perform fraudulent activities. As shown in Figure 1.1, SE occurs in various forms.

Fig. 1.1 is explained as follows, in an anti-clockwise direction:

There are two communication entry points that a SE attack may exploit: direct and indirect communication. Direct communication refers to instances when the social engineer directly communicates with the potential victim. For example, vishing attacks occur when the attacker converses with the targeted victim over the telephone. Indirect communication implies the use

of a communication medium, where the social engineer does not interact with the attacker. For instance, the potential victim logs into a web page that is created by a social engineer.

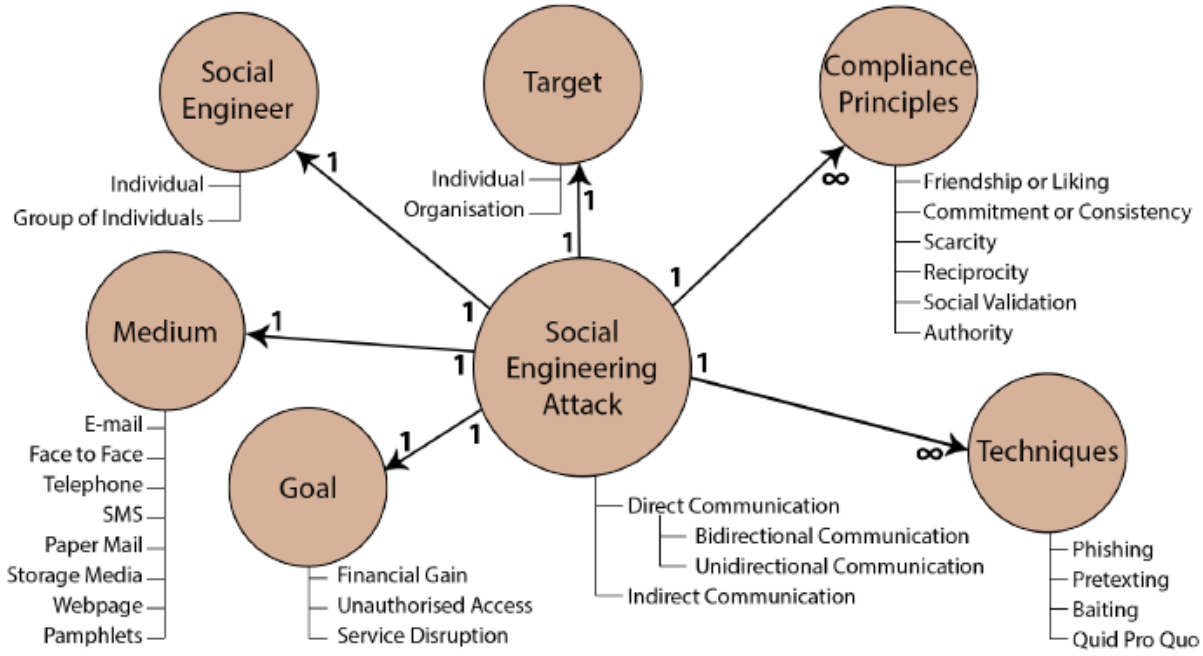

Fig. 1.1: Ontological model of a SE attack (Mouton, Malan, Leenen, & Venter, 2014, p. 2)

Techniques: The diagram illustrates how social engineering has multiple techniques that can be used for a single attack. For instance, a phishing technique message may consist of a baiting technique in order to lure individuals. Therefore, the communication method used would be dependent on the technique that the social engineer uses.

Compliance principles: For the target to comply, the social engineer uses social engineering principles to make the individual trust that the act is harmless. The compliance principles are mechanisms that assist in getting the victim's trust. As illustrated in Fig.1.1, a social engineering attack may use more than one compliance principle to bait the target. For instance, the attacker may use authority and liking principles. The social engineer may act as the target's manager with whom the target has a favourable relationship, friendship.

Target: A planned social engineering attack can have only one target. The target can either be an individual or an organisation. For instance, a phishing attack can be directed to the victim, in order to get the victim's personal details. On the other hand, the phishing attack can be directed to an individual in an organisation in order to get unauthorised access into the organisation's network.

Social engineer: An attack is constructed by a group of individuals or by an individual social engineer.

Medium: There are several mediums that a single attack can use. However, one social engineering attack can only use one medium. The medium is dependent on the technique used. For instance, if the social engineer uses the phishing technique, the e-mail medium is the most appropriate medium to use in order to achieve the intended objective.

Goal: The entire purpose of one social engineering attack is for one benefit. This means that the attack is conducted to either gain unauthorised access, to cause service disruption, or for a financial gain. The communication, techniques, compliance principles, target, social engineer and medium are all chosen to achieve the intended goal.

As illustrated in Figure 1.1, SE is a process whereby the attacker initialises communication with the potential victim in order to achieve the set objective. Prior to committing the attack, the social engineer would have gathered enough relevant information about the targeted individual or organisation (Bezuidenhout, Mouton, & Venter, 2010). The social engineer would then decide on the best technique to use to reach out to the target. A target is more willing to comply with the attacker's message, based on the compliance principle with which the attacker has chosen to lure the individual (Mouton, Leenen, & Venter, 2016). However, the attacker would also disguise him/herself as someone whom the individual knows, for example an authoritative figure or a friend. Amongst the various SE attack techniques, phishing and baiting are the most common forms to lure victims (Tetri & Vuorinen, 2013). The difference between the two is that phishing is mainly used for exploiting the targeted individual's trust in order to get the individual's private information (Dakpa & Augustine, 2017). On the other hand, baiting is based on the greed of the targeted individuals, and the individuals would be required to carry out certain tasks in the belief that they would be rewarded, financially or otherwise (Fan, Lwakatare, & Rong, 2017). The attacker can then decide which medium to use, which would then lead to the actual online attack in which the target either succumbs, or does not.

Social engineering research and awareness are both critical in reducing the success rate of SE attacks, as well as neutralising the attackers (Hassan, 2019). According to Aldawood and Skinner (2018), there is a lack of knowledge on the differing gender response rates to the social engineering threats that are prevalent on online sites. This research investigates whether there is a difference in the way in which males and females respond to social engineering.

Nowadays, it has become almost impossible to achieve an information security level using only technological countermeasures, since modern cyberattacks have the capabilities to bypass all the defense layers. Therefore, education programmes improving user awareness of social engineering threats are important. The importance of awareness and education about social engineering attacks cannot be emphasised enough, considering the likelihood of every individual becoming a victim (Junger, Montoya, & Overink, 2017). Moreover, educating individuals can minimise the number of successful attacks (Krombholz, Hobel, Huber, & Weippl, 2015).

1.2 Background of the study

Online social media users are often active on multiple platforms. This allows social engineers to attack users through increasingly complex methods utilising emerging technologies and multiple attack vectors (Al-Jabri, Sohail, & Ndubisi, 2015). South African users are not immune to these attacks (Harrison, 2013). Regardless of the implementation of security settings on online platforms, users fall victim to online social engineering (OSE) due to insufficient information security and social engineering knowledge (Hinson, 2008). In recent years, studies have shown that students fall victim to various forms of online social engineering due to inadequate control of their online behaviour. However, there have also been apparent gender differences in online behavioural patterns (Malandrino, Petta, Scarano, Serra, Spinelli, & Krishnamurthy, 2013). This suggests that there may also be a gender difference with regards to information security awareness and response. In this study, the researcher investigated whether there is a different gender response to online social engineering using a sample of 379 Pietermaritzburg (PMB) students from Umgungundlovu FET College and the University of KwaZulu-Natal.

1.3 Research problem

Users are vulnerable to social engineering attacks (Mouton et al., 2016) and are the weakest link in any cybersecurity regimen. Although previous studies have been conducted to understand human behaviour, there have been no information systems created to determine human decision-making processes (Noureddine, Keefe, Sanders, & Bashir, 2015). It is only recently that researchers have started to consider conducting research that examines the factors that cause humans to respond to online social engineering attacks. The recent human studies

have been conducted to assist with generating possible social engineering defense mechanisms (Halevi et al., 2013).

Gender is perceived to be embedded with numerous characteristics based on an individual's cultural beliefs (Hudson, 2005). Generally, males are considered more dominant than females (Kachel, Steffens, & Niedlich, 2016). This is due to them being considered as the heads of their households (Wolf, 2000). Therefore, they are usually tasked with security matters, both in the workplace and in their households. Among young adults, gender inequalities, as inherited from previous generations, are still in existence. Technology alone, as seen on the internet, is somehow gendered like the traditional household hierarchies, where males are dominant. Transferring that mindset onto the internet, males tend to be more self-confident in their computer skills; as they would be when facing security tasks in the real world (Zhang, Tran, Hinh, Nguyen, Tho, Latkin, & Ho, 2017). Females are more submissive, even in online domains, as they would be in households due to the cultural hierarchy structure (Bashir, Mahmood, & Shafique, 2016). In a study conducted by Helsper (2010), it was evident that internet usage by all individuals is affected by factors that exist in the physical world. Therefore, an understanding of gender differences in responses to OSE attacks will enable future researchers to better design security interventions in cybersecurity.

Security issues pertaining to online social networks have been extensively studied (Liben-Nowell & Kleinberg, 2007), but the role of gender in the success of OSE attacks amongst young adults in South Africa requires further investigation. This leads to the following key questions to be answered by this research.

1.4 Research questions

The study's research questions are as follows:

Primary Research Question

To what extent is there a gender-dependent response to online social engineering attacks amongst young South African adults?

Research Sub-Questions

1. How aware are young South African adults of online social engineering?

    a. Do the genders have different awareness levels of the different types of online social engineering attacks?
2. What is the attitude of young adults in South Africa to online social engineering?
    a. To what extent is a gender difference apparent?
3. To what extent are young adults' responses to online social engineering adequate to protect them?

1.5 Research objectives

1. to determine whether there is a gender difference in the response of tertiary students to online social engineering;
2. to identify students' knowledge about online social engineering from a gender perspective;
3. to determine if there is a gender difference in online information security among young adult students.

1.6 Significance of the study

There has been no previous research that has investigated the difference in responses to OSE attacks amongst the South African youth from a gender perspective. Therefore, it is important to better understand the different gender responses of young adults to existing OSE attacks. If gender differences are apparent, preventative measures can be appropriately designed.

1.7 Justification

Literature has shown that young adults are heavy users of online social networks. It is important to understand this usage from all perspectives. Gender is one such perspective. This study provides a foundation for researchers who wish to expand upon the ideas explored here in broader contexts. The outcomes of this study may also be of interest to researchers in gender studies.

1.8 Theoretical framework

This research implemented two theoretical frameworks to direct the study in distinguishing the gender responses to online social engineering. The adopted frameworks are Gender and International Security, Feminist Theory and the Theory of Reasoned Action. The following section discusses these theories and highlights their significance in relation to this research.

1.8.1 Gender and International Security, Feminist Theory

This theory was first formulated in 1988 as the Women and International Relations Theory and was later recognised to be the beginning of the feminist methods in international relations (IR) research programmes (Sjoberg, 2009). Discussions involving IR scholars, feminist theorists and others expanded to include the security aspects of online platforms (Wibben, 2010). The discussions do not only show women's importance in international security, but also the significance of gender as a fundamental factor in attaining comprehensive knowledge and addressing security issues.

The Gender and International Security, Feminist Theory argues that gender is not a section of security studies (Sjoberg, 2009). It is argued that gender is theoretically vital in studying international security. It uses gender as the lens of the study. In agreement, Trauth (2013) stated that for gendered IS research, a gender theory is used as the lens to assist in the gathering and interpretation of the raw data. The primary objective would be to look at the study through gendered lenses, concentrating on gender as a way to understand universal processes (Sjoberg, 2009). Furthermore, in agreement, Trauth (2013) stated that having a gendered theory helps in giving the study a sense of direction in understanding the gender phenomenon. In this theory, gender is described as a system that creates social hierarchies associated with the attributes of femininity and masculinity (Tickner, 1992).

Gendered social hierarchies are considered as a social construction since gender is expressed differently across cultures, organisations, languages and individuals. Therefore, feminism is considered to be not just about women, but mainly about changing means of existence (Sjoberg, 2009). Tickner (1992) argued in the same vein, affirming that the term 'gender' does not only refer to the biological aspect of male and female, but rather the established differences between the sexes. Moreover, gender cannot be measured as a male or female question, but rather as a complex symbolic construction. Researchers that look through gender lenses mainly ask about the assumptions associated with gender in order to make meaningfully precise statements (Sjoberg, 2009). Feminist theorists have noted that gender is significant in what we research. Furthermore, feminist theorists' contributions in security studies have been explored and analysed to draw attention to new or disregarded subjects by seriously taking gender into consideration (Kennedy & Dingli, 2018; Sjoberg, 2009). The first subject matter of the feminist theory is to broadly consider and understand what is measured as a security subject. The theory's second theme is to recognise the gendered nature in the domain of international

studies. It is believed that gender adds different contexts into security studies, in as much as gender is an external force in security scholarship and the framework of security generally (Sjoberg, 2009). If security is to be re-envisioned from an individual female's perspective, then it would alter what security is known to be, and how security is conceptualised, acted on and operationalised. According to Blanchard (2003), the term security has been interpreted in contradictory ways, and it is only in recent years that gender has been considered in the information security discipline.

In societies, gender is a salient social category, which is seen as a fundamental source of human diversity (Bussey & Bandura, 1999; Maccoby, 1998). In the same vein, Spence and Helmreich (1980) stated that universally, gender roles differ across human societies. The ubiquitous social reputation that gender has adopted (Bussey & Bandura, 1999) serves as the reasoning for adopting feminist theory in understanding the gender aspect of the study. However, this study is an IS study that incorporates the gender element. Therefore, the gender lenses will be used in this research to touch on attitude and subjective norms, found in the Theory of Reasoned Action (TRA) theory, since attitude is considered a way of thinking learned from an individual's early childhood (Maccoby, 1998). The TRA mainly focuses on individual aspects (Ajzen & Fishbein, 1980) rather than human societies, since the researcher used the feminist theory in determining two of the four TRA constructs. Also, masculinity and femininity are at the heart of a culture's value system and cultural teaching, because an individual's normative belief acts as a guideline to taking any particular action, due to the adopted parent-child behavioural patterns (Spence & Helmreich, 1980).

1.8.2 Theory of Reasoned Action

The Theory of Reasoned Action TRA (Ajzen & Fishbein, 1980) lies within the discipline of information studies. The first adopted theory, Gender and International Security, Feminist Theory only covers the gender aspect of security in general. Fishbein first introduced the TRA in 1967 and it was then developed, after failing repeatedly to predict behaviour from outdated measures of attitude (Ajzen & Fishbein, 1980). The main assumption of the TRA is the belief that an individual reasons in a particular manner due to the individual's acquired knowledge. Individuals assess the state of a situation and thereafter decide whether or not to perform in a certain way, based on their perspective (Ajzen, 1985). Therefore, the most immediate behavioural determinant is behavioural intention.

The TRA focuses on understanding an individual's underlying reasons for acting in a particular way (Glanz, Rimer, & Viswanath, 2015). Arguing in the same vein, Montano and Kasprzyk (2015) claim that the TRA clearly identifies relationships that exist within the framework's constructs, namely attitude, beliefs and behaviour. Furthermore, the TRA is based primarily on the concept of an individual's overall behaviour, which is determined by the individual's intention to behave in a particular way. Additionally, the model proposes that the main reason an individual behaves in a particular way is solely determined by the individual's intention (Cooke, Dahdah, Norman, & French, 2016).

In this study, the TRA was used to determine the individual's intention, attitude and behaviour and the motive behind their response towards the online threats, through a gender lens.

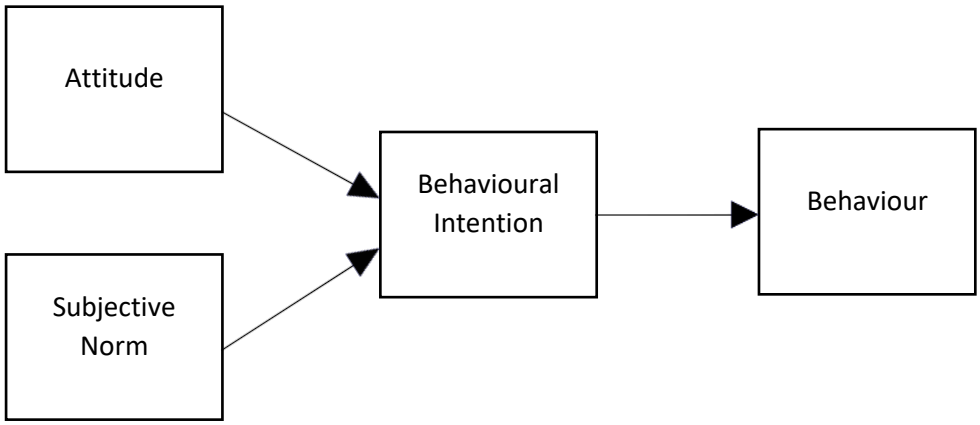

Fig. 1.2: The TRA model (Montano & Kasprzyk, 2015)

Attitude: According to Cooke et al. (2016), attitudes are an individual's perception of behaviour. In this study, this construct was aligned with determining the positive or negative evaluations that young adults have about online social engineering. Literature on social psychology has recognised attitude as a major factor that predicts an individual's behaviour (Mostafa, 2007). The behavioural intention of an individual is considered as a factor that gives an explanation to the individual's conducted behaviour. According to Chang (2013), attitude is explained to be a general feeling of approval or disapproval of a particular behaviour.

Subjective Norm: Normative beliefs are external factors and include individual normative beliefs, such as approval or disapproval from referent individuals, along with the individual's motivation to comply with the given instruction (Montano & Kasprzyk, 2015). In the context

of this study, subjective norms were determined by evaluating whether the individual responds to online social engineering messages if instructed to do so by a known party.

Behavioural Intention: In a definition given by Calisir, Gumussoy, Bayraktaroglu, and Karaali (2014), behavioural intention is an individual's intuition as to whether or not they want to perform a particular task. In addition, motivational factors are captured in an individual's intention. Therefore, this study seeks to discover the motivational factors that lead to the participants' responses to SE.

Behaviour: What drives the individual's decision to act (Montano & Kasprzyk, 2015)? In the context of this study, the factors that lure the individual to respond to online social engineering messages were determined.

1.9 Limitations of the study

This study was carried out in one geographical location, Pietermaritzburg. Thus, care should be taken if the results are generalised to the whole of South Africa. Additionally, the sample consisted only of higher education students, which may not be representative of young adults in general.

1.10 Outline of the Dissertation

This study consists of six chapters which are arranged as follows:

Chapter 1 provides an overview of the dissertation. The chapter presents a discussion of online social engineering and the form of attacks associated with it. Furthermore, the chapter explains the significance of the study and the research questions that were asked. The chapter also presents the two frameworks that were adopted and used to guide this study.

Chapter 2 presents a review of the literature that has been conducted on social engineering. The chapter introduces various forms of social engineering, the information security triad, gender and the vulnerability of young adult students.

Chapter 3 discusses the adopted methodology. The chapter explains the research design and approach implemented. It also provides explanations on the sampling and survey method used.

Chapter 4 presents the findings, data analysis and interpretations of the collected data.

Chapter 5 provides a detailed discussion of the research findings in relation to the research objectives.

Chapter 6 concludes the study and provides recommendations for future research.

1.11 Conclusion

This chapter introduced the study and presented a high-level overview. The research problem was introduced, and the research questions and objectives presented. Furthermore, the two theories guiding this study were discussed. The next chapter presents the literature review underpinning this study.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The internet has grown rapidly and has brought about changes in the way individuals interact, browse for information and shop; and the way in which they spend their time (Curran et al., 2016; Musingafi et al., 2015). Almost two thirds of adults use social network sites today, as compared to 2005 when only 7% of adults were active users (Coyne, Padilla-Walker, Holmgren, & Stockdale, 2019). The internet's size and complexity has increased the need for security for data storage and for communication purposes (Cabaj et al., 2015). The frequent cyberattacks are symptomatic of the prevalent security weaknesses inherent in the structure of the internet. In a recent study, it was discovered that cyberattacks have targeted 131 universities in 16 countries (CreamerMedia, 2018). South African universities are amongst the most targeted, and attackers have tried to obtain staff and students' credentials.

There is no fully secure online environment. Cyberattacks bypass technological defense layers such as antiviruses and firewalls (Sharma, 2012) and also use humans as their entry point to achieve security breaches. Therefore, humans need to be involved in security defense strategies The importance of awareness and education about social engineering attacks cannot be emphasised enough, due to the likelihood of every individual becoming a victim (Junger et al., 2017). Moreover, educating users can minimize the number of successful attacks, as individuals would then be aware of the necessary precautions that they need to take (Krombholz et al., 2015).

This chapter presents a review of the literature on social engineering, information security principles, gender, and social engineering (SE). In the social engineering section, the literature reviews social engineering and the most prevalent types of social engineering. The social engineering section also presents the compliance mechanism that attackers use as a technique to convince the victims to innocently comply with a social engineering attack. Information security principles are included in the literature, to understand how social engineering breaches these security principles. The section also references how online platforms are trying to ensure that they uphold basic security principles. Furthermore, the literature provides an outline of the different views of gender and the prevalent gender differences known to society as a result of the traditional gender norms. The chapter ends by presenting literature on young adults and the reasoning behind why young adults are the primary target group for social engineers.

2.2 Social engineering

Social engineering is defined as the art of deceiving an individual into giving out his personal information. Similarly, Algarni, Xu, Chan, and Tian (2014) explain social engineering as the persuasion of an unsuspecting user into conducting a certain action that breaches security principles. These actions are interpreted as deception, conducted by the attacker, in acquiring the needed information (Krombholz et al., 2015). The attackers seek information such as a password from an individual instead of breaking into a system. To achieve this, the attacker employs different forms of social interaction to obtain information about the potential victim. In online social engineering, the targeted victim does not distinguish between a genuine message and a deceptive message of the social engineer.

In research conducted by Bullée, Montoya, Pieters, Junger, and Hartel (2015), the six principles of persuasion were explained. These researchers explained that attackers use persuasive mechanisms to increase their success rate, namely, conformity, partial liking, reciprocity and assurance. Essentially, these four principles are used to influence an individual to comply, in the full belief that what they are complying with is harmless and legitimate. In a more recent study conducted by Fan et al. (2017), social engineering was further described as the disclosure of personal information to a malicious actor. In relation to information security, social engineering is also defined as misleading an individual into disclosing sensitive information, by exploiting the individual's cognitive and unsuspecting thinking.

In the same vein, Greitzer, Strozer, Cohen, Moore, Mundie, and Cowley (2014) explained how persuasion occurs through means of electronic communication. They explained that the objective of persuasion is to make the user act in a manner that will jeopardise their personally identifiable information (PII). In order for social engineering to succeed, it requires certain mechanisms that help the attacker gain the required information, which are usually based on the attacking technique that will be applied. In most reported cases of social engineering, the common attack methods used are malicious online messages, links and pop-up messages (Wüest, 2010). Accordingly, the attacker uses social engineering as a tool to get the necessary information, regardless of the security defense tools.

Nowadays, the evolution in technology has provisioned criminals with online platforms such as the Dark Web, which is explained as an online market place where social engineers purchase

stolen credentials and malicious malware (Chertoff & Simon, 2015). Traditionally, scammers travelled to deceive consumers with get-rich-quick schemes and miraculous cures. Ever since the emergence of the internet, social engineering has radically evolved in complexity. Ivaturi and Janczewski (2011) affirmed that social engineering attacks can be deemed older than the internet, since there is no difference in the types of offenses committed, but rather in the complexity in the way that the attacks are committed. The difference is that for online attacks, the victim and the attacker have no physical encounter (Okesola, Onashoga, & Ogunbanwo, 2016). The attacker lures the user over the diversified online platforms such as emails, social media and online shopping sites.

The attacker or social engineer plays a crucial role in a social engineering attack. He is regarded as the regulator of an online social engineering attack because he controls the attacking process (Algarni, Xu, Chan, & Tian, 2013). The strategy used by the attackers consists of an attack system which starts from understanding the potential victim and ends with either a financial or information gain. As part of the starting phase, the social engineer tries to determine ways in which he can gain the targeted victim's trust. Thus, the social engineer works towards identifying the online behavioural patterns of the targeted user in order to find exploitable vulnerabilities. In most instances, online behavioural patterns are collected through social network posts and e-commerce sites, due to the amount of personally identifiable information users openly disclose (Tetri & Vuorinen, 2013). For instance, when a social engineer has gained information such as names of close friends of the targeted victim, the information becomes useful in determining ways to entice the victim through techniques such as 'identify theft' and 'impersonation'.

The plan of attack is based on the gathered information because the information is used to develop a plan that consists of a personalised strategy for each target. The social engineers ensure that the plan is believable so that the targeted individual has no suspicions of the conveyed message. Thereafter, the social engineers strategise on the suitable time to execute the attack, which is then followed by the actual attack (Algarni et al., 2014). In South Africa, the most common forms of attack consist of emails or direct messages which are sent to the victim without creating obvious errors that would raise suspicions (Wakama, 2014). However, victims are usually drawn to responding due to the level of attacking skills the social engineers use (Algarni et al., 2013). The reason for responding is because the social engineers present the message as if it comes from a known and reliable source. Therefore, it becomes challenging

for the victim to identify the non-credibility of the message, as compared to in a face-to-face interaction. In agreement, Kvedar, Nettis, and Fulton (2010) stated that, irrespective of an individual's knowledge about social engineering attacks, a well-executed attack has possibilities of being successful. This is due to the attacker's level of professionalism and skillsets (Dhamija, Tygar, & Hearst, 2006).

The internet allows the attackers to use various platforms to execute the attack (Krombholz et al., 2015). The most common form is an email message that requests an individual to conduct a certain task, such as clicking on an email link or providing certain details. This SE technique is amongst several other attacking approaches used to exploit discovered vulnerabilities (Kumar, Chaudhary, & Kumar, 2015). Also, the attacker uses different forms of communication and technological devices based on the nature of the attack (Mouton et al., 2016). The communication techniques are either direct or indirect. Direct communication is in the form of a verbal conversation such as a telephone call; whereas indirect communication is based on sending a message over the internet or via Short Messaging Service (SMS) (Chaudhry, Chaudhry, Rittenhouse, 2016). Given the different types of communication channels used by social engineers, the most frequent forms of social engineering attacks are identified hereunder.

2.2.1 Phishing attacks

Phishing is defined by Huang, Ma, and Chen (2011) as a SE technique that uses an indirect form of communication to obtain an individual's sensitive information. In another definition given by Garera, Provos, Chew, and Rubin (2007), phishing is described as a form of identity theft. In the context of phishing attacks, the phisher who is the social engineer, seeks personal information from users through indirect communication. In most instances, the phisher seeks information such as PII or banking details. This is generally achieved through distributing an email message to a pool of internet users. In a sample of more than 13 million emails, an estimated 12 percent of the emails contain malicious content (Alazab & Broadhurst, 2016). The modern phishing email messages contain instructions that guide the potential victim to click on certain links provided on the email (Downs, Holbrook, & Cranor, 2006). In South Africa, university students frequently receive phishing emails that consist of fake links that lead to spoofed web pages (Broadhurst, Skinner, Sifniotis, Matamoros-Macias, & Ipsen, 2019). This is because phishing hyperlinks are an easier technique to bait recipients of the phishing email messages. Phishing also allows the social engineers to target a large number of users. Also, due

to the sophistication of the phishing emails, the targeted victims have a desire to click on the hyperlinks. Other phishing emails consist of attachments that, when downloaded, run malicious software on the user's workstation. As stated by Butavicius, Parsons, Pattinson, and McCormac (2016), when a link redirects the user to a malicious website, it is regarded as a pharming attack. Typical phishing attacks consist of three key components (Chiew, Yong, & Tan, 2018) :

- **The bait** is an email message that appears to be from a trusted source, such as banks and universities. The message contains a malicious link that is provided by the fake URL.
- The **hook** is the mimicked website. The hook deceives the users into providing their confidential information, believing that the website is legitimate.
- The **catch** consists of the phisher using the collected information for illegal activities.

In 2013, it was estimated that six billion of the 183 billion emails sent out daily contain malicious attachments (Broadhurst, Grabosky, Alazab, & Chon, 2014). Hong (2012) emphasised that phishing attacks have been on the rise and have become the most occurring online threat. This online risk is associated with the lack of safety of internet users' personal and confidential information. In 2014, SA was declared to be the second most phishing-targeted country, from a global context (Wakama, 2014). Also, according to the South African Banking Risk Information Centre (SABRIC), SA citizens lose an estimated R2.2 billion as a result of cyberattacks (BusinessMediaMAGS, 2018). This shows that the phishing phenomenon definitely exists in SA, making every South African individual a possible victim. Kennedy and Dingli (2018) advance that to lessen the number of successful phishing attacks, awareness programmes need to be considered. It is believed that the success of the phishing attacks rely on the level of knowledge the user holds (Florencio & Herley, 2010). Jakobsson and Myers (2006) explained that in phishing attacks, the victim assists the attacker innocently by providing the information the attacker needs; whereas, identifying a phishing email or site can be effortless for a user who is knowledgeable about phishing attacks (Aleroud & Zhou, 2017). Therefore, individuals who have no social engineering knowledge end up falling victim. This leads to an increased success rate for phishing attacks – hence, the high number of successful phishing attacks reported by SABRIC. It has been a concern that, to date, only a few studies have been conducted to measure the vulnerability levels of users to phishing attacks (Algarni et al., 2014).

Phishing attacks are classified into several different forms. The attackers adopt the most appropriate technique that is suitable for a potential victim's environment. The different forms of phishing attack are as follows:

- **Clone phishing**

An attacker uses this type of phishing attack by using previously distributed legitimate email messages (Chiew et al., 2018). The genuine email is replicated and malicious links or attachments are embedded into it and then it is resent (Nagarjuna & Sujatha, 2013). The email will appear genuine, yet it is sent from a spoofed email address (Ma, 2013). Spoofing an email gives the impression that it is a resend or an upgrade from the original known source. The malicious attachments contain spyware and screen grabbers which send the phisher information when the user inputs his sensitive information. Further research has discovered that email attachments and web browsers are the main malware vectors (Bakdash, Hutchinson, Zaroukian, Marusich, Thirumuruganathan, Sample, Hoffman, & Das, 2018). Therefore, users stand a high chance of falling victim due to the failure of identifying spoofed email addresses.

- **Spear phishing**

Another form of phishing attack is the spear phishing method. In this attack, the phisher targets a specific group of individuals, such as lecturers or third year students. The technique of targeting a specific group is to increase the success rate of the attack (Magdalin, 2015). In this technique, malicious emails are sent specifically to the targeted group.

- **Phone phishing**

Phone phishing is a type of phishing attack that is commonly referred to as vishing. As defined by Aburrous, Hossain, Dahal, and Thabtah (2010), vishing has posed a far smaller threat, compared to the other forms of online phishing. Similarly, vishing is further defined by Banu and Banu (2013) as the use of a phone to gain an individual's sensitive information. The attacker makes a phone call to individuals, asking individuals for their personal information (Ekawade, Mule, & Patkar, 2016). The attackers use hoaxed caller ID numbers which hide their actual numbers. Therefore, victims fall for the phone call, believing that the call is coming from a trusted source.

2.2.2 Identity theft

As defined by Ziegeldorf, Morchon, and Wehrle (2014), identity theft is an attack relating an individual with a personal identifier, such as his first name, pseudonym, and address. Identity theft occurs when an attacker obtains an individual's PII and uses it to conduct fraudulent

activities (Vieraitis, Copes, Powell, & Pike, 2015). These fraudulent activities are conducted using a false identity in order to gain the victim's trust. Hille, Walsh, and Cleveland (2015) stressed how identity theft is, rapidly becoming a global concern. The rise of identity theft has been predominant across online transactional sites and in email messages (Kahn & Liñares-Zegarra, 2016). In turn, this causes a major concern for e-commerce retailers and consumers since their PII is at risk of being stolen. This implies that online shops are at risk of losing purchasers, since customers are becoming hesitant in providing their PII on online sites, as well as conducting online transactions. Holtfreter, Reisig, Pratt, and Holtfreter (2015) identified that, in some instances, internet users put themselves at risk due to their risky behaviour, which creates entry points for attackers. Thus, when students fall victim to identity theft, it can be due to their online negligence or lack of identifying false identities. This is because risky online activities by users often lead to personal information leakage. Furthermore, Welsh (2015) emphasised that certain behaviour causes leakages that later cause greater problems. In addition, he explained that identity theft damages the victim's name and subsequently his reputation becomes discredited.

On a global scale, identity theft has cost organisations huge amounts of capital per year (Ibrahim, Ramanathan, Som, & Trevathan, 2016). The capital is either taken by hackers, or after the implementation of social engineering compliance training. In a study conducted by Song, Lew, Song, and Song (2018), it was apparent that once a social engineer has gained an individual's identity, committing fraudulent activities becomes effortless. Nowadays, individuals conduct various online transactions across various platforms such as online banking or mobile applications and, therefore, the scope of identity theft has increased (Ferrell, 2017). To decrease the number of users who fall victim to identity theft, McGlone, Ballard, Berkelaar, Baryshevtsev, and Brown (2015) advised that information campaigns should be conducted. In their study, the campaigns conducted revealed that few consumers were aware of the online crime of identity theft. According to Rebovich, Allen, and Platt (2015), attention needs to be paid to identity theft awareness initiatives that focus on ways that individuals can protect their online identities. The awareness programmes do not benefit individuals only, but also organisations that experience financial losses due to staff negligence. It is believed that awareness programmes covering identity theft would improve the user's ability to distinguish whether a site or email is credible. For instance, individuals would know to check the site's legitimacy before providing their card details or making any form of online transaction.

2.2.3 Online scams

Online scams are online acts that consist of fraudulent activities with the objective of financial gain. Tiwari (2018) stated that email scams are the most common form of social engineering attacks. This attack occurs when an attacker probes an individual via messages that are embedded with hyperlinks or malicious attachments. This form of attack may also include an alert message or a reward message that creates a sense of emergency for the individual to respond. The email link would seem as if it is coming from a legitimate source, yet it would be coming from an attacker who has recreated any reputable company's website. Email messages that stipulate that other users have taken up the offer or have conducted the specific act, lure the victim to also comply. Similarly, if it is stipulated that the offer is available for a short time period, potential victims are more likely to comply with the necessary instructions in the malicious email (Butavicius et al., 2016).

2.2.4 Social engineering compliance mechanism

This section provides an overview explaining why individuals become victims of social engineering. It has been identified that trust is the core compliance mechanism that is compromised by social engineers in order to obtain the necessary information from individuals (Mann, 2017).

- **The role of trust in social engineering attacks**

Thompson (2006) specified that the common form of manipulating an individual is by gaining his trust. In the same vein, Granger (2003) also noted that in information security, trust and validity are considered to be the weakest link in any security chain. This is caused by the natural willingness to accept a stranger's word which appears to be truthful; for example, a social engineer acting as a credible Gmail technician wanting to assist an end-user with privacy settings. In the message, the social engineer, impersonating the technician, would communicate that they require information from the end user. The user, appreciative of the assistance, complies willingly. As part of complying, the user gives the social engineer the necessary personal information that leads to a data breach. It is unfortunate that most attacks succeed due to the difficulty in easily identifying a non-credible source (Sattarova Feruza & Kim, 2007). Thus, by fostering feelings of gratitude, the social engineer takes advantage of the natural human tendency to trust. The response by Workman (2008) is a compliance mechanism that changes behaviour when a direct request is prompted, Hinson (2008). Also, as described by Luo, Brody, Seazzu, and Burd (2011) social engineers are compliance practitioners who lure

individuals to respond to their requests, namely, social proof, scarcity, and reciprocation. Social proof assists social engineers because individuals tend to adhere to the given instructions based on similarity and uncertainty. Scarcity encourages individuals to react to social engineers' messages because they think that the prize is a valuable commodity. Reciprocation allows social engineers to manipulate individuals by making them feel appreciated, and the individual feels obliged to the social engineer and complies due to this feeling of obligation.

Furthermore, Tetri and Vuorinen (2013) identified that once a social engineer gains a user's trust, it becomes easy to obtain all the required information. Impersonation therefore plays a huge role in gaining the victim's trust. Social engineers use impersonation to act as the victim's friend, a technician requiring credentials to fix a technical error, or a person of authority (Van Rensburg, 2017). Thereafter, the social engineer exploits the trusting relationship. However, the authority technique has been found to be the least effective impersonation technique used to gain a user's trust (Butavicius et al., 2016). Users are exploited due to innocently mistaking the credibility of a source that is unreliable, without any concrete verification (Algarni, Xu, & Chan, 2015). Also, they tend to use their intuition when validating a source's reliability. If the user has a positive instinct about the source, they perceive no threat in responding (Rebovich et al., 2015). This is thought to be the reason behind attackers' use of names or organisations that seem familiar, yet are bogus (Greitzer et al., 2014). In that way, victims are easily deceived into thinking that the source is credible. In an effort to prevent naive individuals from being victims to online attacks, educational awareness programmes are proposed (Derksen & Hilbrink, 2012). The programmes are to be guided by information security studies in relation to the prevalent online social engineering attacks, and are regarded as a platform to create awareness in individuals, with the objective of decreasing the number of successful attacks as individuals become more aware of the precautions that can be taken. It is also fundamental to understand the level of trust that causes individuals to comply so that personalised remediation methods can be implemented.

2.3 Information security principles

Information security entails keeping sensitive information confidential. The definition relates to any type of private or personal information that is considered sensitive to an individual or organisation (Da Silva, Da Silva, Melo, Rodrigues, Lucien, De Melo, Colares, & Garcia, 2014). In information security studies, privacy and data theft have been identified as the major concerns (Petkovic & Jonker, 2007; Vieraitis et al., 2015). This is due to the digital forms of

technology which make information accessible through various devices. The ability to access sensitive information over multiple devices makes protecting information challenging since attackers have various attacking options. For instance, attackers can access individuals' banking details either through a mobile banking application or on the bank's online banking site. This results in more vulnerabilities and information security controls that organisations need to put in place.

It is indisputable that there is an existing connection between cybersecurity and information security (Von Solms & Van Niekerk, 2013). In most instances, individuals often misinterpret the two terms as having the same meaning. The difference is that cybersecurity is similar to an online battlefield, where the users have to be alert and ahead of the attacker in order not to fall for online attacks (Oltramari, Henshel, Cains, & Hoffman, 2015). Also, cybersecurity protects mainly technologies, policies, and protocols, which are formed to protect computer networks (Cavelty, 2014). On the other hand, information security relates to the controls that can be used to safeguard private information that can be found once an attacker enters the network. The information could be found either on online sites, or outside the internet. As long as this information is sensitive it requires information security to keep it safe. Moreover, information security entails that sensitive information is accessed only by authorised and authentic users.

Nowadays, online services and social platforms, such as Instagram and Facebook, are used by individuals daily. The constant use of such social platforms means that there is a higher chance that an individual's privacy will be violated (Wüest, 2010). This is because attackers target social networks, mainly to discover individuals' online behavioural patterns (Hung, Shih, Shieh, Lee, & Huang, 2012). Sharma (2012) also affirmed that social networking sites are the main grounds for attackers stealing PII. Social networks also assist the attacker with information regarding the suitable time to steal a user's information. This is because of the individuals' constant exposure of their daily activities, which informs the attackers of times these individuals are most vulnerable. Social engineers make use of public information, such as regular check-ins on social networks, to discover the patterns and a suitable time to attack (Reyns & Henson, 2016). They also take time to build a user's profile in order to get an in-depth understanding of the individual, and to access sensitive information without the user noticing. Considering the size of the internet, attackers' chances of accessing the individual's information is increased (Panchenko, Lanze, Pennekamp, Engel, Zinnen, Henze, & Wehrle, 2016). Thus, measures to protect individuals' information become crucial due to the sensitivity

of their PII. It also appears that attackers will continue stealing individuals' information, since individuals are unaware that certain behaviours on social networks create vulnerabilities which put them at risk.

In the context of information security, online privacy of personal information becomes a complex issue. Privacy is described as the level of control individuals have over the disclosure of online personal information, as part of their PII (Alexander, 2007). Privacy consists of the ability to be able to socialise on social platforms anonymously, using fictitious names (Such & Criado, 2018). In order to combat privacy challenges, social network providers introduced visibility restriction options to only friends, or friends within the circle of friends (Raber, Kosmalla, & Krueger, 2017). The restrictions allow for PII to be confined to people inside the subset group (Sinha, Li, & Bauer, 2013). For instance, Facebook has restriction settings of who may see your profile, pictures or any other biographical information. Despite the introduction of privacy restrictions, young South African adults still do not know that such measures exist (Nyoni & Velempini, 2018). Young adults consider the process of setting the privacy settings manually exhausting, and complex if the structure of the settings is adjusted regularly (Watson, 2015). As a result, users unintentionally share information, which exposes their personal information to a broader audience. It was also found that experienced social network users disclose more PII because their privacy settings are restricted to a selected audience. Further information security research has found that there exists a gender difference in privacy settings (Archer, Wood, Nosko, De Pasquale, Molema, & Christofides, 2015). Young female adults have demonstrated more use of privacy settings than their male counterparts.

The responsibility for online privacy is highly dependent on both information technology (IT) and on physical security (Mann, 2017). IT security dependency relates to measures such as firewalls and secure passwords; whereas physical security incorporates security measures such as computer cable locks and manual access controls. Mann (2017) further argued that, for both IT and physical security, human security is considered the missing link in security control measures. It is perceived that information security requires an extensive approach, beyond IT and physical security, in order to combat online social engineering attacks (Sharma, 2012). This is because both technical and physical security alone cannot prevent the prevalent online attacks. In addition, it is fundamental to investigate the defense measures put in place for online attacks since social engineering techniques bypass all physical and technical security measures. The methods used by the attackers target the human element and humans have repeatedly been

the reason for the success of the attacks. Although humans implement security controls, they are unaware that social engineering can bypass their IT and physical controls.

The rationale behind information security on online sites is adherence to the confidentiality, integrity and availability (CIA) triad. The CIA triad is considered an accountable environment that protects users' PII. As depicted in Figure 2.2 below, an environment that is secure consists of the fundamental information security pillars. The CIA triad serves as a basis for the necessary security measure to protect information.

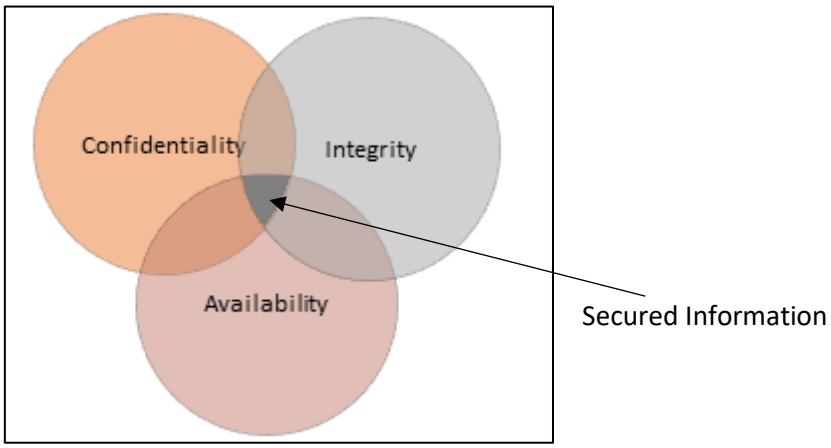

Fig. 2.1: CIA Triad (Mohanty, Ganguly, & Pattnaik, 2018)

The key elements that govern information security are in the CIA triad, which consists of the following elements:

2.3.1 Confidentiality

Peltier (2010) defined confidentiality as the assurance that information will not be revealed to individuals who do not have the appropriate privileges. Generally, confidentiality is a concept that is regularly misunderstood for privacy and often used interchangeably (Corey, 2019). The underlying principal of distinguishing confidentiality and privacy is that confidentiality ensures that privacy of information is upheld. Confidentiality further ensures that an individual's personal information is inaccessible to a third party who has no authorisation. Similarly, Andress (2014) defined confidentiality as a component of privacy which refers to the capability of protecting sensitive information. However, social engineering is considered a threat to confidentiality due to its ability to breach the confidentiality principle (Sattarova Feruza & Kim, 2007). By incorporating skilled attackers and modern social engineering techniques, social engineers effortlessly obtain sensitive information without authorisation.

Confidentiality, as a component of information security, can be implemented at multiple levels of a security process (Corey, 2019). For example, a student's password, used to log into his student portal, to view his marks, would be kept confidential by the student. On the other hand, the student's authorised lecturer has access to the student's marks and the student's biographic information. The lecturer, being authorised, would also maintain the level of confidentiality by not exposing the student's name on the results notice board. Instead, the lecturer would display the marks and use the student's number, a personal identifier, to uphold the level of privacy through confidentiality. Yet, the level of confidentiality may be compromised by a malicious user who could gain unauthorised access to the school's system.

2.3.2 Integrity

Hussein, Khalid, and Khanfar (2016) defined integrity as the practice of safeguarding information to restrict deletion, modification, or fabrication by unauthorised individuals. Integrity is essentially the assurance that any information stored will not be changed maliciously or destroyed unintentionally (Peltier, 2010). Upholding the integrity principle implies that the information stored is consistent and accurate. In the context of social engineering, integrity is violated when attackers infect an individual's system with a virus which is usually malware (Sattarova, Feruza & Kim, 2007). Malware is often used by attackers to breach the integrity pillar of the CIA triad. To prevent integrity breaches, online sites use authorisation to determine the authenticity of the users. The authentication uses measures such as a combination of a user's username and password. This has led to authorisation procedures becoming vital in enforcing data integrity, since social engineers are capable of using false identities (Whitman & Mattord, 2014). Moreover, to ensure a high level of integrity, some social networks ensure an end-to-end encryption. Encryption is used to ensure that the messages have not been intercepted by man-in-the-middle (MITM) attacks (Greenberg, 2015). An example of a social network platform that uses end-to-end encryption is WhatsApp. The objective of using this practice is to eliminate intruders, such as social engineers, from gaining information that is sent through messages between the parties involved.

2.3.3 Availability

According to Mohanty et al. (2018), availability entails the assurance that information is suitable for access whenever the authorised individual requests it. Accordingly, the information should be accessible only to the authorised parties. Similarly, Hussein et al. (2016) stated that,

in their view, information has value to users when it is accessible at the desired time. Over time, the concept has changed, since social engineers see value in sensitive information that they can access. Generally, social engineers use the accessed information to achieve financial gains through ransomware. In recent times, individuals often use the cloud storage applications as a form of backup of their information. For example, Google Drive allows individuals to store any form of information and the individual uses precise credentials to access the information. In cases where social engineers hack the Google Drive storage, they would then insist that the user pays a certain amount, or else they would expose the information. In that way, the availability principle is breached by the social engineers' ability to gain an individual's information. To uphold the availability principle, online storage platforms have implemented authentication, which is aimed at ensuring that the individual is verified prior to obtaining any sensitive information.

2.4 Gender

Traditionally, as discussed by Joffe (1985), gender was classified as a socio-cultural structure, wherein both males and females have distinctive duties to carry out, enforced by the patriarchal system. In an opposing view, Tickner (1992) defined gender as the non-biological features of both males and females. Gender is regarded as the differences that occur in behaviour, attitude, and perception, between males and females. The gender difference continues to exist, and literature has shown that behavioural differences between genders are apparent when it comes to internet use (Dufour, Brunelle, Tremblay, Leclerc, Cousineau, Khazaal, Légaré, Rousseau, & Berbiche, 2016). During the early stages of the internet, the web was dominated by male users. Over the years, the rapid growth and development of the internet has led to an increase in the number of personal daily activities that have shifted online (Ritter, 2015). The growth of the internet has led to an increase in the number of female users, compared to male users (Bae & Lee, 2011). Furthermore, the growth of the internet has permitted both genders to use the online platforms for business, socialising and communication. Thus, more distinct gendered behavioural patterns become evident. Scott (2017) stated that online platforms have permitted individuals to share online information freely, such as their personal information, views and experiences, within their online communities. Although the internet has brought about changes in the ways that individuals interact, it is unfortunate that not much research has been carried out on gendered differences in the information security sector. Recent studies have shown that gender has not been a factor that has been tested in the information security discipline (Trauth, 2013).

Females, as compared to their male counterparts, have little or no influence when using the dominant forms of communication such as Facebook and Twitter (Carli, 2001). Males are regarded as more influential, yet are less dominant on online platforms that have predominantly female users (Maceli, Baack, & Wachter, 2015). Despite males and females having different motives for online use, male online dominance is endorsed by statistics that reveal that males form the majority of the world's population (Countrymeters, 2017). This also means that a higher percentage of males use the internet. Generally, a male's identity is highly influenced by cultural influences and identifiers such as family, race and sexual orientation (Fang, Wen, George, & Prybutok, 2016). In the South African context, males come from socially structured environments where they are taught dominance, control and power, as preconditions to gaining respect (Mashiya, Kok, Luthuli, Xulu, & Mtshali, 2015). To neutralise the hierarchical gender differences, the South African government has established numerous policies to ensure that gender equality exists (Joseph, 2011).

In terms of online information disclosure, such as contact numbers and addresses, studies have shown that such information is disclosed mainly by males (Hajli & Lin, 2014). However, females post the most on social platforms and are more likely to comment and like other individuals' posts. In addition, females have the highest percentage of online risk and privacy concerns. This is due to females posting personal information, and attackers see this as an opportunity to use to gain trust (Hoy & Milne, 2010). The major areas of online concern reported by both genders are receiving an email from an unknown source, and being alerted that personal information is being used by a third party (Butavicius et al., 2016). Thus, individuals continually read unsolicited emails and register for websites that require their personal information. Individuals of both genders assist the attackers unknowingly, due to a lack of social engineering awareness.

Society expects females to take on different roles to males. Females, from a young age, are expected to take on roles that are more nurturing, less technical, and domestic in nature; whereas, males are traditionally expected to take on duties and occupations that allow them to behave in a bold manner (Carli, 2001). It is also commonly known, and acceptable, that males portray more direct forms of aggression than do females. This is realised when traditional types of violence manifest on the internet as forms of cyber-bullying. In a study conducted by Heiman and Olenik-Shemesh (2015), it was noted that females had a higher rate of victimisation;

whereas social engineering and other forms of cybercrime are more commonly committed by males. This is because perceptions of societal masculinity are transferred onto the online domain. The relationship between social engineering and gender follows the nature of societal upbringing. As a result, societal teachings based on gender roles transfer onto the online world. However, there is a gap in the literature showing the gender differences that exist in online social engineering (Algarni et al., 2014; Slonka, 2014).

The gullibility theory explains the willingness to trust someone, even without reasonable proof (Bullée et al., 2015). The optimistic bias theory explains that individuals believe that they have higher chances of positive events than negative ones. Both the above-mentioned theories imply that individuals believe that they are unlikely to become victims to social engineering attacks. Šincek (2014) in his study showed that males have the highest rating for becoming social engineers, whilst females have a higher chance of falling victim to social engineering attacks. It is thought that females fall prey the most because of their online behaviour patterns (Grabner-Kräuter & Bitter, 2015; Hinson, 2008), which are easily obtained due to their active engagement with social platforms and by being active online shoppers. Therefore, female behaviour patterns become easily predictable for social engineers, which aids the social engineer in creating an entry point that would entice the targeted individual (Bae & Lee, 2011). In a similar study, it was evident that young female adults make no effort to familiarise themselves thoroughly with the internet and are therefore unfamiliar with many online websites. This in turn leads to carelessness in their online usage, which leads to vulnerabilities that work in favour of the social engineers (Fathollahi-Fard, Hajiaghaei-Keshteli, & Tavakkoli-Moghaddam, 2018).

It is therefore imperative to understand gendered online behaviour regarding online information security (Lewis, 2015). Gaining an understanding may assist in developing measures that educate both gender groups about prevalent online social engineering threats and risks. The different online environments, such as Twitter and gaming sites, portray distinctly different gender behaviour, and an understanding of these gender differences can be drawn from different online platforms (Helsper, 2010). Also, the difference in technology exposure that exists between males and females plays a vital role in online behavioural patterns. Males are more frequently introduced to various technological gadgets and internet usage, compared to females, despite the equal level of internet accessibility. Learned behaviours become the motive behind the difference in gender roles across the internet (Norona, Preddy, & Welsh,

2015). Gender is therefore socially constructed over time and leads to the identifiable behavioural patterns that bring about differences between male and female behaviours.

2.5 Online social engineering is human-dependent

Internet users are considered the weakest link in information security because of the amount of personal information they expose. The information is useful to social engineers since they target the weakest link in any security chain (Mann, 2017). The issue of social engineering is manifold, and the human element is the major factor in social engineering, due to the diverse techniques that social engineers presently use (Kritzinger, 2006). The common issue that individuals face is the lack of social engineering awareness because not much research has been conducted to understand the human element in social engineering attacks (Noureddine et al., 2015). This, in turn, leads to minimal knowledge about gender-specific ways that can help combat the human element in social engineering attacks. There is also no framework that distinctly identifies and improves social engineering challenges relating to the human component (Abeywardana, Pfluegel, & Tunnicliffe, 2016). Therefore, humans' lack of awareness is displayed across the different attacking methods used by social engineers. Lack of awareness results in opening an email attachment that contains malware, without having the necessary knowledge to recognise the false message. Subsequently, lack of social engineering awareness leads to an individual becoming a social engineering victim.

Humans, irrespective of gender, experience various external influences when growing up (Bornstein, 1991). As males and females mature, they are continuously influenced and taught how to socialise and behave within their societies. These variations are seen on social networks where each culture displays different behaviour. Freeman (2007) argued that children develop an understanding of their gender at a young age, further ascertaining that children act according to their gender, based on their upbringing. A child's cognitive development depends on the parent's elementary child-rearing principles (Ford, Massey, & Hyde, 1985). As a result, a child's parental teachings reach beyond the household into all aspects of the outside world, such the online world. Individuals do not have the same cultural beliefs, and each generation of young adults experiences different cultural events. These different encounters trigger dissimilar behaviours and actions when faced with online social engineering attacks (Twenge, 1997). Therefore, social engineers may choose to use various techniques to lure the target, based on the target's culture (Algarni et al., 2014).

According to Parbanath (2011), in order for attackers to conduct a social engineering attack, they require the individual's personally identifiable information. In most instances, individuals provide their personal information to a social engineer through being deceived. In the South African context, young adults have the highest percentage of internet usage, which implies that young adults have a higher risk of falling victim to online social engineering attacks (Lenhart, Purcell, Smith, & Zickuhr, 2010; Hasim & Salman, 2010).

2.6 Young adults

According to Hasim and Salman (2010), the youth are the leaders of the future and therefore need to master the existing and innovative technology. Nowadays, young adults are constantly using the internet for various forms of activities such as communication, online transactions and educational programmes. The use of the internet by young adult students grows continually as it provides different learning platforms. Furthermore, it has been noted that students are the societal group with the highest percentage of internet usage (Zhang et al., 2017). However, according to Lenhart et al. (2010), students' online behavioural patterns are much like those of teenagers.

A study conducted by Charles (2017) showed that online social engineering is a rising concern, since young adults are falling victim through being misled on the internet by social engineers. Further observations from the study showed that attackers tend to target a specific group of individuals, mainly young adult females. Social engineers target females, mainly because females are known to have considerably more vulnerable traits and are also careless on the internet. According to Tsarwe (2016), females are emotionally open on social network platforms and on other internet sites. Therefore, the expressed emotions become publicly accessible, allowing for attackers to identify the vulnerabilities. Furthermore, it has been reported that the impact of the internet on young adult students is more negative than positive (Thabethe, 2016). The negative impact is caused by malicious users, regardless of students' wise use of the internet (Galloway, 2013). Previous literature has shown that young adult students use the internet for their personal sense of fulfilment, such as conducting online purchases and communicating on social networks.

In South Africa, according to the Internet World Stats (IWS), 52% of the country's population are internet users, as recorded in June 2016 (InternetWorldStats, 2016). In another recent article, it was reported that, for the first time, South Africa has reached over 20 million internet

users (TimesLive, 2017). Table 1.1, below, shows the South African internet users ranked by gender and age. The table shows how the young adult age group (between the ages of 18 and 35 years) comprises the highest percentage of internet users. The table further shows how young female adults have a higher internet usage, compared to their male counterparts. In a study conducted by Perrin (2015), it was evident that females have a slightly higher internet usage than their male counterparts. However, in recent years, both genders have had a comparable rate of internet usage. Social networks are ranked as one of the highest sites for SE attacks (Wüest, 2010), and young adults who are responsive to the attacker's messages, fall victim. This is due to the social engineer's impersonation of a credible source whom the targeted potential victim knows very well, such as a friend or a relative (Algarni et al., 2014).

Table 1.1: South African Internet Users (MyBroadband, 2014)

South African internet users	
Gender	Percentage
Female	50.82%
Male	49.18%
Age	Percentage
Under 15	0.12%
15 – 17	3.22%
18 – 19	6.57%
20 – 24	15.57%
25 – 29	15.70%
30 – 34	13.39%
35 – 39	10.57%
40 – 44	9.36%
45 – 49	7.83%
50 – 54	6.88%
55 – 59	5.37%
Over 60	5.42%

Nowadays, social networking sites have become virtual communities for most young adults and the correlation between age, online social networks, and transactional platforms is strong (Perrin, 2015). It is also evident that young adults who have a form of tertiary education have

the most exposure to the internet. Statistics revealed that the age group that is most likely to use online platforms are young adults aged between 17 and 30 years. Due to the internet's size, young adults' online communication becomes risky since it is possible that they do not know with whom they are communicating (Charles, 2017). This is considered to be one of the reasons why social engineers are successful in winning young adults' trust over the internet, as well as the indirect communication that does not allow the young adult to verify the validity of the social engineer. Therefore, it becomes difficult to identify social engineers from genuine users. As technology evolves, cracking or hacking into young adults' systems is no longer the technique used since it is outdated and requires the social engineer to have physical access to the young adult's device. The current social engineers use young adult students as an instrument to disclose their own personal information through manipulating and misleading the young adult.

Increased internet usage amongst the youth raises other issues such as disclosure of confidential information and lack of privacy awareness (Salehi, Khalili, Hojjat, Salehi, & Danesh, 2014). Drawing attention to the darker side of internet usage, Vanderhoven, Schellens, Valcke, and Raes (2014) assert that the increasing rate of internet usage amongst students perpetuates the information security issues. An example given by Wallace (2014) was that of a young couple in Korea who was determined to raise an online virtual daughter and ended up neglecting their biological daughter.

2.7 Conclusion

This chapter discussed the basis of social engineering and the literature review showed how social engineering can be associated with numerous risks for individuals. This is due to the nature of social engineering threats that are growing on a global scale. Irrespective of gender, an individual's equal chance of being a victim puts his sensitive information at risk. Also, the way in which individuals, especially young adult students, have become heavily reliant on the internet increases the number of vulnerabilities that attackers exploit. Individuals are the weakest link in the information security chain, and social engineering capitalises on this information security gap. The current level of skills that social engineers have makes it difficult for both males and females to detect and defend themselves from online attacks. Therefore, information security in relation to social engineering needs to be encouraged, by educating individuals about ways in which they can protect themselves from the growing social engineering attacks.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The literature review laid a foundation for understanding social engineering and how it breaches information security, as well as the threats that it poses to individuals. Further, the chapter outlined the overall importance of educating individuals about social engineering. The importance of awareness is motivated by the rate at which social engineering attacks are developing. Accordingly, the main objective is to explore the level of knowledge young adult students have of social engineering, and to also determine the type of social engineering attacks young adults encounter. Therefore, online behaviour and attitude of young adults were investigated. Remenyi and Money (2012) defined research methodology as the heart of any research since it consists of techniques that are applied to investigate the phenomenon at hand. Therefore, in this chapter, the researcher elaborates on the research techniques and methods that form a basis for this study.

3.2 Research Objectives

In Chapter 1 the research questions were outlined. The following are the research objectives resulting from the research questions:

1. To determine whether there is a gender difference in the response of tertiary students to online social engineering;
2. To identify students' knowledge about online social engineering from a gender perspective;
3. To determine if there is a gender difference regarding online information security among young adult students.

3.3 Research design

3.3.1 Research Structure

The primary research question for this study is; "To what extent is there a gender-dependent response to online social engineering (OSE) attacks amongst young South African adults?"

As stated by Kothari (2017), the research design explains what the study entails, the unit of analysis, the data collection method and the type of results the study seeks to achieve. This in turn allows the researcher to respond to the main research question. Also, to further provide an

analysis that meets the objectives of the study, the researcher implemented the following phases:

1. Research method: qualitative research design
2. Sampling plan
3. Data collection
    a. Questionnaire design
    b. Distribution of questionnaire
    c. Capturing data
4. Data analysis
    a. Data processing
    b. Analysis
    c. Interpretation
    d. Reporting

3.3.2 Nature of the study

Research design has several different forms, namely exploratory, explanatory or descriptive. Marshall and Rossman (2014) described the three type of studies:

- **Exploratory research** is usually conducted when not much is known about the phenomenon. The researcher conducts this type of study when there is no knowledge available on the research problem and no related studies that indicate ways in which a similar phenomenon has been addressed.
- **Explanatory research is** mainly used to identify any form of causal relationships between factors that relate to the research phenomena. This type of study is also referred to as an analytical study which has a structured nature.
- **Descriptive research is** aimed at providing an exact reflection of the variables that are related to the research question. Also, this research type is more structured than the exploratory study.

The nature of this study is exploratory because not much is known about the research phenomenon. As stated by Bhattacherjee (2012), exploratory research is most effective when exploring causes and outcomes. In this study, the researcher's objective is to explore the gender differences in online social engineering attacks amongst young adults. Therefore, the study is aimed at investigating the motives that cause both genders to comply with social engineers'

instructions; as well as the types of social engineering to which both genders are susceptible. Hence, an exploratory design was chosen.

3.3.3 Exploratory research design

There are four types of exploratory research design (Bhattacherjee, 2012):

- Survey research design
- Secondary data research design
- Case study design
- Interview research design

A survey research design is used to allow a researcher to gain information from participants. The information that is gained usually relates to the perception, behaviour and attitude of the participants (Beam, 2017). Also, surveys are designed to define the frequency of occurrences across a population (Cooper & Schindler, 2014). Therefore, for this study, the researcher adopted the survey design as it was the most suitable.

3.3.3.1. Data collection instruments for survey designs

i.) **Interviews:** Interviews are constructed in two different ways, using structured and semi-structured interview techniques (Bradburn, Sudman, & Wansink, 2004). Structured interviews consist of the interviewer only asking a set of questions Semi-structured interviews also consist of a set of questions. However, they allow the interviewer to probe the participant's perspective to gain an in-depth understanding of the participant's reasoning.

ii.) **Questionnaires:** According to Dörnyei and Taguchi (2009), questionnaires are the most commonly used data collection instrument for statistical studies. Bhattacherjee (2012) specified that a questionnaire is a standardised research tool that was invented to gather responses from participants, either in a structured or unstructured manner. Structured questions, which are also referred to as closed-ended questions, are challenging to construct yet easier to analyse, with less code contradiction (Bradburn et al., 2004). Whereas, open-ended questions, unstructured questions, are used for developmental studies which explore the phenomenon in detail. Furthermore, unstructured questions allow participants to state their opinions, attitude and beliefs.

Questionnaires also come in different forms such, as interview schedules and self-administered documents (Dörnyei & Taguchi, 2009). Interview schedules are conducted through using fixed questions that are posed to a participant and the interviewer marks or records the participants' responses on the answer sheet. On the other hand, self-administered questionnaires are manually distributed or posted to participants' mailboxes, or via electronic mail. However, the disadvantage of posted questionnaires is the low response rate and participants are unable to be guided through the questions if they seek clarity (Sekaran & Bougie, 2016).

For this study, questionnaires were adopted as the data collection instrument. Manual, self-administered, questionnaires were considered the most appropriate for this type of study, primarily driven by the data which was collected across different locations. The electronic method of distributing questionnaires was not considered, due to the disadvantage of low response rates. Thus, questionnaires were distributed by hand to the participants which allowed participants to ask if they required any clarity.

3.3.4 Questionnaire design

Kothari (2017), stressed that for a quantitative study, a questionnaire is an important part of the study. Therefore, it is essential that questionnaires are carefully constructed. The questionnaire for this study was adapted from similar studies previously conducted on online attacks. Thus, questions were adjusted to suit the context of this study. The structure of the questionnaire was designed into sections as follows:

Section A: Demographic information

This section presented questions relating to the participants' gender, age, race, institution, and faculty. Gender was the main factor that would reveal the gendered differences in the analysis phase.

Section B: Awareness

This section consisted of questions that required the respondents to identify and match the question with the provided options. This was aimed at identifying the knowledge of the respondents about the different types of social engineering attacks. Also, the awareness section consisted of questions that asked respondents to match their understanding of preventative

measures which they considered appropriate. The aim was to understand if participants were aware of measures that could help secure their online information.

Section C: Adequate responses

The objective of this section was to obtain information about respondents' conduct regarding online messages and attachments that they receive via email, links, online pop-ups, or from social network sites. Further, the section was aimed at understanding gender responses to messages that seem malicious; and additionally, to determine whether there are gender differences in responding to security alerts and emails from known sources, as compared to unknown sources.

Section D: Attitudes

This section was in a form of a Likert scale, questioning individuals about their security beliefs and concerns about online security controls and responses.

Section E: Behaviour

This section posed various questions to get information about the respondents' online behaviour, with respect to passwords. The objective was to understand if respondents' were careless, leading to vulnerabilities which are later exploited. The questions explored privacy on social sites, password sharing and the extent of personally identifiable information (PII) shared online.

3.4 Research approaches

Research approaches are categorised into two methods (Bhattacherjee, 2012) which are as follows:

3.4.1 Qualitative

Moore (2016) stressed that qualitative studies consist of how, what and why questions that require data to be collected using qualitative methods. This method of data collection consists of interviews or open-ended responses from a questionnaire, conducted in an interview format. According to Yilmaz (2013), qualitative information is collected using observation, document analysis, focus groups, and in-depth interviews.

3.4.2 Quantitative

A quantitative study has the objective of investigating the variance between the how and why of the phenomenon (Kefalas, 2017). Further, quantitative studies use statistical analysis which provides numeric findings. The findings describe relationships between constructs found in the adopted theory. Moreover, quantitative studies also test the hypothesis by collecting quantifiable data, whereby the hypothesis states the nature of the relationship (Moore, 2016).

This study adopted the quantitative research approach so that the formulated hypotheses could be tested accordingly. The quantitative approach was also used because it provided statistical results on the gender differences, based on the research phenomena. The questionnaire also consisted of structured questions; hence, the numeric findings were objective.

3.5 Sampling

3.5.1 Sample design

A sampling process consists of three phases (Kothari, 2017) which are as follows:

1. **Defining the population:** This is a selection of the group of individuals a researcher has identified to study.
2. **Sampling frame:** A list of the population is provided to a researcher where the sampling frame can be deduced.
3. **Sample selection:** A definite selection of the sample, based on the sampling technique adopted, is selected from the sampling frame.

3.5.2 Sample size

The sample size was selected, based on the table presented by Krejcie and Morgan (1970). The table shows that for a target population between 27000 and 30000, the sample size must be 379. Therefore, 379 students were selected. Based on the odd number, 190 questionnaires were distributed to female students. The remaining 189 questionnaires were handed out to male students. Studies have revealed that there are more females than males in SA universities (Moosa, 2017). Therefore, the researcher opted to administer the extra questionnaire to a female student.

3.5.3 Sampling techniques

According to Flick (2015), sampling methods in quantitative research can be grouped as follows:

- non-random/ non-probability sampling designs and
- random/ probability sampling designs

In a non-probability sampling technique, some units in the sample have no chance of being selected (Bhattacherjee, 2012). Each unit is selected via non-random conditions. The following non-probability sampling techniques were identified (Creswell, 2002):

i. Quota sampling

Researchers consider this sampling technique if there is ease of access to the sample population (Mackey & Gass, 2015). Primarily, the sample is selected based on a location convenient to the researcher. Also, if the researcher comes across an individual that meets the criteria of being a participant, the researcher asks the individual to participate in the study. This type of technique is the least expensive method of selecting a sample and not much sampling information is needed. Information such as total number of units, location and sampling frame is not required. However, the disadvantage is the resulting sampling not being a probability of one.

ii. Convenience sampling

This sampling technique relies on the convenience of accessing the sampling population. The population does not share the same characteristics. Also, data collection is stopped when the desired number of respondents in the sample is met (Mackey & Gass, 2015).

iii. Expert sampling

In this sampling technique, participants are non-randomly selected. Participants are selected based on their knowledge of the research problem being studied. This approach has credible opinions because the sample experts are familiar with the subject matter (Bhattacherjee, 2012).

In a random sampling technique, Bilau, Witt, and Lill (2018) stressed the importance of an equal chance of selection for each unit. This implies that the probability of selection is

independent and not influenced by bias preferences. The identified probability sampling techniques in quantitative research are as follows:

i. Simple random sampling

This type of technique is commonly used since it is the simplest of all the methods of probability sampling and is suitable for smaller populations. Simplicity is the advantage of this technique because the sampling frame is not subdivided, and the findings are generalised.

ii. Stratified random sampling

The stratified technique allows the researcher to divide the sampling frame into different groups (Bhattacherjee, 2012). The groups are created through categorising common characteristics, such as male and female.

iii. Cluster sampling

Cluster sampling is based on dividing the sampling population into groups, in instances of large population sizes. The groups are called clusters and can be formed based on common characteristics or geographic locations. The challenge with this sampling frame is identifying each sampling unit within the population (Bhattacherjee, 2012).

This study applied the probability sampling technique using the stratified sampling method. The subset of the target population was ranked according to gender: male and female and 150 questionnaires were distributed to the FET college and 229 at the University of KwaZulu-Natal, Pietermaritzburg (UKZN-PMB). The intention was for a 50% distribution to male students and the other 50% to female students. However, due to the predominance of female students in academic institutions, more female students were present (Moosa, 2017). Therefore, more female than male students completed the questionnaires.

3.6 Study site

The study site is South Africa; and within South Africa, the KwaZulu-Natal province was the site of the research. This study was conducted in the capital city of KwaZulu-Natal, Pietermaritzburg, due to the ease of data collection for the researcher.

3.7 Target population

For this study, the target population consisted of young adults in South Africa. The sampling frame was young adult students from Pietermaritzburg. The sample was taken from Umgungundlovu FET College and UKZN-PMB campus. The population size is approximately 27000 students and the target population was further divided into two groups, or subsets, classified according to gender.

3.8 Data analysis

Descriptive and inferential analyses are statistical methods of analysing numeric data (Neuman, 2013). According to Bhattacherjee (2012), descriptive statistics describe the population and inferential statistics make a generalisation about the population. In this study, the collected data was interpreted into meaningful numeric variables. Thereafter, it was captured into the Statistical Package for Social Sciences (SPSS) for analysis. SPSS is a software package that allowed the data to be analysed effortlessly (Hinton, McMurray, & Brownlow, 2014). This study used both inferential and descriptive analyses. Descriptive analysis was used for the graphical interpretation to summarise the data. Inferential analysis was used to make logical meaning of the findings by simplifying and interpreting the data in a general manner.

3.8.1 Reliability and validity

In order for a study to be valid and reliable, it must implement a data collection instrument that will accurately measure the research questions and hypotheses (Neuman, 2013). Reliability consists of accuracy and consistency of the measurement tool in measuring the study's phenomenon. Validity highlights the credibility of the researcher's conclusions (Sekaran & Bougie, 2016). The reliability of this study was verified accordingly, using the Cronbach Alpha. Validity was ensured by submitting the questionnaire to the researcher's supervisor for input and corrections. Thereafter, the questionnaire was sent to UKZN's research office for approval.

As identified by Sekaran and Bougie (2016), the reliability tests are as follows:

3.8.1.1 Reliability

Stability of measurements

- **Test-retest reliability** is achieved when the same measurement is tested over time on the same set of respondents several months later.

- **Parallel-form reliability** is defined as using different research instruments to measure the same set of respondents. For instance, dividing questions in a questionnaire into two sets.

Internal consistency of measurements

- **Inter item consistency reliability** is used to test the consistency of the participants' responses to all the sub-topics in a construct. Independent measurements of the same construct will have the same correlation.
- **Split-half reliability** shows the relationship consistency between a knowledge area which is divided into two sets.

A quantitative study ensures validity by considering the following (Van Rensburg, 2017) :

3.8.1.2 Validity

- **Construct validity** determines the extent to which the data collection instrument connects to the primary research framework. This study was influenced by the two research theories discussed in Chapter 1.
- **Face validity** is met when the measurement tool measures what it projected to measure (Sekaran & Bougie, 2016). For this study, the questions found in the questionnaire intended to investigate the difference in the young adults' responses to online social engineering attacks. The measurement of young adults' responses is based on gender.
- **Content validity** is achieved when the research instrument adequately measures the research concept. The questionnaire covered a wide range of areas related to online social engineering.

3.9 Theoretical frameworks

This study implemented two frameworks. The Gender and International Security Feminist Theory was formulated in 1988 by Sjoberg (2009). This theory was used as the lens of the study, for the gender context. The second theory employed was the Theory of Reasoned Action (TRA) developed by Ajzen and Fishbein (1980). The TRA theory was used as the information security studies theory which is within the discipline of the research paper. There are no theoretical frameworks in information security studies that examine the element of gender (Trauth, 2013). Therefore, the research had to implement the two theories to incorporate the gender aspect of the research project.

3.9.1 The Gender and International Security Feminist framework

The Gender and International Security Feminist framework was used to understand the research objectives from a gendered perspective. Based on the questionnaire, this framework examined the participants' responses, in relation to the TRA constructs. The two frameworks are used to understand the differences that exist between male and female students. Further, understanding the responses of both genders helps in determining the gender that falls victim the most due to their lack of knowledge or careless online behaviour. Further, understanding the gendered differences regarding social engineering will assist in developing awareness programmes that can be tailored to each gender group. Therefore, awareness programmes will be personalized, based on the findings of this research.

3.9.2 Theory of Reasoned Action

The TRA theory, which is an information studies theory, explains how individuals behave, based on their acquired knowledge of information security. The relationship of the framework's constructs in relation to the research questions were as follows:

Attitude

Individuals' attitudes to security practices are based on their learned behaviour or social engineering knowledge (Cooke et al., 2016). For instance, if an individual ensures that their privacy settings are restricted to their circle of friends, it implies that they do not want unknown individuals to know about their life. Such an attitude leads to them excluding certain individuals or even not accepting their friend invitations. In this study, this construct was used to understand the young adults' attitude to the importance of online security, and to discover if both male and female students have concerns about online security. It is believed that their online attitude or concerns would influence their online behaviour.

Subjective norm

Normative beliefs are external factors that influence an individual to behave in a certain manner (Cooke et al., 2016). For this study, the subjective norm was used to pose behavioural questions based on different situations. In the questionnaire, young adult students were asked whether they would give their details to an unknown person. Also, in another question they were asked if they would give out their personal details to an unknown person in order to win a prize. This was to determine whether external factors, such as winning a prize, influences students' behaviour.

Behavioural intention

Behavioural intention is an individual's instinctive behaviour while performing an action (Ajzen & Fishbein, 1980). Certain questions were aligned with this construct, when asking both male and female students whether they would act in a certain manner, based on their instincts. For example, there were questions that asked if an individual would share their credentials with a close friend. Therefore, if certain individuals instinctively believe that there is no harm in doing so, they would share information such as their passwords and usernames. This means that they innocently expose their information to possible attackers.

Behaviour

Behaviour is considered to be the final stage of an individual's behavioural decision-making process (Ajzen & Fishbein, 1980). In this study, this construct was aligned by asking questions that sought to understand both male and female students' online behaviour. Individuals were asked whether they revealed their true identities on their online social network profiles. They were also asked how often they changed their security settings and whether they checked in on social network sites. The objective was to understand the way they conducted themselves on online and on social platforms.

3.10 Ethical considerations

Beauchamp and Childress (2001) identified four important ethical philosophies that need to be considered in a research project:

1. **Autonomy:** Participants have the right to participate in a study without intimidation. The participants also have a right to be informed what the study is about. To ensure autonomy, this study implemented the following steps:
    - Participants were asked of their willingness to participate in the study.
    - Willing participants were taken through an explanation of the research and further questions from the participants were addressed.
    - To have full assurance of the participants' consent, the study was explained to the interested participants and they were asked if they were still interested in taking part in the study. Reassured participants were given a questionnaire that included a consent form which they were required to sign. Their signatures implied that they were agreeing to participate. Furthermore, their signatures would be affirmation that

they had full understanding and were willing to contribute to the research. Unwilling individuals were given the freedom to not participate in the study.

- To satisfy further ethical considerations, the researcher obtained signed gatekeeper letters from the institutions where the data was collected.

2. **Non-maleficence:** Mechanisms to prevent participants from psychological or physical harm were put in place. This study achieved non-maleficence by an ethical clearance application that was submitted to the university's ethical clearance committee. The application addressed maleficence issues.
3. **Beneficence:** Both the participants and society benefit from the research. One of the research objectives of this study is to provide platforms for awareness programmes, based on the findings of the research. By conducting awareness programmes, participants and society will have more knowledge of social engineering and will be more cautious in their online conduct. Participants will have less chance of being victims.
4. **Justice:** This refers to fairness in the way that all participants are treated. In this study, all participants were treated equality. No special incentives were given to specific individuals.

3.11 Summary of Chapter 3

The chapter highlighted the following key research areas:

1. The nature of this research was exploratory. The survey research design technique was adopted, and questionnaires were used as the data collection instrument. The questionnaires were self-administered.
2. The questionnaires were evaluated for validity and amended prior to their administration.
3. The sample population consisted of young adult students from Pietermaritzburg institutions, the UKZN and Umgungundlovu FET. The sample size was determined by the Krejcie and Morgan (1970) table.
4. Gatekeeper letters were obtained from UKZN and Umgungundlovu FET.
5. Collected data was coded and then captured into SPSS for analysis.
6. The results of the statistical analysis are presented in Chapter 4.

CHAPTER 4: FINDINGS AND ANALYSIS

4.1 Introduction

The preceding chapters presented the approaches that were used in conducting this study. This chapter presents the findings obtained from the student respondents. It additionally analyses the responses in relation to the research questions. As discussed in Chapter Three, this study's objective is to identify the gendered responses to online social engineering (OSE) among young adult students. Identifying the difference in responses of males and females leads to understanding the gender that is more susceptible to falling victim to online social engineering attacks, this can assist in personalising awareness programmes according to gender. This chapter presents the results obtained from the respondents. Further interpretations of the results are presented in Chapter Five.

4.2 Response rate

In this study, 379 questionnaires were distributed to the sample population on site. Both UKZN and Umgungundlovu FET College are based in Pietermaritzburg (Appendix C). The sample population was in conformity with the Krejcie and Morgan (1970) table. Of the total questionnaires, 229 were distributed at UKZN and 150 questionnaires at Umgungundlovu FET College. Umgungundlovu FET College had a smaller number of students enrolled for the NC4, which is equivalent to a tertiary qualification. A total of 361 valid questionnaires were returned, yielding a 95% acceptable response rate.

4.3 Consistency and reliability

To determine the internal consistency of the responses provided by the students, a Cronbach alpha reliability test was conducted. This test was conducted to determine whether the study generated comparable results for the tested questions, provided the research was to be conducted with a larger sample. The Cronbach alpha coefficient ranges from 0 to 1. Heale and Twycross (2015) stated that the closer the Cronbach alpha value is to 1, the higher the reliability of the responses. The items in the research instrument used for this study were assessed using the reliability test in the Statistical Package for Social Sciences (SPSS). The Cronbach alpha tested the 83 questionnaire items including the demographic variables of the respondents. The test results for all the items gave a Cronbach alpha value of 0.720, as presented in Table 4.1 (Appendix D).

Table 4. 1: Reliability test results

Cronbach's Alpha	No. of Items
.720	83

4.4 Normality test

The Kolmogorov Smirnov and the Shapiro-Wilk tests were used to determine the data characteristics. Norman (2010) noted that if the data is normally distributed, parametric tests such as t-tests and ANOVA are suitable. Therefore, data sets that do not follow a normal distribution employ non-parametric tests such as the Chi-square test and Mann-Whitney U test (McCrum-Gardner, 2008). The normality test hypotheses used are as follows:

H_0: The variables tested are normally distributed
H_1: The variable tested are not normally distributed

The normality of a data set is determined by producing a significance value greater than 0.05 for both the Kolmogorov Smirnov and the Shapiro-Wilk tests. The significance value obtained for this study was less than 0.05 (see Appendix E). Therefore, the results reject the null hypothesis (H_0) for all the variables. Thus, non-parametric tests are applicable to test the variables of this study. Hence, the Chi-square test was employed on the variables of this study to determine the significance of the results obtained.

4.5 Descriptive statistics

The descriptive statistics were generated, based on the data code entered in SPSS. Detailed descriptive statistics for each of the items in the research instrument are presented in Appendix F. The respondents' demographic information for this study is as follows:

4.5.1 Gender

Gender responses for the study's population size had an outcome of 44.6% males and 55.4% female students (See Fig 4.2). These findings correlate with a study conducted by Cloete (2014), where it was evident that tertiary institutions have a higher number of female students.

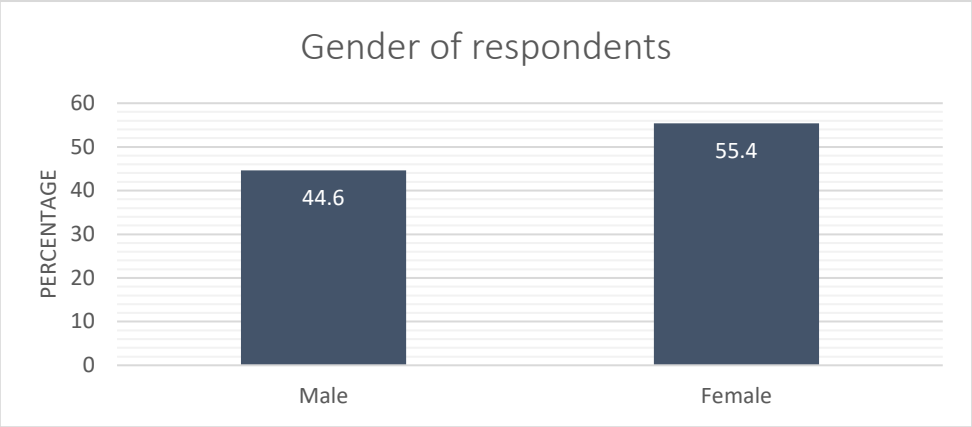

Fig. 4. 1: Gender representation of respondents

4.5.2 Respondents' ages

The respondents' ages, as in Fig 4.2, show that out of the 361 students that participated in this study, 46.0% were between the ages of 21 and 23; with 27.7% between the age of 18 and 20; 17.5% were aged 24 to 26; and 8.9% were 27 years and older. This resonates with a study conducted by Cloete (2014) which found that most students enrolled in universities are between the ages of 20 and 24.

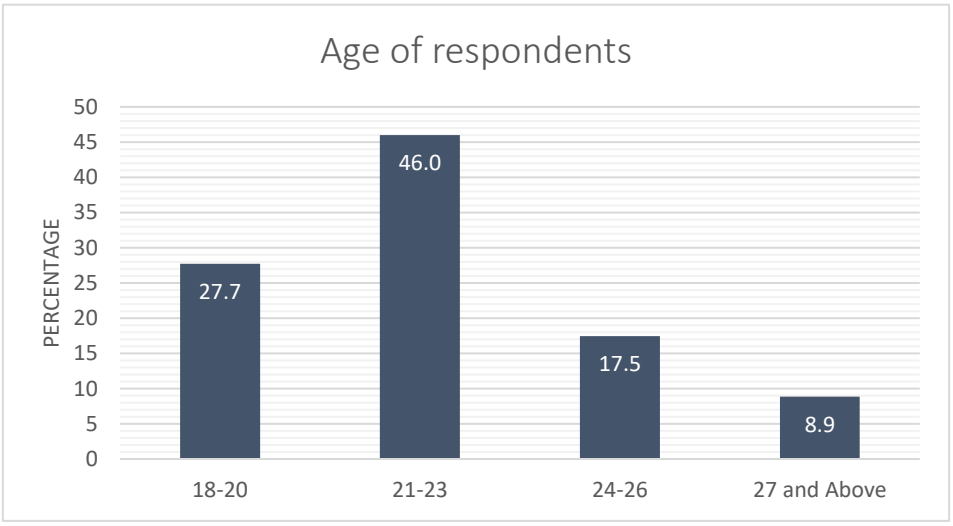

Fig. 4. 2: Age range of respondents

4.5.3 Respondents' racial classification

The targeted population of this study was young adult South African students based Pietermaritzburg, in the KwaZulu-Natal province. KwaZulu-Natal is dominated by the African population, followed by the Indian ethnic group (Naidoo, 2011). South Africa has a predominance of four ethnic groups, namely African, Indian, Coloured and White. The ethnic

groups of the respondents of this study consisted of 73.4% African; 21.1% belonged to the Indian ethnic group; 1.9% were of Coloured ethnicity; 3.3% of the White ethnic group; and 0.3% of the respondents did not wish to disclose their ethnicity (Fig 4.3).

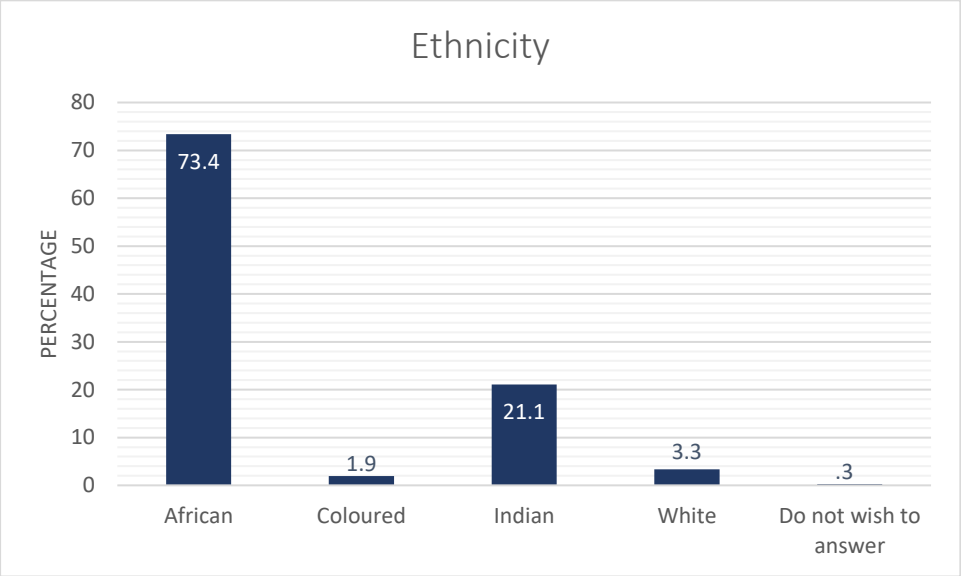

Fig. 4. 3: Ethnicity of the respondents

4.5.4 Tertiary institution of respondents

This study was carried out in two Pietermaritzburg tertiary institutions: UKZN and Umgungundlovu FET College, where 361 students were the respondents in this study. Of the valid questionnaires from both institutions, 74.2% were UKZN students and 25.8% were Umgungundlovu FET College students. (See Fig 4.4.)

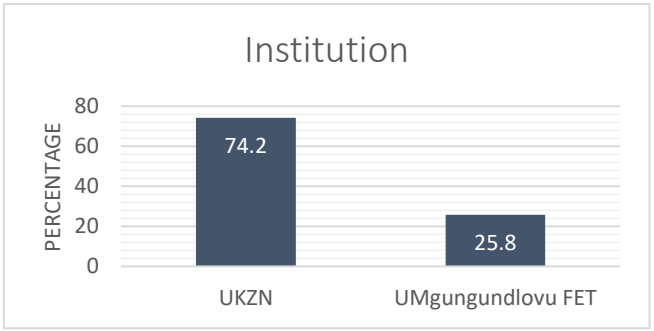

Fig. 4. 4: Respondents' respective institutions

4.5.5 Faculty

The study consisted of student respondents from varying disciplines. As seen in Fig 4.5, the results show that 39.3% were students from the Law and Management faculty; 26% from Social

Sciences; 25.5% from Science and Technology; 7.5% from Art and Drama; and 1.7% respondents were from Health Sciences. All of the above-mentioned faculties are found at UKZN, while Umgungundlovu FET students were from the Management and Science and Technology faculties.

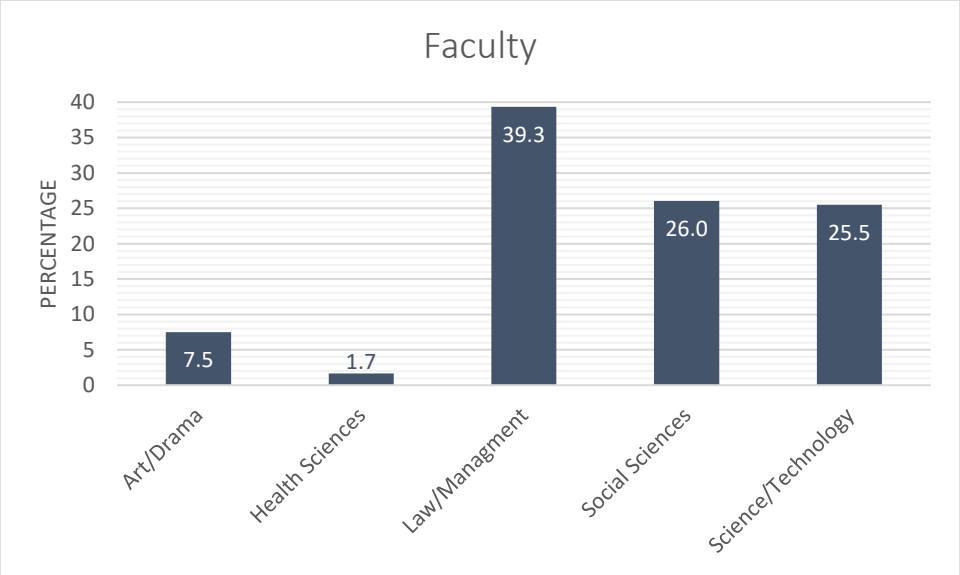

Fig. 4. 5: Faculty grouping of respondents

4.5.6 Awareness

To determine the awareness level of the respondents about online attacks, the respondents were required to categorise examples of online attacks with a given definition of the attack. If the respondents did not know the answer, there was an option for them to mark that they do not know.

The findings of this study for the phishing example showed that 30.5% categorised the example as an email spam; 20.2% of the respondents did not know the answer; 19.9% classified the given example as a phishing attack; 17.5% categorised the example as cyber-crime; 8.9% indicated that the example is identity theft and 3.0% noted the example as malware (A in Fig 4.6).

In the identity theft example for which the respondents had to select an answer, findings that revealed that 62.3% of students correctly identified it as identity theft (B in Fig 4.6). However, 15.8% classified it as cyber-crime; 14.7% of the respondents did not know the answer; 3.3% classifying it as a phishing attack; 2.8% categorised it as an email spam; leaving 1.1%

perceiving it to be malware. As presented in Fig 4.6 (C), the majority of the respondents (59.8%) identified the third example as cyber-crime, which was accurate. A further 17.7% of the students did not know the answer, with 8.3% considering malware as the answer. Also, 6.9% of the respondents indicated that the correct answer was identity theft and only 2.8% considered the example as a form of an email spam.

Another example provided was that of an email spam. The results showed that 37.7% of the respondents accurately identified the example as an email spam. However, 18% of the respondents did not know what form of attack the example was. Also, the smallest percentage (1.4%) of students thought it was an example of identity theft (D in Fig 4.6). The last example provided was a malware example. The findings show that the majority of respondents (42.4%) were able to correctly identify the example as malware. However, this was followed by 23.8% of students who did not know what type of attack it was. The lowest percentage (1.7%) of students categorised the example as identity theft (E in Fig 4.6).

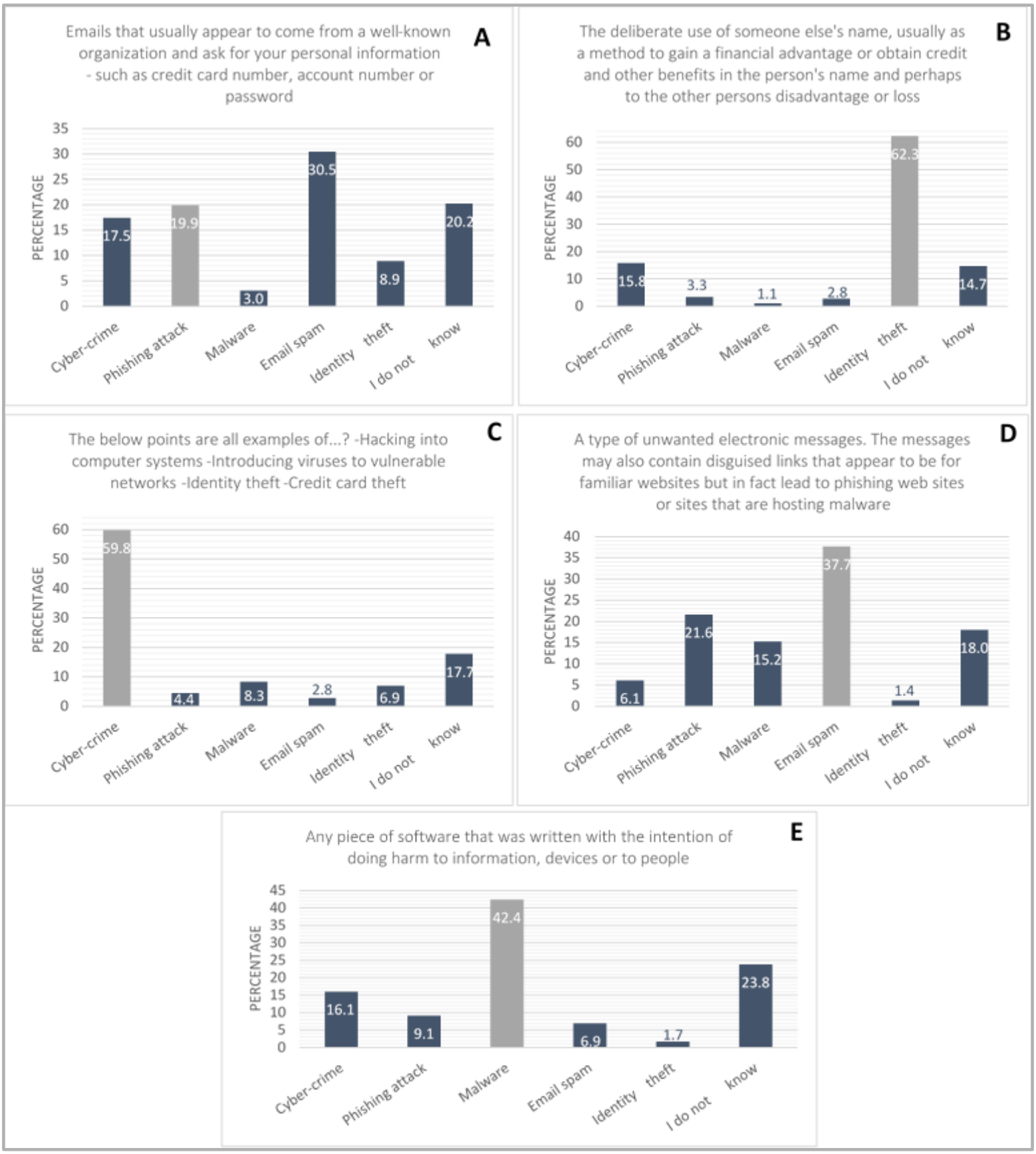

Fig. 4.6: Respondents' online attack awareness

4.6 Constructs used in this study

To address the framework used in this study, the respondents were asked questions that were aligned with the research constructs, namely attitude, subjective norm, behavioural intention and behaviour. The questions ranged from ordinal to nominal scaling. The responses obtained from the student respondents are as follows:

4.6.1 Attitude

To test attitude, a Likert scale of 'Strongly Agree' to 'Strongly Disagree', was used to rank the respondents' attitudes to, and perception of, the importance of online security (Refer to Appendix C and G.). Most respondents (83.4%) perceived online security as important, while 0.60% strongly disagreed that online security is important. The respondents were further asked whether they considered online security to be outside a user's control, and 36% of the students gave a neutral response, neither agreeing nor disagreeing. This response was followed by 20.2% of students that disagreed. The smallest percentage was 9.1%, who strongly disagreed that online security is outside the user's control. Regarding the students' concern about online security, 36.8% of students showed that they are strongly concerned about online security, while 10.2% strongly disagreed that online security is of concern to them. To understand the students' attitudes to information security, 64.5% of students were willing to be taught about information security, whereas 2.8% strongly disagreed that it was necessary.

4.6.2 Subjective norm

The responses given by students showed that 61.8% considered no threat when responding to an email from a known source (i.e. a friend or lecturer). Meanwhile, the remaining 38.2% had an opposing opinion. The findings also revealed that 83.9% of students have accepted a friend request on social media from someone they do not know, while 89.2% of students would respond to a social media request from someone they think they know. In another subjective norm question, it was evident that 49.9% of the respondents would not share their social network password with somebody close to them. However, 31% of the respondents indicated that they would share their password, provided they are convinced by the requester's response. A further 10% indicated that they would give somebody close their password and 9.1% also indicated that they would give the password by typing it in.

4.6.3 Behavioural intention

Young adult students were asked the same question, under different facilitating conditions, about an ordinary telephone call as compared to a telephone call where they stood a chance of winning something. Without verifying the caller, the students' responses to someone that they know showed that 93% of the students would provide their personally identifiable information (PII) over the telephone, knowing that they stand a chance to win something. Whereas, if there was nothing to be won, 90% of the students would provide their PII in a telephone call. Also, the findings showed that 91% of young adult students would send their PII to someone close, without verifying the sender, if they stood a chance to win something. If there was nothing to be won, 81% of students would send their PII without verifying the sender.

4.6.4 Behaviour

As shown in Appendix G, this construct was used to identify the young adults' online information security behaviour. The students' responses revealed that the majority of young adults (73.1%) use their actual names on social networks. The findings also showed that 58.2% of the students never change their social network passwords. To further understand the students' behaviour, they were asked if they have responded to an email message, link, online pop-up or social media message that they suspect was an attempt to get their personal details. Of the students, 33.8% have responded to a social media message; 21.6% have responded to an email message; 13.9% have responded to a link; and 11.6% have responded to an online pop-up. Also, the responses showed that only 21.1% of students attend to security alerts and 5% of the students do not know how to attend to such alerts.

4.7 Cross-tabulations

Cross-tabulations were used to identify existing gendered relationships between variables in this study. They were used to determine the gender relationships existing between the study variables and both males and females. According to Morgan, Leech, Gloeckner, and Barrett (2004), a cross-tabulation is a frequency distribution that further investigates the different variables. This study also employed the Chi-square test which was conducted to determine the significance of the relationships between variables. A Chi-square test generates a 'p' value that indicates whether the variable relationship is valid or not. A p value greater than 0.05 indicates that there is no relationship between the tested variables. Alternatively, if the p value is less

than 0.05 it is an indication that there exists a significant relationship between the tested variables.

4.7.1 Cross-tabulation between gender and phishing attack awareness

The cross-tabulation conducted between gender and phishing attack shows that 42 males (26.1%) identified the example to be a phishing attack and 30 females (15%) considered the example as a phishing attack example. The total number of both females and males that correctly identified the example was 19.9% (Table 4.2). However, 23.5% of females did not know the response and 16.1% of male respondents indicated that they do not know. The other respondents incorrectly identified the example provided: 33.5% of males and 28% of females identified the example as email spam. The majority of students (30.5%) identified the example as email spam rather than a phishing attack.

Table 4. 2: Cross-tabulation between gender and phishing attack awareness

			Emails that usually appear to come from a well-known organization and ask for your personal information - such asas credit card number, account number or password						
			Cyber-crime	**Phishing attack**	Malware	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	22	**42**	3	54	14	26	161
		% within Gender	13.7%	**26.1%**	1.9%	33.5%	8.7%	16.1%	100.0%
	Female	Count	41	**30**	8	56	18	47	200
		% within Gender	20.5%	**15.0%**	4.0%	28.0%	9.0%	23.5%	100.0%
Total		Count	63	**72**	11	110	32	73	361
		% within Gender	17.5%	**19.9%**	3.0%	30.5%	8.9%	20.2%	100.0%

The Chi-square test conducted for this cross-tabulation resulted in a ‘p’ value of 0.028. This signifies that there is a significant relationship between gender and phishing attack awareness. Males are more likely to be aware of phishing attacks than their female counterparts (Appendix G).

4.7.2 Cross-tabulation between gender and identity theft awareness

The gender responses for identifying identity theft example showed that 67% of males and 58.5% of females were able to correctly classify the example, leaving 62.3% of the overall 361

students able to identify the type of attack as identity theft (Table 4.3). A larger percentage (19%) of females did not know the attack type and 9.3% of males indicated that they did not know the correct answer, so 14.7% of the students did not know what type of attack the example was. However, 15.8% of the students (17.4% of males and 14.5% of females) identified the example as cyber-crime. The smallest number of students, consisting of 1.2% of males and 1% of females, thought the example was a malware attack.

Table 4. 3: Cross-tabulation between gender and identity theft awareness

			The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss						
			Cyber-crime	Phishing attack	Malware	Email spam	**Identity theft**	I do not know	Total
Gender	Male	Count	28	5	2	3	**108**	15	161
		% within Gender	17.4%	3.1%	1.2%	1.9%	**67.1%**	9.3%	100.0%
	Female	Count	29	7	2	7	**117**	38	200
		% within Gender	14.5%	3.5%	1.0%	3.5%	**58.5%**	19.0%	100.0%
Total		Count	57	12	4	10	**225**	53	361
		% within Gender	15.8%	3.3%	1.1%	2.8%	**62.3%**	14.7%	100.0%

The asymptotic significance of the above-mentioned correlation gave a ‘p’ value of 0.147. This indicates that there is no existing relationship between the two variables, gender and identity theft awareness. This implies that, irrespective of gender, students are familiar with what identity theft is.

4.7.3 Cross-tabulation between gender and cyber-crime awareness

The two variables, gender and cyber-crime were tested. The results, in Table 4.4 below, showed that more male students (68.3%) are aware of what cyber-crime is, compared to their female (53%) counterparts. Also, more female students (21.5%) indicated that they do not know what the provided example was. A smaller percentage of males (13%) also indicated that they did not know what type of attack the example was. However, it can be concluded that more males than females were aware of how cyber-crime manifests. Only a few of the students (4.5% of female and 0.60% of male students) mistook the example as email spam.

Table 4. 4: Cross-tabulation between gender and cyber-crime awareness

			The below points are all examples of...? -Hacking into computer systems -Introducing viruses to vulnerable networks -Identity theft -Credit card theft						
			Cyber-crime	Phishing attack	Malware	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	**110**	7	11	1	11	21	161
		% within Gender	**68.3%**	4.3%	6.8%	.6%	6.8%	13.0%	100.0%
	Female	Count	**106**	9	19	9	14	43	200
		% within Gender	**53.0%**	4.5%	9.5%	4.5%	7.0%	21.5%	100.0%
Total		Count	**216**	16	30	10	25	64	361
		% within Gender	**59.8%**	4.4%	8.3%	2.8%	6.9%	17.7%	100.0%

A Chi-square test applied to these two variables indicated that there is an existing relationship between gender and cyber-crime knowledge. The Chi-square test produced a 'p' value of 0.026. This relationship implies that male students are more aware of the cyber-crime.

4.7.4 Cross-tabulation between gender and email spam awareness

The cross-tabulation showed that more male students (42.9%) were able to correctly recognise the type of attack illustrated by the example. The findings showed that fewer male students (14.3%) did not identify the email spam example. On the other hand, fewer female students (33.5%) were able to associate the given example with the right attack type. More female (21%) than male students did not know what the correct response was. In total, 18% of the students, irrespective of gender, were unable to identify the example. It can be seen in Table 4.5, below, that the second largest percentage (21.6%) of students confused an email spam with a phishing attack.

The p value for the two tested variables was 0.199 for the Chi-square test. This implies that no significant relationship exists between gender and email spam awareness. Therefore, it can be deduced that both genders have the same knowledge of email spam (see Appendix G).

Table 4. 5: Cross-tabulation between gender and email spam awareness

			A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware						
			Cyber-crime	Phishing attack	Malware	**Email spam**	Identity theft	I do not know	Total
Gender	Male	Count	6	37	24	**69**	2	23	161
		% within Gender	3.7%	23.0%	14.9%	**42.9%**	1.2%	14.3%	100.0%
	Female	Count	16	41	31	**67**	3	42	200
		% within Gender	8.0%	20.5%	15.5%	**33.5%**	1.5%	21.0%	100.0%
Total		Count	22	78	55	**136**	5	65	361
		% within Gender	6.1%	21.6%	15.2%	**37.7%**	1.4%	18.0%	100.0%

4.7.5 Cross-tabulation between gender and malware awareness

As portrayed in Table 4.6, gender was cross-tabulated against malware. The findings of the cross-tabulation revealed that most male students (60.9%) were able to accurately associate the example with the form of attack. A low percentage (13%) of the male students indicated that they do not know the response, whereas most female students (32.5%) indicated that they did not know what form of attack the example was. The results showed that only 27.5% of female students responded with the accurate category. The lowest percentage (1.7%) of students specified that the example was identity theft. This percentage comprised of 2% female students and 1.2% of male students.

Table 4.6: Cross-tabulation between gender and malware awareness

			Any piece of software that was written with the intention of doing harm to information, devices or to people						
			Cyber-crime	Phishing attack	**Malware**	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	20	13	**98**	7	2	21	161
		% within Gender	12.4%	8.1%	**60.9%**	4.3%	1.2%	13.0%	100.0%
	Female	Count	38	20	**55**	18	4	65	200
		% within Gender	19.0%	10.0%	**27.5%**	9.0%	2.0%	32.5%	100.0%
Total		Count	58	33	**153**	25	6	86	361
		% within Gender	16.1%	9.1%	**42.4%**	6.9%	1.7%	23.8%	100.0%

The Chi-square test (p=0.00) highlighted an existing relationship between malware awareness and gender. The relationship implies that male students are more likely to identify a malware attack as they are knowledgeable about how a malware attacks manifest.

4.7.6 Cross-tabulation between gender and receiving and responding to an email message

This cross-tabulation was conducted to identify the number of students who have received email messages in a form of social engineering, and to identify which gender responds the most. The results showed that a higher percentage of male students (82%) have received emails that they believed were malicious in nature. Female students who had received similar email messages constituted 67.5%. Table 4.8 shows that, in as much as 74% (Table 4.7) of students received social engineering email messages, 78.4% of students did not respond. However, both male students (21.7%) and female students (25.2%) had similar response rates. As shown in Table 4.7 and Table 4.8, below, there was a higher percentage of students that have received malicious emails and most students, irrespective of gender, did not respond.

The Chi-square test conducted revealed an existing relationship between receiving a malicious email message and gender. Hence, the Chi-square test produced a 'p' value of 0.002. This implies that male students have higher chances of receiving social engineering attacks via emails. Further, the Chi-square test conducted between gender and responding to an email message that seems suspicious produced $p>0.05$, which showed that there is no existing relationship between responding to a malicious email message and gender (see Appendix G). The findings indicate that both female and male students are non-responsive towards emails that seem suspicious. This behaviour is believed to be due to the students' knowledge of phishing attacks.

Table 4. 7: Cross-tabulation between gender and receiving an email message

			Have you ever received an email message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	132	29	161
		% within Gender	82.0%	18.0%	100.0%
	Female	Count	135	65	200
		% within Gender	67.5%	32.5%	100.0%
Total		Count	267	94	361
		% within Gender	74.0%	26.0%	100.0%

Table 4. 8: Cross-tabulation between gender and responding to an email message

			Have you ever responded to an email message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	35	126	161
		% within Gender	21.7%	78.3%	100.0%
	Female	Count	43	157	200
		% within Gender	21.5%	78.5%	100.0%
Total		Count	78	283	361
		% within Gender	21.6%	78.4%	100.0%

4.7.7 Cross-tabulation between gender and receiving and responding to an online link

The results for this cross-tabulation showed that more male students (73.3%) suspected that they had received online links that they considered were attempts to obtain their personal details. On the other hand, 60.5% of female students also suspected that they had received such online links. As shown in Table 4.10, both genders had higher percentages (86.1%) of non-responsiveness to the suspicious online links; although, 15.5% of male students and 12.5% of female students responded to the links they received. More male students received and responded to the online links (Table 4.9 and Table 4.10).

The Chi-square test (Appendix G) conducted on gender and receiving suspicious online links yielded a p value of 0.011 which indicates an existing relationship. This indicates that male students are more likely to receive malicious links. However, the Chi-square test (p=0.408)

between gender and responding to online links indicated that no relationship existed. This implies that both male and female students' response rates are similar. There are no distinct differences towards responding to online links that are suspicious in nature.

Table 4. 9: Cross-tabulation between gender and receiving an online link

			Have you ever received a link that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	118	43	161
		% within Gender	73.3%	26.7%	100.0%
	Female	Count	121	79	200
		% within Gender	60.5%	39.5%	100.0%
Total		Count	239	122	361
		% within Gender	66.2%	33.8%	100.0%

Table 4. 10: Cross-tabulation between gender and responding to an online link

			Have you ever responded to a link that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	25	136	161
		% within Gender	15.5%	84.5%	100.0%
	Female	Count	25	175	200
		% within Gender	12.5%	87.5%	100.0%
Total		Count	50	311	361
		% within Gender	13.9%	86.1%	100.0%

4.7.8 Cross-tabulation between gender and receiving and responding to an online pop-up message

Gender was cross-tabulated against two variables, receiving and responding, in the behaviour construct. The cross-tabulations obtained between gender and receiving an online pop-up showed that males are perceived to receive more pop-up messages that were an attempt to

obtain their PI information. As shown in Table 4.11, 77.6% male students and 52.5% female students are convinced they have received questionable online pop-up messages. The response variable showed that most students (92.5% of females and 83.2% of males) did not respond to the online pop-ups (Table 4.12). However, some students (16.8% of males and 7.5% of females) did respond, irrespective of the online pop-up message being an attempt at obtaining their personal details, or not.

A Chi-square test result for gender and receiving suspicious online pop-up messages showed that there is a significant relationship, $p<0.05$ (Appendix G). This implies that receiving malicious pop-up messages is most common amongst male students. Further, the p value between gender and responding to pop-up messages produced a value of $p<0.05$. This value indicates that male students have higher chances of falling victim to online pop-up social engineering attempts since they are the most responsive gender.

Table 4. 11: Cross-tabulation between gender and receiving an online pop-up message

			Have you ever received an online pop-up that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	125	36	161
		% within Gender	77.6%	22.4%	100.0%
	Female	Count	105	95	200
		% within Gender	52.5%	47.5%	100.0%
Total		Count	230	131	361
		% within Gender	63.7%	36.3%	100.0%

Table 4. 12: Cross-tabulation between gender and responding to an online pop-up message

			Have you ever responded to an online pop-up that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	27	134	161
		% within Gender	16.8%	83.2%	100.0%
	Female	Count	15	185	200
		% within Gender	7.5%	92.5%	100.0%
Total		Count	42	319	361
		% within Gender	11.6%	88.4%	100.0%

4.7.9 Cross-tabulation between gender and receiving and responding to a social media message

Table 4.13 below presents the cross-tabulation between gender and receiving a social engineering social media message. The table presents findings that show a relatively high percentages of students that claim to have received deceptive messages on social networks. Female students (78.5%) receive more social engineering messages than male students (70.8%). The overall percentage of students that receive deceptive social media messages was 75.1%, as seen in Table 4.13. To test the percentage of gender responses, a cross-tabulation between the response rate and gender was conducted. This showed that female students (41.5%) respond the most to social media messages that have malicious intentions. The percentage of male students that have responded to such messages was 24.2%. Furthermore, the results of both genders showed that 75.8% of male students and 58.5% of female students have not responded to the messages; while an overall 33.8% (Table 4.14) of the students respond to the messages.

A p value of 0.93 was produced by the Chi-square test for gender and receiving social media messages that were perceived to be malicious (Appendix G). This implies that malicious social media messages received are non-gender-dependent. Also, the Chi-square test for gender and responsiveness to the suspicious social media messages yielded a value p=0.001. As seen in Appendix G, the value confirms that the response rate is gender-dependent. This implies that female students are more than likely to fall victim to social engineering attempts which are conducted over social networks.

Table 4. 13: Cross-tabulation between gender and receiving a social media message

			Have you ever received a social media message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	114	47	161
		% within Gender	70.8%	29.2%	100.0%
	Female	Count	157	43	200
		% within Gender	78.5%	21.5%	100.0%
Total		Count	271	90	361
		% within Gender	75.1%	24.9%	100.0%

Table 4. 14: Cross-tabulation between gender and responding to a social media message

			Have you ever responded to a social media message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	39	122	161
		% within Gender	24.2%	75.8%	100.0%
	Female	Count	83	117	200
		% within Gender	41.5%	58.5%	100.0%
Total		Count	122	239	361
		% within Gender	33.8%	66.2%	100.0%

4.7.10 Cross-tabulation between gender and online security perceptions

Students' responses to the importance of online security showed that the majority of students (86.3% of males and 81% of females) considered online security important. However, there were a few female students (1.0%) who considered online security unimportant by indicating on the 'strongly disagree' option. It is important to note that the students had an option of 'disagree', but none of the students took this option (Table 4.15). The Chi-square test conducted for this question revealed that the attitude to security importance has a significant relationship with gender. This was concluded by the significant value p=0.022 (see Appendix G) from the Chi-square analysis, and supported by the cross-tabulation results, which implies that males are the gender that perceive online security to be important. Also, a cross-tabulation conducted between gender and the perceived necessity for online security showed that 71.5% of students, consisting of 74.5% male and 69% female student, do consider online security necessary (Table 4.16). The significance value produced indicated that there is no relationship between gender and perceived necessity for online security. This suggests that both male and female students find online security necessary.

Table 4. 15: Cross-tabulation between gender and online security

			Online security is important				
			Strongly Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	0	4	18	139	161
		% within Gender	0.0%	2.5%	11.2%	86.3%	100.0%
	Female	Count	2	0	36	162	200
		% within Gender	1.0%	0.0%	18.0%	81.0%	100.0%
Total		Count	2	4	54	301	361
		% within Gender	.6%	1.1%	15.0%	83.4%	100.0%

Table 4. 16: Cross-tabulation between gender and necessity for online security

			Online security is necessary					
			Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	1	2	3	35	120	161
		% within Gender	.6%	1.2%	1.9%	21.7%	74.5%	100.0%
	Female	Count	1	1	8	52	138	200
		% within Gender	.5%	.5%	4.0%	26.0%	69.0%	100.0%
Total		Count	2	3	11	87	258	361
		% within Gender	.6%	.8%	3.0%	24.1%	71.5%	100.0%

The majority of the student respondents (35.7%) were neutral as to whether online security is outside the user's control (Table 4.17). Male students had a stronger sense of agreement ('strongly agree' = 12.4% and 'agree' = 23%) and disagreement ('strongly disagree' = 6.2% and 'disagree' = 24.8%) whether online security is outside a user's control, while 37.5% of female students were more neutral in their responses. The Chi-square test conducted to assess the relationship between gender and whether online security is outside the user's control resulted in a significant value (0.034, as shown in Appendix G). The p value suggests that male students are more aware of the users' control in online security.

Table 4. 17: Cross-tabulation between gender and user control of online security

			Online security is necessary					
			Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	1	2	3	35	120	161
		% within Gender	.6%	1.2%	1.9%	21.7%	74.5%	100.0%
	Female	Count	1	1	8	52	138	200
		% within Gender	.5%	.5%	4.0%	26.0%	69.0%	100.0%
Total		Count	2	3	11	87	258	361
		% within Gender	.6%	.8%	3.0%	24.1%	71.5%	100.0%

A further cross-tabulation was conducted between gender and online security. The results of the respondents concerning online security were tabulated in Table 4.18, below. The table shows that female students are more concerned about online security than males. Based on the findings, 37.5% and 30.5% of female students noted that they strongly disagree and disagree, respectively, with the question posed. The majority of male students also indicated that they have a concern about online security ('strongly disagree' = 35.4% and 'disagree' = 29.2%). The Chi-square test produced a value greater than 0.05. The results show that there is no relationship between gender and online security concerns. This implies that both female and male students have similar concerns about online security.

Table 4. 18: Cross-tabulation between gender and online security concern

			I am not concerned about online security					
			Strongly Disagree	Disagree	Neutral	Agree	Stronlgy Agree	Total
Gender	Male	Count	57	47	25	15	17	161
		% within Gender	35.4%	29.2%	15.5%	9.3%	10.6%	100.0%
	Female	Count	75	61	21	21	22	200
		% within Gender	37.5%	30.5%	10.5%	10.5%	11.0%	100.0%
Total		Count	132	108	46	36	39	361
		% within Gender	36.6%	29.9%	12.7%	10.0%	10.8%	100.0%

The cross-tabulation conducted between gender and responding to a sender, provided the source is unknown or the source is a friend, showed that most students are concerned (Table 4.19 and Table 4.20). As shown in Table 4.19, 53.2% of students (54% of males and 52.5% of

females) are very ('strongly') concerned and 24.1% of students (23.6% of males and 24.5% of females) are somewhat concerned when responding to an unknown source. Further findings, in Table 4.20, showed that 14.4% (18% of males and 11.5% of females) of students are very concerned and 24.4% of students are somewhat concerned (26.7% of males and 22.5% of females) about online security when responding to a friend. However, the results show that there is less concern about online security when the both genders are responding to a friend. Both Chi-square tests conducted against gender and security concerns when responding to a friend and to an unknown source yielded non-significant relationships (Appendix G). This suggests that being concerned about online security when responding to a known or unknown individual has no relationship with the gender variable. So students have online security concerns, irrespective of their gender.

Table 4. 19: Cross-tabulation between gender and online security concern when responding to an unknown source

			I am concerned about online security when responding to an unknown source					
			Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	13	5	18	38	87	161
		% within Gender	8.1%	3.1%	11.2%	23.6%	54.0%	100.0%
	Female	Count	17	13	16	49	105	200
		% within Gender	8.5%	6.5%	8.0%	24.5%	52.5%	100.0%
Total		Count	30	18	34	87	192	361
		% within Gender	8.3%	5.0%	9.4%	24.1%	53.2%	100.0%

Table 4. 20: Cross-tabulation between gender and online security concern when responding to a friend

			I am not concerned about online security when responding to a friend					
			Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	27	25	37	43	29	161
		% within Gender	16.8%	15.5%	23.0%	26.7%	18.0%	100.0%
	Female	Count	45	44	43	45	23	200
		% within Gender	22.5%	22.0%	21.5%	22.5%	11.5%	100.0%
Total		Count	72	69	80	88	52	361
		% within Gender	19.9%	19.1%	22.2%	24.4%	14.4%	100.0%

4.7.11 Cross-tabulation between gender and information security-related principles

To understand the effect of gender on attitudes to information security, various cross-tabulations were conducted. In a cross-tabulation to identify the gender differences in attitudes to online privacy, the majority of the students (55.3% of males and 49.5% of females) considered protection of their information to be the reason why online privacy exits. However, a few students (7% of females and 5% of males) stated that they did not know the reason behind online privacy on social networks. A similar response was given by both genders (29.2% of males and 28% of females) who considered online privacy important as a mechanism to prevent identity theft (Table 4.21). A further 15.5% of females and 10.6% of males believed that online privacy on social networks is for hiding their images and contact information from unknown sources. The Chi-square p value produced was 0.414, which indicated a non-significant relationship (Appendix G). Therefore, understanding the importance of online privacy is not gender-dependent. Both male and female students have similar perceptions about the reasons behind the importance of online privacy.

Table 4. 21: Cross-tabulation between gender and perceptions of the importance of online privacy

			Which of the options presented do you believe represents the most important reason behind online privacy on social networks				
			Prevention of Identity Theft	Protection of my Information	Hiding my Image and contact info from unknowns	I dont know	Total
Gender	Male	Count	47	89	17	8	161
		% within Gender	29.2%	55.3%	10.6%	5.0%	100.0%
	Female	Count	56	99	31	14	200
		% within Gender	28.0%	49.5%	15.5%	7.0%	100.0%
Total		Count	103	188	48	22	361
		% within Gender	28.5%	52.1%	13.3%	6.1%	100.0%

To ascertain whether gender influenced opinions regarding safeguarding of online information, a cross-tabulation tab was conducted between gender and the actions they believed could help secure their information on online sites. Appendix G shows that 66.5% of male, and 61.5% of female, students considered installing an antivirus as a measure to help secure their online information. However, the second highest percentage of students (23% of males and 21% of females) indicated that they did not know which of the presented options would help them in protecting their online information. Also, as seen in Appendix G, more female students (14.5%) than male students (6.2%) specified that not changing their password is a technique that can help in safeguarding their online information. To determine any existing relationships, the Chi-square test was conducted. The results of the test showed that there is no existing relationship between gender and approaches to safeguarding information on social media, since the p value from the Chi-square test had a value of 0.085. Therefore, male and female students have similar opinions about the correct and incorrect methods of safeguarding their information.

A further information security-related cross-tabulation was conducted between gender and the students' opinions of the least suitable ways of securing a password. A similar percentage of both males (62.1%) and females (62%) said they understand that writing down a password was not a good way to secure a password (Appendix G), while 19.9% of males and 15.5% of females noted that memorising a password is not a secure way to secure that password. A further 13% of female and 11.8% of male students also indicated that it is not safe practice to write down a password and leave it in a secured place with no title, or information of what the

password is for. However, 9.5% of female and 6.2% of male students indicated that they do not know which practice is not appropriate for securing their passwords. The Chi-square test showed that there is no relationship between gender and unsuitable ways of securing passwords.

A cross-tabulation was conducted between gender and behaviour when someone close requests a social network password (see Appendix G). It was evident that 54% of male students and 46.5% of female students would not give their partner any of their social media passwords. However, 33.5% of female and 28% of male students would give their passwords to their partners after asking questions and receiving convincing responses. Also, 10.6% of male and 8% of female students would provide their passwords by typing them in; whereas 12% of females and 7.5% of males would give their partners their social network passwords. The p value produced was 0.222, which means that there is no relationship between gender and sharing a social network password with someone close.

Table 4.22, below, shows the cross-tabulation between gender and the students' concern for their information being accessed by third parties without their knowledge. Most students indicated that they were very concerned about their information being accessed by third parties. The majority of the students who were very concerned consisted of 48% of female and 47.8% of male students. These results were followed by 28.6% of male and 26% of female students, who indicated that they were, to a certain degree, concerned about their information being accessed by a third party. Nevertheless, 20.2% of the respondents (20.5% of males and 20% of females) were not too concerned; and 4.7% of the students (6% of females and 3.1% of males) were not at all concerned. The Chi-square results showed that there was no relationship ($p = 0.612$) (Appendix G) between gender and concern for information being accessible to third parties without one's knowledge.

Table 4. 22: Cross-tabulation between gender and online security concern

			How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge				
			Not at all concerned	Not too concerned	Somewhat concerned	Very concerned	Total
Gender	Male	Count	5	33	46	77	161
		% within Gender	3.1%	20.5%	28.6%	47.8%	100.0%
	Female	Count	12	40	52	96	200
		% within Gender	6.0%	20.0%	26.0%	48.0%	100.0%
Total		Count	17	73	98	173	361
		% within Gender	4.7%	20.2%	27.1%	47.9%	100.0%

Gender was cross-tabulated against when students last changed their privacy settings on social networks (Table 4.23). The results indicated that 37% of females and 26.7% of males changed their privacy settings after having a profile for a while. A further 30.4% of male, and 22.5% of female, students indicated that they changed their privacy settings after they had worked out how to change them; whereas 5.3% of students (7% of females and 3.1% of males) indicated that they did not know how to change their privacy settings on social networks. Also, 18.5% of female and 16.1% of male students indicted that they had never changed their privacy settings on social network sites; while 18.8% (23.6% of males and 15% of females) specified that they changed their social network privacy settings right at the beginning of their profile creation. The two variables, gender and changing of privacy setting on social networks, resulted in a significant p value of 0.022. The relationship is interpreted to mean that male students have a better understanding of the importance of changing their privacy settings on social networks.

Table 4. 23: Cross-tabulation between gender and change of privacy settings on social network sites

			When did you change your privacy settings on social networks since creating your profile					
			I do not know how to	I have never changed the settings	After having a profile for a while	After I figured out how to	Right at the beginning	Total
Gender	Male	Count	5	26	43	49	38	161
		% within Gender	3.1%	16.1%	26.7%	30.4%	23.6%	100.0%
	Female	Count	14	37	74	45	30	200
		% within Gender	7.0%	18.5%	37.0%	22.5%	15.0%	100.0%
Total		Count	19	63	117	94	68	361
		% within Gender	5.3%	17.5%	32.4%	26.0%	18.8%	100.0%

A cross-tabulation was conducted between gender and the last time that students changed their privacy settings on their email accounts. This showed that most students (27.7%; 31% of females and 23.6% of males) had changed their email settings after having the email account for some time. A further 23.8% of students (26.1% of males and 22% of females) changed their settings after they had worked out how to; and 23.5% of the students (25% of females and 21.7% of males) had never changed their privacy settings. Moreover, 23% of male and 13.5% of female students changed their email privacy settings right at the beginning, after opening an email account. Additionally, 8.5% of female and 5.6% of male students indicated that they did not know how to change their privacy settings on their email accounts. The Chi-square results showed that there was no relationship between gender and changing of privacy settings on email accounts. The p value produced was 0.079.

A cross-tabulation between gender and whether students would like to be taught about information security was conducted. The responses given by students are displayed in Table 4.24. The table shows that both male and female students are willing to be taught about information security. The percentage of female students (66.5% = ‘strongly agree’ and 22.5% = ‘agree’) willing to be taught about information security was slightly higher than for the male students (62.1% = ‘strongly agree’ and 21.7% = ‘agree’). Only a few students across both genders denied having an interest in being taught about information security: 2.8% = ‘strongly disagree’ and 2.2% = ‘disagree. Furthermore, 11.2% of males and 6% of females gave neutral responses.

Table 4. 24: Cross-tabulation between gender and online security learning

			I would like to be taught about information security					
			Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Gender	Male	Count	5	3	18	35	100	161
		% within Gender	3.1%	1.9%	11.2%	21.7%	62.1%	100.0%
	Female	Count	5	5	12	45	133	200
		% within Gender	2.5%	2.5%	6.0%	22.5%	66.5%	100.0%
Total		Count	10	8	30	80	233	361
		% within Gender	2.8%	2.2%	8.3%	22.2%	64.5%	100.0%

The cross-tabulation produced a p value of 0.485, which indicates that no relationship between gender and the willingness to learn about information security exists. Thus, it can be inferred that male and female students are both interested in learning about information security.

4.7.12 Cross-tabulations between gender and responding to a random email message

A cross-tabulation was conducted between gender and responses to a random email message in a given circumstance. The cross-tabulation showed that 49.7% of male students and 37.5% of female students would verify the sender before providing their PII in a random email message. The majority of the female students (62.5%) and 50.3% of male students would not verify the sender before providing their PII (Table 4.25). The Chi-square test produced a p value of 0.02, which implies a relationship between gender and verifying the sender before responding, namely, that verifying the sender before responding is less likely to occur amongst female students. On the other hand, a cross-tabulation of the same concept was conducted to determine the gender response rate, provided they are going to win something (Appendix G). The cross-tabulation showed that 54% of female and 52.8% of male students would not verify the sender; whereas, 47.2% of male and 46% of female students would verify the sender before responding. The Chi-square test produced a value of p=0.820, which indicated that there is no relationship between gender and verifying the sender if students are to win something (see Appendix G). This is interpreted to mean that both female and male students respond in a similar manner if they are going to win something.

Table 4. 25: Cross-tabulation between gender and verifying the sender of a random email message

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you verify the sender		
			Yes	No	Total
Gender	Male	Count	80	81	161
		% within Gender	49.7%	50.3%	100.0%
	Female	Count	75	125	200
		% within Gender	37.5%	62.5%	100.0%
Total		Count	155	206	361
		% within Gender	42.9%	57.1%	100.0%

Table 4.26 shows the results from a cross-tabulation to determine the gender response of both female and male students to whether they would respond without verifying the sender. The cross-tabulation results showed that the majority of the students (95% of females and 93.2% of males) would not respond without verifying the sender. The remaining students (6.8% of males and 5% of females) indicated that they would respond with their PII without verifying the sender. The Chi-square test (p=0.46) found no relationship between gender and responding without verifying (refer to Appendix G). However, when a similar cross-tabulation was conducted between gender and the response rate if the students were to win something, the likelihood of responding without verifying the sender increased. Appendix G shows that 12.5% of female and 11.8% of male students would respond to the email message without verifying the sender. However, the majority of both male (88.2%) and female (87.5%) students would not respond without verifying the sender. The Chi-square test conducted between gender and responding without verifying the sender, if students were going to win something, showed no relationship (p=0.840) between the two variables. This implies similar behaviour from males and females, regarding not verifying the sender, if the students were going to win something.

Table 4. 26: Cross-tabulation between gender and responding without verifying the sender of a random email message

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you respond without verifying the sender		
			Yes	No	Total
Gender	Male	Count	11	150	161
		% within Gender	6.8%	93.2%	100.0%
	Female	Count	10	190	200
		% within Gender	5.0%	95.0%	100.0%
Total		Count	21	340	361
		% within Gender	5.8%	94.2%	100.0%

Gender was further cross-tabulated against responding after verifying the email sender. The cross-tabulation showed that most students (81% of females and 63.4% of males) would not respond to the email, even after verifying the sender, while 36.6% of male and 19% of female students would respond to the email with their PII after verifying the sender (Table 4.27, Appendix G). The Chi-square test generated a p value of 0.000, which implies that there is a relationship between gender and responding to an email after verifying the sender. Furthermore, the findings suggest that female students are less responsive after verifying the sender, whereas, male students are more responsive after verifying the sender. This implies that male students have a higher likelihood of falling victim through email messages if the social engineers use impersonation. Another cross-tabulation was conducted between gender and response rates after verifying the sender, if students knew they stood a chance to win something. As seen in Table 4.28, more female students (77%) would not respond with their PII, compared to male students (65.2%). The findings showed that 34.8% of male, and 23% of female, students would respond with their information after verifying the sender of the email. A Chi-square test was conducted between gender and the response rates of students to a random email message if they were to win something. A significance value of 0.013 for p was produced, which implies a relationship between the two variables. Therefore, it can be concluded that male students' higher response rates make them more vulnerable to social engineers. This implies that male students have a higher chance of falling victim to social engineering attempts in email messages, if something were to be won.

Table 4. 27: Cross-tabulation between gender and responding after verifying the sender of a random email message

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, after verifying the sender would you respond		
			Yes	No	Total
Gender	Male	Count	59	102	161
		% within Gender	36.6%	63.4%	100.0%
	Female	Count	38	162	200
		% within Gender	19.0%	81.0%	100.0%
Total		Count	97	264	361
		% within Gender	26.9%	73.1%	100.0%

Table 4. 28: Cross-tabulation between gender and responding after verifying the sender of a random email message when something will be won

			Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, after verifying the sender would you respond		
			Yes	No	Total
Gender	Male	Count	56	105	161
		% within Gender	34.8%	65.2%	100.0%
	Female	Count	46	154	200
		% within Gender	23.0%	77.0%	100.0%
Total		Count	102	259	361
		% within Gender	28.3%	71.7%	100.0%

4.7.13 Cross-tabulations between gender and responding to an email from someone close

Table 4.29 presents the results of a cross-tabulation conducted between gender and whether female and male students would or would not verify the sender. The cross-tabulation results showed that the majority of the students (57.8% of male and 53% of female students) would not verify the sender. Whereas, the rest of the students, 47% of female and 42.2% of male students would verify the sender. The Chi-square test produced a significant value of p=0.366, which means that there is no relationship between the two variables. This implies that students, males and females, behave in a similar manner when verifying, or not verifying, someone close who is emailing them. On the other hand, a cross-tabulation was conducted to determine the

effect of gender when verifying an email sender, supposedly from someone close, provided the student stood a chance to win something. The results showed an increasing number of female students (55.5%) who would not verify the sender; whereas, more male respondents would verify the sender (49.7%). The Chi-square test showed that there was no relationship (p=0.326) between gender and verifying, or not verifying, the sender if there was something to be won. This suggests that male and female students react in a similar manner to email messages that come from someone close, when they stand a chance of winning something.

Table 4. 29: Cross-tabulation between gender and verifying if it is someone close

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you verify the sender		
			Yes	No	Total
Gender	Male	Count	68	93	161
		% within Gender	42.2%	57.8%	100.0%
	Female	Count	94	106	200
		% within Gender	47.0%	53.0%	100.0%
Total		Count	162	199	361
		% within Gender	44.9%	55.1%	100.0%

A cross-tabulation was conducted to determine whether gender influenced behaviour when responding, without verifying, to an email from someone close. Table 4.30 shows that 30.4% of male, and 16% of female, students would not verify the sender before responding. Furthermore, the cross-tabulation showed that more females (84%) than their male (69.6%) counterparts would not respond without verifying the sender. The Chi-square test conducted for gender and whether the students would respond without verifying the sender resulted in a p value of 0.001. This implies that there is a relationship between gender and responding without verifying the sender. It can be concluded that male students are more likely to fall victim if social engineers use identity theft to email them. This further means that female students are less likely to respond with their PII as they understand the value of their personal information. However, if there is something to be won, female students (26.5%) would respond more, without verifying the sender; while more male students (76.4%) would verify the sender. The Chi-square test produced a p=0.529, indicating no relationship between gender and responding to someone close, if there is something to be won. This suggests that the behaviour

of male and female students is similar when responding to someone close, despite standing a chance to win something.

Table 4. 30: Cross-tabulation between gender and response without verifying that it is someone close

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you respond without verifying the sender		
			Yes	No	Total
Gender	Male	Count	49	112	161
		% within Gender	30.4%	69.6%	100.0%
	Female	Count	32	168	200
		% within Gender	16.0%	84.0%	100.0%
Total		Count	81	280	361
		% within Gender	22.4%	77.6%	100.0%

A cross-tabulation was conducted to determine the percentage of students that would only respond after verifying the email sender (Table 4.31). The cross-tabulation conducted between gender and whether students would respond after verifying showed that most students would not respond; and 69% of female and 68.9% of male students would not respond with their PII, even after verifying the sender. However, a similar percentage of both genders (31.1% male and 31% female) would respond with their information after verifying the sender. The p value produced by the Chi-square test was p=0.991 (see Appendix G), which indicates no relationship between gender and response after verifying the sender. Nevertheless, when students stand a chance to win something the response behaviour changes. In a cross-tabulation between gender and whether students would respond if they stood a chance to win something, it was evident that 69.5% of female and 61.5% of male students would not respond to the sender, even after verifying the email sender. However, there was an increase in the percentage of male students (38.5%) that would respond after verifying the sender, as compared to female students (30.5%). According to the Chi-square test, p=0.110 for the two variables. This indicates that there is no apparent relationship between gender and response after verifying the sender.

Table 4. 31: Cross-tabulation between gender and response after verifying if it is someone close

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, after verifying the sender would you respond		
			Yes	No	Total
Gender	Male	Count	50	111	161
		% within Gender	31.1%	68.9%	100.0%
	Female	Count	62	138	200
		% within Gender	31.0%	69.0%	100.0%
Total		Count	112	249	361
		% within Gender	31.0%	69.0%	100.0%

4.7.14 Cross-tabulation between gender and responding to a direct message on social media

A cross-tabulation conducted between gender and whether students verify a sender on social media showed that most students do not verify a sender of a direct message on social media. Table 4.31 shows that 60.2% of male, and 56.5% of female, students would not verify the sender. Whereas, 43.5% of female, and 39.8% of male, students would verify the sender. A Chi-square test was also conducted for the two variables, and it resulted in a p value of 0.473 (Appendix G). This means that there is no relationship between gender and verifying a sender of a direct message on social media. The results also indicate that there is no distinct difference in behaviour for male and female students, for the tested variables. To identify if there is a difference in behaviour if students stood a chance to win something, a further cross-tabulation was constructed. The two variables tested were gender and whether students would verify the sender of a direct social media message, provided they stood a chance to win something. As shown in Table 4.32, the gender behaviour is similar. However, the percentage of males who would not verify significantly decreases to 55.3%. On the other hand, 44.7% of male, and 44% of female, students would verify the sender of the online message. The Chi-square test conducted generated a significance value of 0.891, indicating no relationship between gender and verifying the sender of a message on social media.

Table 4. 32: Cross-tabulation between gender and verifying the social media message sender

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you verify the sender		
			Yes	No	Total
Gender	Male	Count	64	97	161
		% within Gender	39.8%	60.2%	100.0%
	Female	Count	87	113	200
		% within Gender	43.5%	56.5%	100.0%
Total		Count	151	210	361
		% within Gender	41.8%	58.2%	100.0%

To test whether students do respond to social media direct messages without verifying the sender, gender was cross-tabulated against whether students would respond without verifying the sender. The results showed that the majority of students would not respond with their PII without verifying the sender. As shown in Table 4.33, 92.5% of female, and 78.3% of male, students would not respond with their PII without verifying the sender. Yet, 21.7% of male, and 7.5% of female, students would send their information without verifying the sender. A Chi-square test was conducted and produced an asymptotic value of p=0.000. This signifies a relationship between gender and response rate without verifying the sender. The relationship suggests that females are less likely to send their PII, compared to male students. Therefore, male students have higher chances of falling victim on social networks since they do not verify the sender prior to sending their PII. Moreover, to identify any gender-dependent differences in behaviour if students stood a chance to win something, a cross-tabulation was conducted. The tested variables were gender and whether students would respond without verifying, if they had a possibility of winning something. As shown in Appendix G, most students (88% of females and 86.3% of males) would not respond without verifying the sender, even though they stood a chance of winning something. The value of p produced by the Chi-square test was 0.637, which implies no relationship between gender and responding without verifying the social media sender (Appendix G). Therefore, response behaviours to social media messages when something is to be won, are not gender-dependent.

Table 4. 33: Cross-tabulation between gender and responding without verifying the social network sender

			Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you respond without verifying the sender		
			Yes	No	Total
Gender	Male	Count	35	126	161
		% within Gender	21.7%	78.3%	100.0%
	Female	Count	15	185	200
		% within Gender	7.5%	92.5%	100.0%
Total		Count	50	311	361
		% within Gender	13.9%	86.1%	100.0%

Gender was further cross-tabulated against whether students would send their information after verifying the sender (see Appendix G). The cross-tabulation showed that more female students (78.5%), than male students (72.7%), would not respond with their PII to a direct social media message; while 27.3% of male, and 21.5% of female, students would respond to a social media message with their information. The variables – gender and whether students would respond with their PII – were further tested using a Chi-square test. The test showed that there is no relationship between the two variables, since p=0.198. To further identify a gender difference in response if students knew they stood a chance of winning something, a cross-tabulation between the two variables was completed. Table 4.34 presents the results that show that 77.5% of female, and 66.5% of male, students would not respond to the social media message after verifying the sender. However, other students (33.5% of males and 22.5% of females) would respond with their PII after verifying the social media sender. As seen in Appendix G, a Chi-square test produced a significance value of p=0.019 for gender and responding after verifying the sender when there is something to be won. The results suggest that a relationship exists. In this instance, the relationship implies that male students respond more after verifying the sender, if they stand a chance of winning; whereas, female students are not responsive to social media messages, regardless of verifying the sender. Therefore, male students are more susceptible to falling victim on social networks if there is something to be won since they willingly provide their PII.

Table 4. 34: Cross-tabulation between gender and response after verifying the social network message sender when something will be won

			Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, after verifying the sender would you respond		
			Yes	No	Total
Gender	Male	Count	54	107	161
		% within Gender	33.5%	66.5%	100.0%
	Female	Count	45	155	200
		% within Gender	22.5%	77.5%	100.0%
Total		Count	99	262	361
		% within Gender	27.4%	72.6%	100.0%

4.7.15 Cross-tabulation between faculty and phishing awareness

To gain an understanding of the level of awareness, based on each faculty, a cross-tabulation was carried out between the two variables. Table 4.35 shows the phishing example that was posed to the respondents. The findings showed that 29.3% of students from Science and Technology were able to correctly identify the example. Also, 19.7% of students from Law and Management Studies, 14.9% of students from Social Sciences and 11.1% of students from Art and Drama accurately classified the given example. However, no student from Health Sciences was able to accurately identify the provided example. Furthermore, the Health Sciences students, consisting of 50% of both male and female students, indicated that they do not know the attack type. Also, 26.6% of students from Social Sciences, 25.9% of students from Art and Drama and 17.6% of students from Law and Management indicated that they did not know the answer to the given example. Science and Technology students had the second lowest percentage (14.1%) of students who said that they did not know the answer. A Chi-square test, giving a significance value p=0.162, showed that there was no relationship between faculty and phishing awareness. This shows that, regardless of the faculty, students lack awareness about the different types of online attacks. Therefore, awareness campaigns need to be driven across all faculties as there are students in Science, Technology, Engineering and Mathematics (STEM) who do not know about social engineering attacks.

Table 4. 35: Cross-tabulation between faculty and phishing awareness

			Emails that usually appear to come from a well-known organization and ask for your personal information - such as credit card number, account number or password						
			Cyber-crime	Phishing attack	Malware	Email spam	Identity theft	I do not know	Total
Faculty	Art/Drama	Count	5	3	0	10	2	7	27
		% within Faculty	18.5%	11.1%	0.0%	37.0%	7.4%	25.9%	100.0%
	Health Sciences	Count	0	0	0	3	0	3	6
		% within Faculty	0.0%	0.0%	0.0%	50.0%	0.0%	50.0%	100.0%
	Law/Management	Count	25	28	8	45	11	25	142
		% within Faculty	17.6%	19.7%	5.6%	31.7%	7.7%	17.6%	100.0%
	Social Sciences	Count	16	14	0	29	10	25	94
		% within Faculty	17.0%	14.9%	0.0%	30.9%	10.6%	26.6%	100.0%
	Science/Technology	Count	17	27	3	23	9	13	92
		% within Faculty	18.5%	29.3%	3.3%	25.0%	9.8%	14.1%	100.0%
Total		Count	63	72	11	110	32	73	361
		% within Faculty	17.5%	19.9%	3.0%	30.5%	8.9%	20.2%	100.0%

4.7.16 Cross-tabulation between gender, ethnicity and online security concern

A cross-tabulation was carried out between three variables, namely gender, ethnicity and online security concern (refer to Appendix G). The objective of the cross-tabulation was to identify gender differences in attitudes to online security, based on race. The findings showed that the most concerned students were White female students (77.8%), followed by White male students (66.7%), who were equally as concerned as Indian female students (66.7%). Also, African male student (56%) were strongly concerned, as well as 50% of Indian male students and 49.4% of female African students. A male respondent, who did not wish to specify his race, noted that he was very concerned (100%) about online security. However, it is important to note that Coloured male students (0%) showed no concern about online security when responding to an unknown source; whereas Coloured female students (20%) showed a greater concern. Furthermore, the results showed that Coloured students (50% of males and 20% of females) are the least concerned of the ethnic groups. Also, small percentages of African students (9% females and 7.3% males), Indian students (8.7% males and 3.3% females) and White students (11.1% females) indicated that they are not concerned about online security when responding. A Chi-square test was conducted for the variables and all the test results

produced p>0.05, which signified no relationships between the tested variables. The results suggest that online security concern exists across all genders and races.

4.8 Summary of gender-dependent results

Below is a high-level overview of the gender differences identified in this study. These relationships of the existing correlations are supported by Chi-square tests that provided a p value less than 0.05.

4.8.1 Awareness:

- Phishing knowledge
- Cybercrime knowledge
- Malware knowledge

4.8.2 Receiving and responding to random SE messages

- Receiving social engineering attempts over online links
- Receiving social engineering attempts over online pop-up messages
- Responding to social engineering attempts over online popup messages
- Responding to social engineering attempts over social media messages

4.8.3 Online security perceptions

- Online security is important
- Online security is outside the user's control

4.8.4 Information security-related principles

- Changing of privacy settings on social networks

4.8.5 Responding to random email messages

- Verifying the email sender
- Responding after verifying the email sender
- Responding after verifying the email sender when there is something to be won

4.8.6 Responding to random email messages from someone close

- Responding without verifying the email sender

4.8.7 Responding to a social media direct message

- Responding without verifying the message sender
- Responding after verifying the email sender when there is something to be won

4.9 Conclusion

This chapter discussed the participants' responses. The total response rate was 95% and the majority of the respondents were female students. The data for this study did not follow a normal distribution; therefore, non-parametric tests were conducted. Cross-tabulations were used to identify relationships between the constructs. The following chapter (Chapter 5) discusses these results in more detail and in relation to the research objectives outlined in Chapter 1.

CHAPTER 5: DISCUSSION OF RESULTS

5.1 Introduction

In the previous chapter, a detailed analysis of the responses, including descriptive statistics generated from the data, were presented. This chapter presents a detailed discussion of the findings in relation to the research objectives of this study. In addition, the chapter discusses how the study's research objectives were achieved through the analysed data.

5.2 Alignment of the findings with the research objectives

As noted in Chapter 1, the research objectives of this study are as follows:

1. To determine whether there is a gender difference in the response of tertiary students to online social engineering;
2. To identify students' knowledge, from a gender perspective, about online social engineering;
3. To determine if there is a gender difference in attitudes to online information security among young adult students.

5.3 Answering research objectives

5.3.1 Research Objective 1:

Determine whether there is a gender difference in the response of tertiary students to online social engineering

To achieve the gender dependence objective, young adult students were asked to complete questionnaires that consisted of situational-based questions. The questions had different scenarios that tested whether the student would respond. Based on the gender construct, the analysed responses showed the following:

- male dominance in receiving social engineering messages

The findings indicated that more male students acknowledged receiving email messages that were suspicious in nature. Generally, both male and female students use the internet extensively for their learning assessments and for communication purposes with the university. Male students are often considered to be technology enthusiasts, using technology for numerous purposes; and have more email addresses, mainly for online gaming purposes (Noguti, Singh, & Waller, 2019). Hence, a higher percentage of male students claimed to have received random email messages. The findings further indicated that both female and male students have similar response rates. However, male students have a higher response rate to random email messages.

Similar findings were also discovered in a study conducted by Tewari (2015). It was discovered that email messages are commonly used to initiate different types of phishing attempts. Furthermore, it can be implied that male students stand a higher risk of falling victim to social engineering attacks, since they have more email accounts which lead to more phishing attack attempts. In addition, the influence of gender was verified by the Chi-square test, which showed a relationship between gender and receiving a random email message.

Furthermore, based on the findings, more male students indicated that they had received online links that are possible social engineering attempts. The findings showed that more male students respond to the random online links, compared to female students. These findings can be interpreted to mean that female students are aware that random online links are malicious. Therefore, they more often refrain from responding to the link attempts, compared to male students. In a similar study conducted by Al Hasib (2009), it was noted that students tend to avoid clicking on online links because they have identified them as scams. These findings further support the studies of Cai, Fan, and Du (2017), which found that male students tend to have confidence when performing online activities; whereas female students demonstrated computer anxiety when conducting online tasks. Therefore, the higher percentage of male students responding to random online links can be associated with their online confidence over the internet. Additionally, the Chi-square tests showed that a relationship exists between gender and receiving a random online link. This implies that male students are more likely to fall victims to social engineering online link attempts, since they receive and respond more to online link messages. However, there is no gender-dependent relationship with responding to random online links, as both genders showed similar response behaviour.

The results obtained for online pop-up messages showed that male students reported having received more messages that appeared to be malicious in nature. This is not unexpected, as males have been reported to spend more time online (Noguti et al., 2019). Diffley, Kearns, Bennett, and Kawalek (2011) noted in their study that male student respondents specified that they are not bothered by online pop-up messages. Evidently, based on this research study's findings, the percentage of male students who have responded to pop-up messages is more than double that of their female counterparts. This is due to males being more curious (Malandrino et al., 2013) which suggests that they are likely to respond to the online pop-up messages that appear, whilst they are browsing the internet. Furthermore, significant relationships were found

between gender and receiving and responding to online pop-up messages that seemed to be SE attacks, confirming that male students are more susceptible to online pop-up messages.

- female dominance in receiving direct social media messages

In this study, a higher percentage of female students indicated that they have received direct social media messages. These messages appeared to be an attempt at obtaining their personal information. Despite the messages being suspicious in nature, more female students admitted that they have responded to similar messages in the past. These findings correspond to a study conducted by Perrin (2015), in which females indicated that they were active participants on social media sites. This behaviour works in favour of social engineers since they target users continually on social networking sites, due to the significant amount of 'available' personally identifiable information (PII). Similarly, in a study conducted by Joiner, Cuprinskaite, Dapkeviciute, Johnson, Gavin, and Brosnan (2016), females and males demonstrated differences in their responses to social media. In most instances, females demonstrated more sympathy in their responses, compared to males. In another study conducted by Herring and Kapidzic (2015), females were more likely to use social networks for communication. This implies that females are more likely to respond, based on their emotional supportive nature. Furthermore, it means that female students stand a higher chance of falling victim in instances where social engineers convey a sense of urgency, since females would feel the urge to assist. A study conducted by Veltri, Krasnova, Baumann, and Kalayamthanam (2014) showed that online gender patterns exist and are motivated by societal roles of both male and females.

In addition to the cross-tabulations of receiving, and responding to, social media messages, Chi-square tests were conducted. The results showed that there is no relationship between gender and receiving a suspicious social media message. This can be because both genders engage actively on social media sites (Perrin, 2015). However, there exists a relationship between gender and responding to suspicious direct social media messages, showing that females on social media are more likely to fall victim. If social engineers use the trust mechanism to communicate with females, female students would engage with the sender and comply with the given instructions.

5.3.2 Research Objective 2:

Identify students' knowledge about online social engineering from a gender perspective

In this study, students were required to match the appropriate attack type with the given example. Cross-tabulations were conducted to identify the difference in social engineering knowledge between male and female students. The cross-tabulation findings were as follows:

- gender-based awareness and knowledge of attacks related to social engineering

A phishing attack example was provided, and the respondents were asked to identify it. More male students than females were able to identify it accurately as a phishing attack. Equally importantly, more female students acknowledged that they did not know the answer. The Chi-square test showed a relationship between gender and phishing attack awareness. These findings suggest that female students require more social engineering education relating to phishing attacks. In support of the findings, it was also found, in the study conducted by Diaz, Sherman, and Joshi (2020), that females are less knowledgeable about phishing attacks. However, despite male students being more knowledgeable about phishing attacks, there is a risk of them falling victim to phishing attacks. This is due to careless online behavioural patterns. This is supported by a study conducted by Munien (2010) that studied users' awareness levels and the probability of falling victim to phishing attempts. The study found that individuals, irrespective of their knowledge of phishing, fall victim to phishing attacks. The susceptibility of individuals falling victim was due to inadequate online security behaviour.

Techopedia (2014) noted that identity theft victims experience severe consequences, such as damaged credit scores and reputations. Students were given a description of an identity theft that they had to identify. Most of the students were able to accurately classify the example as identity theft. However, the findings indicated that more male students provided accurate responses, compared to female students. These findings can be aligned with the studies of Luo et al. (2011) and Hassan (2019), which reported that young adult students are aware of identity theft and the repercussions. However, more female students indicated that they did not know the answer. This echoes the study conducted by Harrell and Langton (2015) which indicated that young adult students fall victim to identify theft, although they were not familiar with the appropriate term for the attack. Therefore, this implies the possibility that female students who indicated that they 'do not know' had previously had identity theft encounters, without knowing that it was a form of identity theft. However, due to the lack of knowledge and information about security, they did not identify the encounter as identity theft. Also, females'

trusting nature makes them unaware that they are victims of social engineering. No relationship between gender and identify theft awareness was uncovered by the Chi-square test.

To determine whether students are familiar with cybercrime, they were provided with a question which was specific to cybercrime identification. According to the findings, more male students correctly categorised the given example, suggesting that more male students are aware of what cybercrime is and how it operates. These findings correlate with the research conducted by Yu (2014), which concluded that males are aware, and less fearful of, cyberbullying. In support of those findings, Erdur-Baker (2010) also showed how males are more likely to be the perpetrators of cybercrime, compared to their female counterparts. Back, Soor, and LaPrade (2018) conducted a study which affirmed that males, in numerous countries, have a close association with computer hacking. Similarly, Walker, Sockman, and Koehn (2011), in their study, found that there is a positive correlation between physical crime and cybercrime. Furthermore, a higher percentage of female students admitted that they did not know the response. This implies that more attention should be focused on female students as they are more likely to fall victim to cybercrime. Moreover, female students need to be educated about security measures that can be applied to adequately protect themselves in cybercrime situations, similar to the physical campaigns that females stage in South Africa (Gouws, 2018). The awareness programmes should also include how to timeously discover that they have fallen victim to any form of cyberattack. The Chi-square test showed that cybercrime awareness is gender-dependent. This means that male students are less likely to fall victim to cybercrime since they will easily identify that they are being attacked. Also, in most cybercrime offenses, males are the perpetrators.

Further findings from this study showed that more male students were able to accurately identify the email spam example. In support of the findings, Alazab and Broadhurst (2016) revealed how the rapid growth of social networks has contributed to the volumes of spam. Tewari (2015) identified that, nowadays, spam emails are embedded with phishing links, causing differentiation difficulties. This is due to the similarities between email spam and phishing emails, such as language and links embedded in the emails. The Chi-square test conducted indicated that there is no relationship between gender and email spam awareness.

Male students demonstrated a greater awareness of malware. These findings suggest that female students are at risk of downloading content that contains malware since they are not as

knowledgeable about malware. Furthermore, in this research, more female students indicated that they could not identify the malware example presented. A Chi-square test was conducted and showed a relationship between gender and malware knowledge. Therefore, it can be deduced that male students' exposure to technology makes them familiar with malicious software, such as malware. It also implies that male students would be able to identify if their computer is affected with malware and know the necessary measures to be taken. Chandarman and Van Niekerk (2017) stressed that malware campaigns should be conducted to emphasise the importance of regular updates of personal computers. It is believed that campaigns would assist in decreasing the number of successful malware attacks. However, more focus should be given to female students since they are underrepresented in academic streams that provide exposure to both technology hardware and software knowledge.

5.3.3 Research Objective 3:

Determine if there is a gender difference in attitudes to online information security among young adult students

- gender-based interest in online security

This research found that male students have more interest in online security. These findings correlate with those of Bada, Sasse, and Nurse (2019). Their study revealed that male students are more adventurous in technology domains. Therefore, the constant usage of the internet, apparent in male students, leads to a better understanding of the relevance of online security. This also suggests the possibility that male students have previously encountered various forms of social engineering attacks which have made them realise the need for online security. This is reflected further in the research findings, where more male students considered online security important. Gender and the perception of whether online security is necessary were tested to determine if there is a relationship. Although more male students indicated that online security is necessary, there was no relationship. The Chi-square tests indicated that, in as much as male students perceived that online security is necessary, there was no major difference in perception.

- gender-based knowledge about online security

Most male students disagreed that online security was outside the user's control. A study conducted by Herring and Kapidzic (2015) corresponds to these research findings. In their study, it was evident that male students are aware that assigning security measures lies within the users' control. The study implied that male students are more experimental and practical in computer-related matters, which leads to familiarity with computer security. For instance, male students are more aware that installing an antivirus is the users' responsibility. These findings are supported by the findings of Lund (2018). His study showed that male students are knowledgeable about how to safeguard their workstations and how to modify their online security settings. Also, this study's results showed a higher percentage of female students who provided neutral responses as to whether online security is outside the user's control. These results are supported by a study which showed that when students do not know the adequate answer to a question, they provide neutral responses (Saltzman & Price, 2017). This is also believed to be due to the lower representation of female students in the Science, Technology, Engineering and Mathematics (STEM) fields (Liu & Murphy, 2016). The Chi-square test results indicated that there is a relationship between gender and an understanding of whether online security is outside the user's control. The Chi-square test results affirm that male students are more likely to have adequate security controls and security knowledge since they understand that security measures are their responsibility as users.

- gender-based perceptions of information security

Further findings about information security perceptions showed that most male respondents considered online privacy as a mechanism to protect their information. Similar findings were presented in the study by Hunter and Taylor (2019), where male students indicated that social networks use online privacy settings to protect their information from hackers. The findings of this research further showed that more male students considered online privacy a means to prevent identity theft. The findings of this study correlate with the findings of a study conducted by Hayat, Lesser, and Samuel-Azran (2017), who presented findings that revealed that fewer female students used privacy settings.

- the differences in gender behaviour on online social platforms

A higher percentage of female students indicated that hiding their image and contact information is the important reason behind online privacy. This is supported by Mazman and Usluel (2011), whose findings in their study showed that more female students, as compared to males, hide their PII on social networks. The findings also relate to the study conducted by Markman (2012), which indicated that females hiding their personal information is associated with traditional societal roles that women uphold. This is in relation to the social pressure that defines how females should conduct themselves. The findings also showed that many female students do not know the reason behind the importance of online privacy. This implies the possibility that female students will expose their PII information on social networks as they do not know the relevance of online privacy, indicating that a higher number of female students are vulnerable to social engineering attempts. The conducted Chi-square test showed that privacy perception is not gender-dependent. This is interpreted to mean that no gender is more knowledgeable than the other in terms of online privacy importance on social networks. Also, both genders hold similar views about online privacy.

- Gender beliefs towards safeguarding their online information

To further understand gender-dependent attitudes of students to mechanisms that can help safeguard their information, a cross tabulation was conducted. The results showed similar results for both male and female students. More male students considered installing an antivirus as a means of safeguarding their information. Similarly, a study conducted by Malandrino et al. (2013) revealed that male students had false perceptions about protecting their PII. Their findings also showed that some students knew the right tools required to protect their information; yet they lacked the skill, and had negative attitudes, to implementing the tool. Therefore, despite male students claiming to take adequate measures to protect their information, it does not guarantee that they are safe from SE attacks. Male students may not have the necessary skill to install the antivirus. Accordingly, Shen, Yang, and Zhou (2015), highlighted the common mistake that individuals make, by perceiving that installing an antivirus is an adequate measure to safeguard their information. Therefore, more accurate responses are due to the male students' familiarity with technology. In support of these findings, Rathore, Sharma, Loia, Jeong, and Park (2017) noted male students' familiarity with computers.

On the other hand, more female students considered not changing their password as the best solution. These findings indicate that more females than males lack information security knowledge about password security. The cause may be influenced by the lack of females' exposure to computers and other technologies. Similarly, this is presented in the study by Singh, Chandwani, Singh, and Kumar (2019) where female respondents displayed anxiety when using computers. Also, a relatively high percentage of both male and female students indicated that they do not know the best suitable solution for protecting their online information. This implies that both genders have similar challenges with the knowledge that can help safeguard their information. The results relate to a study conducted by Chandarman and Van Niekerk (2017) which showed that students have the misperception that social engineers see no value in their PII. Students are vulnerable due to their lack of information security knowledge, which may help safeguard and prevent them from falling victim to social engineering attacks. The Chi-square test conducted showed no relationship between gender and the perception of protecting online information. Therefore, both genders have similar attitudes to adequate and non-adequate measures of protecting their information.

- gendered concerns about online security

Further results obtained showed that most male students are very concerned about online security. The concern arises when students respond to an unknown source. Students were asked to indicate their level of online security concern when responding to a friend. Male students showed more concern than females. However, more male students were less concerned when responding to a friend than an unknown source. Findings about perception, regarding concern, showed that male students are the more concerned gender. Yet, when responding to a known source, the concern is reduced. It can be deduced that male students' higher level of concern for online security arises from their greater internet usage. In a study conducted by Bashir et al. (2016), it was noted that males spend most of their time online. Also, in another study conducted by Siomos, Dafouli, Braimiotis, Mouzas, and Angelopoulos (2008), male students had the most internet addition disorder and were at risk from internet usage. The findings further indicated that, when students are familiar with an individual, they are less concerned. This is believed to work in favour of social engineers who use identity theft on individuals through messages and emails. The results indicate that both genders would fall victim to social engineering when social engineers present themselves as friends. Grabner-Kräuter and Bitter (2015), in their study, found that both genders fall victim due to the trust mechanism used by

social engineers. The Chi-square test results for both – responding to a friend and to an unknown source – showed no gender influence. These results imply that both female and male students have similar risks of falling victim to the attacker's deception that leads the students into thinking that they are responding to someone known to them.

- gendered attitudes about information security

The overall findings regarding students' attitudes to being taught about information security were positive. Both female and male students noted that they would definitely like to be taught about information security; and female students showed a higher interest in being taught about information security. Only a few students were disinterested in learning about information security. The findings of Heartfield and Loukas (2015) highlighted the approaches to educational activities that raise SE awareness levels. Their approach entailed a multilayered technique in terms of incorporating the human and technical aspects of social engineering. The findings of this study correspond, since most students showed interest in being taught about information security. Also, as shown in the studies of Glanz, Rimer, and Viswanath (2008); Luo et al. (2011); Williams, Beardmore, and Joinson (2017), increasing young adults' awareness levels leads to a change in behaviour, which supports information security practices. In their study, they also found that educational awareness programmes are more meaningful when they consist of explaining the dangers of social engineering. The Chi-square test which was conducted showed that there is no relationship between gender and students' attitudes. This further implies that students share the same eagerness for knowledge about acquiring information security.

A study by Potgieter (2019) stated that students are regarded as the population which is most vulnerable to cybersecurity attacks since they spend most of their time on the internet. The study further found that, in most cases, students are often irresponsible when using the internet, and they their personal information on online sites. Behaviour was cross-tabulated against gender in order to identify gender-dependent behaviours. Students were asked to indicate their behaviour regarding changing their social network passwords. The findings showed that more male students changed their privacy settings, after creating their social network passwords. The findings further showed that other male participants changed their privacy settings after they had worked out how to do the security changes. These findings can be associated with the internet knowledge that male students have. It is evident that male students are more

knowledgeable about the technical details of the internet, and other platforms on the internet. Similarly, in a study conducted by Nami and Vaezi (2018), it was apparent that male students understood the technical details of computer hardware and software. This study shows that male students' computer knowledge transfers into the online world and assists them in protecting their information. The Chi-square test signified a positive relationship between gender and privacy settings on social networks. The relationship implies that male students' information is not as exposed, compared to that of female students. This further implies that female students on social networks are more exposed, compared to male students.

- gendered response rates to messages associated with social engineering

The research findings revealed that male students were more likely to verify a random email message sender. A higher percentage of female students indicated that they would not verify the sender, even though the email message would be random. Similarly, in a study conducted by Heartfield and Loukas (2015), it was evident that young adults, despite their awareness of the risks involved, continue to reveal their information online. The behaviour was noted in instances where young adults download or watch videos from untrusted sites. The Chi-square test conducted found a significant relationship between gender and verifying an email sender of a random message. These findings imply that female students are the more susceptible gender since they indicated no intention of verifying an email sender. The findings further revealed that, if there is something to be won, more female students would again not verify the sender. These findings are supported by a study conducted by Beneito-Montagut (2017) which noted how females are easily influenced by emotional and social associations to products. Also, in support of the findings, a study conducted by Malandrino et al. (2013) showed that individuals fill in their personal information on the sites in order to stand a chance of winning a gift. Furthermore, a study conducted by Liu and Murphy (2016) indicated that females have a higher susceptibility to products advertised online products than do men. Therefore, in the context of this research's findings, it can be concluded that female students are more likely to reveal their information, provided there is something to be won. This also means that female students can be lured, due to their trust in the advertised product. As shown in the research results, female students habitually do not verify the message sender if there is something to be won. Verifying a random email message was tested against gender. However, the Chi-square test to analyse verifying an email message when there is something to be won showed no gender

dependence. This implies that both males and females can be lured by social engineers in random email messages, provided there is something to be won.

The findings for random email messages further showed that gender-dependent relationships exist in responding to the email sender after verifying the sender. The relationships were for both responding after verifying the sender when there is nothing to be won, and for when there is something to be won. In both instances, more male students noted that they would respond to the message by providing their PII after they had verified the sender. The findings relate to a study by Chaudhry et al. (2016) which showed that more male students are risk-takers, compared to their female counterparts. These findings imply that male students are more likely to responding to random email messages. Even though they respond after verifying, it does not provide any assurance that the sender is a legitimate source. Therefore, male students are more likely to fall for phishing attempts, based on their behaviour in responding to the random email messages.

Students were further asked to indicate whether they would respond to a direct social media message without verifying the sender. The findings showed that most female students would not respond to a direct social network message without verifying the message sender. Also, even after verifying the sender, only a few of the female respondents indicated that they would provide their PII. These findings were confirmed by the relationships uncovered by the Chi-square test for both situations. Similar findings are found in the study by Cai et al. (2017), in which female students responded to social network messages from individuals in their circle of friends. This shows that female students are more cautious about their PII, compared to male students. This also emerged in this research, as a gender-dependent relationship. Furthermore, the findings imply that male students willingly provide their personal information to individuals with whom they are not familiar, over social platforms. There is also the possibility that male students verify the sender; yet it can be a fictitious sender, or a profile created by the attackers to lure the individual. Therefore, male students are more vulnerable on social network sites since they are the more responsive gender.

The students' responses indicated that male students have received the most random email messages, online links, and online pop-up messages that seemed to be attempts at social engineering. Thus, the findings show that male students are the more-targeted gender. Also, phishing messages are the most common social engineering attempts. In support of these

research findings, a study conducted by Falk (2016) showed that students use emails daily. Therefore, this research's findings can be related to the constant use of email messaging used by universities and students as a communication platform. It can therefore be deduced that students' constant use of emails exposes them to more phishing attacks; and male students received the most social engineering attempts, which indicates that male students are more vulnerable. Also, the Chi-square tests for receiving a phishing, online link and online pop-up social engineering attempt revealed gender-dependent relationships. The Chi-square results show that social engineers are more likely to attack male students through phishing, online links, and online pop-ups.

On the other hand, female students received the most social engineering attempts on social media. These finding correlate with the study of Al-Jabri et al. (2015), where it was evident that female students are the more active on social networks. However, the Chi-square test conducted on gender and social engineering on social media showed that no relationship exists. This implies that there is no gender-dependent relationship with attempts at social engineering on social media. Furthermore, these findings suggest that both male and female students have the same risk of falling victim to social engineering across all social networks.

5.4 Adaptation of the Gender and International Security, Feminist Theory to the study

The study adopted the feminist theory, since gender concepts are not covered by existing information security theories. The adopted theory focused on interpreting the study's findings from a gendered perspective. This research shows that there are prevalent gender differences in online social engineering (OSE). The findings further showed that subjective norms and attitudes do have an impact on the behavioural intentions of both genders. This is believed to be the influence of learned gendered societal roles which play a part in the way that both male and female students respond to online attacks. For instance, this study shows how the traditional norm for females is to portray characteristics of nurturing. This in turn leads to the vulnerability of female students on the online platform when social engineers use the trust mechanism. This study also found that female students are easily influenced by social associations due to their emotional nature. On the other hand, male students showed a more dominant online presence, linked to their traditional masculinity teachings. Also, the greater exposure of males to technology allows them to be more knowledgeable about social engineering. This is because society regards technology as a male domain; hence the lack of females in the Science, Technology, Engineering and Mathematics streams. This study found

that male students have more knowledge about social engineering and of ways that can help safeguard their information. However, the findings showed that male students are more responsive to most online social engineering attempts. These findings affirm the masculinity teachings of males having to portray bravery as they are considered the leaders of their families. This in turn reveals that gendered societal norms do transfer into the online world.

To determine a gendered attitude towards information security, the feminist theory was further applied. This study found that both male and female students have a positive attitude to being educated about information security. The findings also showed that male students place more importance on online security. More male students understand the importance of online security, and that it is in the user's control, due to their knowledge of the prevalent online social engineering attacks which were addressed earlier in this chapter. Also, the early exposure of males to technical fields leads them to understand that users control the online safety of their information. It is believed that such differences in attitudes and behaviour are habits, resulting from early childhood teaching that shapes the behaviour of both genders.

5.5 Adaptation of the Theory of Reasoned Action (TRA) to the study

This study further tested constructs from the TRA theory that are believed to influence behaviour.

Attitude: The feminist theory guided this construct and it produced results which indicated that both male and female students approve of information security.

Subjective Norm: This study found that external factors, such as feminism and masculinity, impact on behavioural intentions. The feminist theory applied looked at this construct in more depth.

Behavioural Intention: The study was aimed at discovering whether female and male students' behavioural intentions are influenced by attitude and subjective norms. Based on the findings, the motivations for behaviour are influenced by normative beliefs and attitudes. The findings showed that female students act out of femininity teachings. This was shown by females indicating that they would comply with messages if they stood a chance to win something. This suggests a vulnerability in female students, due to their social associations to products. It is also believed that female students' lack of technology exposure influences their

behaviour, as it is traditionally believed that technology is a male domain. The research further found that male students' behavioural intentions are influenced by patriarchal teachings. Male students exhibited boldness in most of the social engineering attacks. Also, male students were more capable in terms of understanding social engineering and adequate controls to protect their online information. This further confirms that social norm impacts behaviour based on masculinity. However, both male and female students' attitudes are similar in nature. This was indicated by the respondents showing similar online security concerns and a positive attitude to learning about information security. This implies that the attitude construct is not gender-dependent, compared to social norms. The only commonality of attitude exists regarding online security training.

Behaviour: Based on the previously defined constructs, it can be inferred that behaviour is driven by external constructs. Although higher percentages of male students respond more to the different categories of social engineering attempts, they are also more knowledgeable about measures that can help safeguard their information; whereas female students are more reluctant on online platforms, as they are less knowledgeable. However, female students act when they have an emotional connection to messages offering rewards. The findings highlight the possible vulnerabilities make both female and male students more susceptible on the internet.

5.6 Conclusion

This chapter explained the results obtained, relative to the research objectives. The chapter also outlined the research objectives and how they have been achieved. The primary research objective of this study was to explore the gender dependence of OSE responses among young adult students. Based on this objective, it was evident that both female and male students have different response behaviours. The research findings further showed that male students have received and responded more to social engineering attempts. The responses were to social engineering attempts in random email messages and random online links. The chapter also presented the gender differences in knowledge about social engineering knowledge. It was concluded that male students have better social engineering awareness than females. In most instances, female students indicated that they did not know the 'suitable' answer. However, both genders indicated a strong willingness to being taught about information security. This demonstrates a positive attitude to information security awareness programmes. Furthermore, the findings highlight areas where students need to be educated about social engineering and ways of protecting themselves. In addition, the chapter provided a summary of how the two

frameworks correlate with the research findings. Both the frameworks show that behaviour is mostly influenced by subjective norms. It is believed that social engineering campaigns can change the mindset of students and lead to similar behavioural patterns and social engineering knowledge in both male and female students.

CHAPTER 6: CONCLUSION

6.1 Introduction

The previous chapter discussed the research findings in relation to the study's research objectives. It further presented how the research objectives were achieved through data analysis. The current study was rooted in its objectives, presented in Chapter 1. The aim of the study was to explore, explain and examine, according to gender, online social engineering attacks on young adult students. The quantitative research approach taken was to better understand, quantify and provide explanations of attacks on students. This chapter provides the conclusion, and thereafter summarises the major findings based on the study's results. Furthermore, this chapter presents recommendations for social engineering (SE) awareness initiatives. In addition, it provides suggestions for future research.

6.2 Summary of the study

Chapter 1 provided an outline of the study. It introduced the concept of online social engineering (OSE) and the existing attacks on various online channels. It also explained why young adult students are the most vulnerable to social engineering attacks. It further provided an overview of the problem statement and the research questions and objectives. In addition, the chapter explained in detail the two adopted research frameworks used in this study. Furthermore, the chapter provided the limitations of the study and an overview of the subsequent chapters.

Chapter 2 presented previous literature on social engineering. It also explained the common attack types of social engineering. Furthermore, it reviewed social engineering in relation to information security, gender and young adult students. The chapter also provided an overview of social engineers use of compliance mechanisms to lure young adult students into falling victim. Additionally, it explained the concept of online social engineering and how it is human-related.

Chapter 3 presented an in-depth description of the research methodology and techniques used in this study. It also described the methods by which data was collected and analysed. Data was collected through questionnaires from students at two academic institutions in Pietermaritzburg. It discussed the Krejcie and Morgan table, used to select the sample size (379), and the probability sampling method used. Furthermore, the chapter provided a

description data analysis which was conducted using the Statistical Package for Social Sciences (SPSS).

Chapter 4 presented the analysed findings from the collected data. The chapter presented the reliability test and normality test results as the introduction, prior to the detailed description of the analysed data. The normality test results indicated that this study's collected data was not normally distributed. Hence, the study employed non-parametric tests on the data. In addition, this chapter presented the results of cross-tabulations and chi-square tests. The results were used to distinguish existing relationships between tested variables.

Chapter 5 discussed the findings in detail, in relation to the research objectives of this study. The results presented were aligned to the research objectives.

6.3 Conclusion of the study

The primary objective of this study was to discover whether there is a gender difference in responses to online social engineering attempts, and to provide awareness programmes based on the findings of the research. Two frameworks were adopted in order to conduct the study through a gendered lens. A feminist theory, in conjunction with the Theory of Reasoned Action (TRA), was used to guide the study. The two theoretical frameworks guided the study in terms of gender and IT. The constructs of the TRA theory guided the formulation of the study's research questions and objectives. The first research question focused on identifying the students' gender differences in online social engineering attempts. The research question centered around identifying the gender differences in online social engineering attempts. It also tested the different recognition levels of both female and male students. The second research question investigated the young adults' attitudes. It was aimed at identifying the extent to which there is a gender difference in social engineering attitudes. The third question focused on identifying the gender differences in responses to online social engineering. It was aimed at discovering whether the social engineering responses are adequate to protect both males and females.

The study employed a quantitative research approach, which used 379 questionnaires that were distributed to students at UKZN, Pietermaritzburg campus, and Umgungundlovu FET college. The collected data was further analysed using the Statistical Package for Social Sciences

(SPSS). Based on the research findings, it was found that there is a gender difference in responses to online social engineering attacks. These gender differences were influenced by external factors, found in the TRA theory, which contribute to behavioural intentions that impact the overall behaviour of both female and male students. Thus, the variables in the TRA theory are considered valid, based on the data analysis of this study.

The study revealed that gender plays a significant role in behavioural intentions, which are built upon normative beliefs. These beliefs, in turn, shape the differences in behaviour of female and male students. Due to gendered normative beliefs, such as the traditional societal roles of males and females, male students showed more online presence and familiarity with the online domain. This is due to a males' prior exposure to technology as technology is considered a male domain. This exposure contributes to the male students' knowledge about social engineering attacks and information security-related principles. This was revealed in the positive correlations that were found between gender and SE awareness. The findings showed that male students have better recognition levels and understanding of attacks. Also, traditional male upbringing nurtures bravery in male students, which influences their behaviour. In this study, such teachings were found to influence the way in which male students respond boldly to random online messages without knowing or verifying the message sender. On the other hand, it was found that female students showed inadequate social engineering awareness and more reserved behaviour in responding to online messages. It was also evident that, due to the female students' underrepresentation in technology fields, female students lacked awareness and knowledge of SE attacks and adequate measures to protect their information on online social networks.

Findings also revealed that behaviour regarding SE attacks is influenced by the differences in the gendered attitudes. Prior exposure to technology and the dominant online presence of male students led to their understanding the importance of online security. Also, male students showed more understanding of user controls and privacy settings to safeguard their online information. Prior exposure to technology also influenced the behavioural intentions of male students. It was found that male students' knowledge of technology, and their online attitude, led to the bold behaviour noted by the male students. Male students consider themselves 'tech savvy', which allows them to be more curious and behave in a manner that makes them more vulnerable to online attackers. Female students' lack of understanding of information security led to them perceiving online security as unimportant. Therefore, the female students', 'I do

not know' attitude, influenced their behaviour, and they were more reluctant to respond to random messages. However, both genders showed positive attitudes to being taught about online security. This is believed to shape both males' and females' behaviour regarding online information security.

6.4 Recommendations

Email and intranet notifications

Academic institutions can provide awareness notifications via the intranet and by using the students' emails. The notifications can be sent out in bulk, educating students about social engineering. This approach will reach every student on the university's emailing system, as per the school's standard notification system. However, the limitation is the low number of students who would take their time to thoroughly read the email.

Information security module

Universities can introduce an information security module, focusing on social engineering. The module can consist of theoretical and practical ways of identifying online social engineering attacks. The practical aspect of the module can include interactive real-life social engineering simulations. The shortcoming of this approach may be that students do not register for the module as they may be disinterested. This limitation can be addressed by making the module compulsory for students, across all the faculties. The module can be an introductory module to information security as per the research findings, Chapter 5. It was noted that the majority of the students agreed to being educated about information security.

Computer screensavers

In the university's local area networks (LAN), the computers utilised by students may have screen messages. The messages can be updated, based on the current and predominant types of social engineering attacks. However, there is no guarantee that students will read the screensavers. In order to ensure that students have read the screensaver message, the message can be interactive and made compulsory. In order to log onto a computer, the students would be required to identify the suspicious example, such as a phishing email, online pop-up or social media message. This awareness method can assist with data collection to identify other social engineering topics that need attention.

Online security and privacy posters

The university can post awareness posters that show students how to safeguard their information on the internet. The posters can contain steps on how to change security settings across the different social networks, in order for students to better secure their online information. Also, the posters can inform students about the potential dangers to their personal information, as well as why it is necessary to constantly change passwords across online channels such as Gmail and Facebook. In highlighting the 'why', students would understand the relevance of complying with the tips provided on the posters. The limitation is that there is no assurance that students will read the posters. Thus, it is believed that this approach will provide a subconscious awareness, based on the continuous security messages carried out on the posters.

Information security centre

The university can provide an information security centre that focuses on conducting workshops and provides support for students who wish to gain more information security knowledge. Also, students will be shown what social engineering attacks look like, as well how to avoid falling victim. The centre could also assist those students who experience a digital divide gap**.** Therefore, students will be given direct assistance, such as modifying their online security settings and installing antiviruses to enforce online privacy. The shortfall of this technique is that students may not approach the centre for advice. Therefore, to ensure that students are capitalising on the information security center, the centre can be situated next to the Information and Communication Technology (ICT) help desk to create awareness whenever students come in for their student account assistance.

University policy

Universities can implement a password policy that regulates email accounts. The policy can consist of password expiry and non-recycling of passwords. The policy will mean students are unable to use the same password repeatedly after its expiry date.

6.5 Suggestions for future research

The study has confirmed the need for further scientific social engineering research. Thus, based on this research, the areas that are suggested for future research are as follows:

- A qualitative in-depth investigation of the victimisation impact that female and male students face due to social engineering. The study should particularly focus on investigating the impact of identity theft.
- A further quantitative study conducted across students from various provinces in South Africa. This study will provide broader findings which can be generalised.
- A quantitative study that will test awareness through simulation exercises at the beginning of the year; thereafter, heighten social engineering awareness and then retest. This study will provide statistics based on the impact that awareness has on female and male student behaviour.
- A qualitative study that looks deeper into the gender dimensions by incorporating additional gender-based theories, such as the Hofstede's Masculinity versus Femininity dimension, into technology.

REFERENCES

Abeywardana, K. Y., Pfluegel, E., & Tunnicliffe, M. J. (2016). A layered defense mechanism for a social engineering aware perimeter. *2016 SAI Computing Conference (SAI)*, 1054–1062. https://doi.org/10.1109/SAI.20167556108

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation, 2*(3), 242-253. https://doi.org/10.1007/s12559-010-9042-7

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11–39). Springer, Berlin, Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. United States of America: Prentice-Hall.

Al-Jabri, I. M., Sohail, M. S., & Ndubisi, N. O. (2015). Understanding the usage of global social networking sites by Arabs through the lens of uses and gratifications theory. *Journal of Service Management*, *26*(4), 662–680. https://doi.org/10.1108/JOSM-01-2015-0037

Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *36*(11), 335–344. https://doi.org/10.1109/ACSAC.2008.36

Alazab, M., & Broadhurst, R. (2016). *Trends & issues in crime and criminal justice Spam and criminal activity*. *526*. https://aic.gov.au/publications/tandi/tandi526

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018, December*, 62–68. https://doi.org/10.1109/TALE.2018.8615162

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. https://doi.org/10.1016/j.cose.2017.04.006

Alexander, G. (2007). The emergence of cybercrime and the legal response. *Journal of Security Education, 2*(2), 47-79

Algarni, A., Xu, Y., & Chan, T. (2015). Susceptibility to social engineering in social networking sites: The case of Facebook. *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015, December*, 13–16. https://doi.org/10.1057/s41303-017-0057-y

Algarni, A., Xu, Y., & Chan, T. (2016). Measuring source credibility of social engineering attackers on Facebook. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2016-March*, 3686–3695. https://doi.org/10.1109/HICSS.2016.460

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). Social Engineering in Social Networking Sites : Affect-based model. *Information Science and Technology (ICIST), 2013 International Conference*, 508–515. https://doi.org/10.1109/ICITST.2013.6750253

Algarni, A., Xu, Y., Chan, T., & Tian, Y.C. (2014). Social engineering in social networking sites: how good becomes evil. *Proceedings of the 18th Pacific Asia conference on information systems (PACIS)*. https://eprints.qut.edu.au/73379/

Andress, J. (2014). The basics of information security. Understanding the fundamentals of infosec in theory and practice. United States of America: Elsevier Inc.

Archer, K., Wood, E., Nosko, A., De Pasquale, D., Molema, S., & Christofides, E. (2015). Disclosure and privacy settings on social networking sites: Evaluating an instructional intervention designed to promote informed information sharing. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (pp. 287–306). https://doi.org/10.4018/978-1-4666-8111-8.ch015

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory. *International Journal of Cybersecurity Intelligence & Cybercrime, 1*(1), 40-55.

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, 11. https://arxiv.org/abs/1901.02672

Bae, S., & Lee, T. (2011). Gender differences in consumers' perception of online consumer reviews. *Electronic Commerce Research, 11*(2), 201-214. https://doi.org/10.1007/s10660-010-9072-y

Bakdash, J. Z., Hutchinson, S., Zaroukian, E. G., Marusich, L. R., Thirumuruganathan, S., Sample, C.,

Hoffman, B., & Das, G. (2018). Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy007

Banu, M. N., & Banu, S. M. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *4*(6), 783–786.

Bashir, S., Mahmood, K., & Shafique, F. (2016). Internet use among university students: a survey in University of the Punjab, Lahore. *Pakistan Journal of Information Management and Libraries, 9*(1).

Beam, G. (Ed.). (2017). *The Problem with Survey Research*. New York: Routledge. https://doi.org/10.4324/9781315134215

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of Biomedical Ethics*. New York: Oxford University Press.

Beneito-Montagut, R. (2017). Emotions, everyday life, and the social web: Age, gender, and social web engagement effects on online emotional expression. *Sociological Research Online, 22*(4), 87-104. https://doi.org/10.1177/1360780417732955

Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010). Social Engineering Attack Detection Model: SEADM. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. https://doi.org/10.1109/ISSA.2010.5588500

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. In *Pure and Applied Chemistry* (2nd ed.). United States of America: Global Text Project.

Bilau, A. A., Witt, E., & Lill, I. (2018). Practice framework for the management of post-disaster housing reconstruction programmes. *Sustainability*, *10*(11). https://doi.org/10.3390/su10113929

Blanchard, Eric, M. (2015). Gender, International Relations, and the Development of Feminist Security Theory. *Signs Journal of Women in Culture and Society*, *28*(4), 1289–1312. https://doi.org/10.1086/368328

Bornstein, M. H. (2012). Cultural Approaches to Parenting. *Parenting: Science and Practice*, *12*(2–3), 212–221. https://doi.org/10.1080/15295192.2012.683359

Bradburn, N. M., Sudman, S., & Wansink, B. (2004). *Asking Questions: The Definitive Guide to Questionnaire Design - For Market Research, Political Polls, and Social and Health Questionnaires*. San Francisco: Jossey-Bass.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1–20.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and Cybercrime Risks in a University Student Community. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(1), 4-23.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology, 11*(1), 97-115.

BusinessMediaMAGS. (2018). SA Ranks World's Third Highest Cybercrime Victims. *Business Media MAGS*.

Bussey, K., & Bandura, A. (1999). Social cognitive theory of gender development and differentiation. *Psychological review, 106*(4), 676. https://doi.org/10.1037/0033-295X.106.4.676

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *Australasian Conference on Information Systems 2015*, 1–10. https://arxiv.org/abs/1606.00887

Cabaj, K., Grochowski, K., & Gawkowski, P. (2015). Practical Problems of Internet Threats Analyses *Advances in Intelligent Systems and Computing, 365.* Cham: Springer.

Cai, Z., Fan, X., & Du, J. (2017). Gender and attitudes toward technology use: A meta-analysis. *Computers & Education, 105*, 1-13. https://doi.org/10.1016/j.compedu.2016.11.003

Calisir, F., Gumussoy, A.C., Bayraktaroglu, A. E., & Karaali, D. (2014). Predicting the intention to use a web-based learning system: Perceived content quality, anxiety, perceived system quality, image, and the technology acceptance model. *Human Factors and Ergonomics in Manufacturing & Service Industries, 24*(5), 515-531. https://doi.org/10.1002/hfm.20548

Carli, L. L. (2001). Gender and social influence. *Journal of Social Issues, 57*(4), 725-741. https://doi.org/10.1111/0022-4537.00238

Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-715. https://doi.org/10.1007/s11948-014-9551-y

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication, 20*, 133-155. https://doi.org/10.23962/10539/23572

Chang, M. K. (2013). Predicting unethical behavior: A comparison of the theory of reasoned action and the theory of planned behavior *Citation classics from the Journal of Business Ethics*, 433-445. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-4126-3_21

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247–256. https://doi.org/10.14257/ijsia.2016.10.1.23

Charles, A. T. (2017). *The Abuse of Teenagers by Online Predators Facilitated Through the Internet and Social Media.* [Utica College].

Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. *Global Commission on Internet Govrnance*, *6*.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Cloete, N. (2014). A new look at demographic transformation: Comments on Govinder et al.(2013). *South African Journal of Science, 110*(1-2). https://doi.org/10.1590/sajs.2014/a0048

Cooke, R., Dahdah, M., Norman, P., & French, D. P. (2016). How well does the theory of planned behaviour predict alcohol consumption? A systematic review and meta-analysis. *Health psychology review, 10*(2), 148-167. https://doi.org/10.1080/17437199.2014.947547

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods*. 11th Edition. New York: McGraw-Hill.

Corey, R. (2019). What Is the CIA Triad? Confidentiality, Integrity and Availability. Retrieved from https://www.cybrary.it/blog/2015/06/what-is-the-cia-triad-confidentiality-integrity-and-availability/#:~:text=CIA%20stands%20for%20confidentiality%2C%20integrity,important%20elements%20of%20reliable%20security

Countrymeters. (2017). World population. Retrieved from http://countrymeters.info/en/World

Coyne, S. M., Padilla-Walker, L. M., Holmgren, H. G., & Stockdale, L. A. (2019). Instagrowth: a longitudinal growth mixture model of social media time use across adolescence. *Journal of research on adolescence*, *29*(4), 897-907. https://doi.org/10.1111/jora.12424

CreamerMedia. (2018). Scholars beware: phishing fraudsters hunt for university credentials. Retrieved from http://www.engineeringnews.co.za/article/scholars-beware-phishing-fraudsters-hunt-for-university-credentials-2018-10-24/rep_id:4136

Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative*. 1st Edition. Upper Saddle River, NJ: Prentice Hall.

Curran, J., Fenton, N., & Freedman, D. (2016). *Misunderstanding the Internet*. London: Routledge. https://doi.org/10.4324/9781315695624

Da Silva, C. M. R., Da Silva, J. L. C., Melo, R. M., Rodrigues, R. B., Lucien, L. R., De Melo, S. P., Colares, A., & Garcia, V. C. (2014). A privacy maturity model for cloud storage services. *2014 IEEE 7th International Conference on Cloud Computing, CLOUD*, 944–945. https://doi.org/10.1109/CLOUD.2014.135

Dakpa, T., & Augustine, P. (2017). Study of Phishing Attacks and Preventions. *International Journal of Computer Applications, 163*(2), 5-8. https://doi.org/10.5120/ijca2017913461

Derksen, T., & Hilbrink, A. (2012). *Training at the Dutch Police Academy and Digital Forensic Training Programme New Developments and Involvement in ISEC and ECTEG*. 6th International Conference on Cybercrime Forensics Education & Training.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Conference on Human Factors in Computing Systems*, 581–590. https://doi.org/10.1145/1124772.1124861

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53-67. https://doi.org/10.1080/01611194.2019.1623343

Diffley, S., Kearns, J., Bennett, W., & Kawalek, P. (2011). Consumer behaviour in social networking sites: implications for marketers. *Irish Journal of Management*, *30*(2), 47-65.

Dörnyei, Z., & Taguchi, T. (2009). *Questionnaires in second language research: Construction, administration, and processing*. New York: Routledge.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *ACM International Conference Proceeding Series*, *149*, 79–90. https://doi.org/10.1145/1143120.1143131

Drucker, P. F. (2015). Internet of things. *European Commission Information Society and Media*.

Dufour, M., Brunelle, N., Tremblay, J., Leclerc, D., Cousineau, M.-M., Khazaal, Y., Légaré, A. A., Rousseau, M., & Berbiche, D. (2016). Gender Difference in Internet Use and Internet Problems among Quebec High School Students. *The Canadian Journal of Psychiatry*, *61*(10), 663–668. https://doi.org/10.1177/0706743716640755

Ekawade, S., Mule, S., & Patkar, U. (2016). Phishing Attacks and Its Preventions. *Imperial Journal of Interdisciplinary Research*, *2*(12).

Erdur-Baker, Ö. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society*, *12*(1), 109–125. https://doi.org/10.1177/1461444809341260

Falk, C. (2016). *Knowledge modeling of phishing emails* [Purdue University]. https://docs.lib.purdue.edu/open_access_dissertations/754

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*, *9*(1), 1–11. https://doi.org/10.5815/ijcnis.2017.01.01

Fang, J., Wen, C., George, B., & Prybutok, V. R. (2016). Consumer heterogeneity, perceived value, and repurchase decision-making in online shopping: the role of gender, age, and shopping motives. *Journal of Electronic Commerce Research*, *17*(2), 116.

Fathollahi-Fard, A. M., Hajiaghaei-Keshteli, M., & Tavakkoli-Moghaddam, R. (2018). The social engineering optimizer (SEO). *Engineering Applications of Artificial Intelligence*, *72*, 267-293. https://doi.org/10.1016/j.engappai.2018.04.009

Ferrell, O. (2017). Broadening marketing's contribution to data privacy. *Journal of the Academy of Marketing Science*, *45*(2), 160-163. https://doi.org/10.1007/s11747-016-0502-9

Flick, U. (2015). *Introducing research methodology: A beginner's guide to doing a research project*: SAGE.

Florencio, D. A., & Herley, C. E. (2010). Preventing phishing attacks. United States of America: Patent and Trademark Office.

Ford, D. S., Massey, K. K., & Hyde, D. (1985). Factors related to authoritarian versus nonauthoritarian attitudes toward parenting among college students. *Health education*, *16*(6), 26-28. https://doi.org/10.1080/00970050.1986.10614483

Freeman, N. K. (2007). Preschoolers' perceptions of gender appropriate toys and their parents' beliefs about genderized behaviors: Miscommunication, mixed messages, or hidden truths? *Early Childhood Education Journal*, *34*(5), 357-366. https://doi.org/10.1007/s10643-006-0123-x

Galloway, K. L. (2013). *Selected marketing communication methods influencing young adults' perceptions and buying intentions of healthy foods in South Africa* [Nelson Mandela Metropolitan University]. http://vital.seals.ac.za:8080/vital/access/BibliographyStatistics/Galloway, Kelly Lou

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks. *In Proceedings of the 2007 ACM workshop on Recurring malcode* (pp. 1-8)

Glanz, K., Rimer, B. K., & Viswanath, K. (2008). *Health behavior and health education: theory, research, and practice*. San Francisco: John Wiley & Sons.

Glanz, K., Rimer, B. K., & Viswanath, K. (2015). *Health behavior: Theory, research, and practice*. San Francisco: John Wiley & Sons.

Gouws, A. (2018). # EndRapeCulture Campaign in South Africa: Resisting Sexual Violence Through Protest and the Politics of Experience. *Politikon*, *45*(1), 3-15. https://doi.org/10.1080/02589346.2018.1418201

Grabner-Kräuter, S., & Bitter, S. (2015). Trust in online social networks: A multifaceted perspective.

Forum for Social Economics, *44*(1), 48–68. https://doi.org/10.1080/07360932.2013.781517
Granger, S. (2003). Social engineering fundamentals, part I: hacker tactics. *Security Focus, 18*.
Greenberg, A. (2014). Hacker Lexicon: What Is End-to-End Encryption? *Wired*. Retrieved from https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/
Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *2014 IEEE Security and Privacy Workshops*, 236–250. https://doi.org/10.1109/SPW.2014.39
Hajli, N., & Lin, X. (2014). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x
Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737–744. https://doi.org/10.1145/2487788.2488034
Harrell, E., & Langton, L. (2015). Victims of Identity Theft, 2014. *Bureau of Justice Statistics*. https://www.bjs.gov/content/pub/pdf/vit14.pdf
Harrison, G. (2013). *Neoliberal Africa: The Impact of Global Social Engineering*. United Kingdom: Zed Books. https://www.scribd.com/read/326040815/Neoliberal-Africa-The-Impact-of-Global-Social-Engineering
Hasim, M. S., & Salman, A. (2010). Factors affecting sustainability of internet usage among youth. *The Electronic Library*, *28*(2), 300–313. https://doi.org/10.1108/02640471011033657
Hassan, N. A. (2019). Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks. New York: *Apress*. https://doi.org/10.1007/978-1-4842-4255-1
Hayat, T. Z., Lesser, O., & Samuel-Azran, T. (2017). Gendered discourse patterns on online social networks: A social network analysis perspective. *Computers in Human Behavior, 77*, 132-139. https://doi.org/10.1016/j.chb.2017.08.041
Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-based nursing*, ebnurs-2015-102129. https://doi.org/10.1136/eb-2015-102129
Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1–38. https://doi.org/10.1145/2835375
Heiman, T., & Olenik-Shemesh, D. (2015). Cyberbullying experience and gender differences among adolescents in different educational settings. *Journal of Learning Disabilities, 48*(2), 146-155. https://doi.org/10.1177/0022219413492855
Helsper, E. J. (2010). Gendered internet use across generations and life stages. *Communication Research, 37*(3), 352-374. https://doi.org/10.1177/0093650209356439
Herring, S. C., & Kapidzic, S. (2015). Teens, gender, and self-presentation in social media. *International encyclopedia of social and behavioral sciences, 2*, 1-16.
Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19. https://doi.org/10.1016/j.intmar.2014.10.001
Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. *EDPACS, 37*(4-5), 32-46. https://doi.org/10.1080/07366980801907540
Hinton, P. R., McMurray, I., & Brownlow, C. (2014). *SPSS Explained*. London: Routledge. https://doi.org/10.4324/9781315797298
Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime and Law, 21*(7), 681-698. https://doi.org/10.1080/1068316X.2015.1028545
Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81. https://doi.org/10.1145/2063176.2063197
Hoy, M. G., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168
Huang, C.-Y., Ma, S.-P., & Chen, K.-T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications, 34*(4), 1292-1301. https://doi.org/10.1016/j.jnca.2011.02.004

Hudson, H. (2005). 'Doing'security as though humans matter: A feminist perspective on gender and the politics of human security. *Security Dialogue, 36*(2), 155-174. https://doi.org/10.1177/0967010605054642

Hung, S.-H., Shih, C.-S., Shieh, J.-P., Lee, C.-P., & Huang, Y.-H. (2012). Executing mobile applications on the cloud: Framework and issues. *Computers & Mathematics with Applications, 63*(2), 573-587. https://doi.org/10.1016/j.camwa.2011.10.044

Hunter, G. L., & Taylor, S. A. (2020). The relationship between preference for privacy and social media usage. *Journal of Consumer Marketing*, *37*(1), 43–54. https://doi.org/10.1108/JCM-11-2018-2927

Hussein, N. H., Khalid, A., & Khanfar, K. (2016). A survey of cryptography cloud storage techniques. *International Journal of Computer Science and Mobile Computing, 5*(2), 186-191.

Ibrahim, M., Ramanathan, S., Som, T. K., & Trevathan, M. B. (2016). System and method to support identity theft protection as part of a distributed service oriented ecosystem. United States of America: Patent and Trademark Office.

InternetWorldStats. (2016). *South Africa: Internet usage, broadband and telecommunications reports*. Retrieved from https://www.internetworldstats.com/af/za.htm

Ivaturi, K., & Janczewski, L. (2011). A Taxonomy for Social Engineering attacks. *International Conference on Information Resources Management*, 1–12.

Jakobsson, M., & Myers, S. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*: John Wiley & Sons.

Joffe, A. O. (1985). *Psychological gender: the relationship between sex-role and gender identity.* [University of Cape Town].

Joiner, R., Cuprinskaite, J., Dapkeviciute, L., Johnson, H., Gavin, J., & Brosnan, M. (2016). Gender differences in response to Facebook status updates from same and opposite gender friends. *Computers in Human Behavior, 58*, 407-412.

Joseph, C. (2011). *An Investigation of Grade 10 and 11 Boys' Perceptions of Gender, Gender Equality and Sexism in a Secondary School [University of KwaZulu-Natal]*. http://ukzn-dspace.ukzn.ac.za/handle/10413/8234

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75-87. http://dx.doi.org/10.1016/j.chb.2016.09.012

Kachel, S., Steffens, M. C., & Niedlich, C. (2016). Traditional Masculinity and Femininity: Validation of a New Scale Assessing Gender Roles. *Frontiers in Psychology*, *7*, 1–19. https://doi.org/10.3389/fpsyg.2016.00956

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter? *Journal of Financial Services Research, 50*(1), 121-159. https://doi.org/10.1007/s10693-015-0218-x

Kefalas, A. (2017). *The relevance of traditional Collective Management Organisations in the digital age: Current challenges and future possibilities.* [Universitetet i Agder; University of Agder]. https://uia.brage.unit.no/uia-xmlui/handle/11250/2457424

Kennedy, C., & Dingli, S. (2018). Gender and Security. In: Collins, A. (ed.), *Contemporary Security Studies.*United Kingdom: Oxford University Press.

Kothari, C. (2017). *Research Methodology: Methods and Techniques*. New Delhi: New Age International.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607-610. https://doi.org/10.1177/001316447003000308

Kritzinger, E. (2006). *An information security retrieval and awareness model for industry.* [University of South Africa]. https://core.ac.uk/download/pdf/43165935.pdf

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122.

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology*, *2*(11), 15-19.

Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges, 26*(2), 80-87.
Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. *Pew internet & American life project*.
Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice, 16*(4), 473-475.
Liben-Nowell, D., & Kleinberg, J. (2007). The link-prediction problem for social networks. *journal of the Association for Information Science and Technology, 58*(7), 1019-1031.
Liu, X., & Murphy, D. (2016). *Engaging females in cybersecurity: K through Gray.* Paper presented at the Intelligence and Security Informatics (ISI), 2016 IEEE Conference on.
Lund, P. (2018). Information Security Awareness amongst students: A study about information security awareness at universities. [Lulea University of Technology].
Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ), 24*(3), 1-8.
Lynch, B. K. (1990). Designing Qualitative Research by Catherine Marshall an Gretchen B. Rossman. *Issues in Applied Linguistics*, *1*(2). https://escholarship.org/uc/item/3m25g8j8
Ma, Q. (2013). The process and characteristics of phishing attacks-A small international trading company case study. *Journal of Technology Research*, *4*, 1.
Maccoby, E. E. (1998). *The two sexes: Growing up apart, coming together*: Harvard University Press.
Maceli, K. M., Baack, D. W., & Wachter, M. K. (2015). The impact of gender on electronic word-of-mouth communication. *Academy of Marketing Studies Journal, 19*(3), 281.
Mackey, A., & Gass, S. M. (2015). *Second language research: Methodology and design*. New York: Routledge.
Magdalin, V. (2015). Securing networks against spear phishing attacks: United States of America: Patent and Trademark Office.
Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013). Privacy awareness about information leakage: Who knows what about me? *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, 279–284. https://doi.org/10.1145/2517840.2517868.
Mann, I. (2017). *Hacking the human: social engineering techniques and security countermeasures*. London: Routledge.
Markman, K. M. (2012). A Networked Self: Identity, Community and Culture on Social Network Sites. *New Media & Society*, *14*(7), 1240–1242. https://doi.org/10.1177/1461444812453432
Mashiya, N., Kok, L., Luthuli, N., Xulu, S., & Mtshali, Z. (2015). Foregrounding the gender divides in early childhood teacher education: A case of South Africa. *Journal of Social Sciences, 42*(3), 259-265. https://doi.org/10.1080/09718923.2015.11893413
Mazman, S. G., & Usluel, Y. K. (2011). Gender differences in using social networks. *Turkish Online Journal of Educational Technology-TOJET, 10*(2), 133-139.
McCrum-Gardner, E. (2008). Which is the correct statistical test to use? *British Journal of Oral and Maxillofacial Surgery, 46*(1), 38-41. https://doi.org/10.1016/j.bjoms.2007.09.002
McGlone, M. S., Ballard, D. I., Berkelaar, B., Baryshevtsev, M., & Brown, L. (2015). The "Identity Literacy" Scale: A Preliminary Report. *Center for Identity*.
Mohanty, S., Ganguly, M., & Pattnaik, P. K. (2018). CIA Triad for Achieving Accountability in Cloud Computing Environment. *International Journal of Computer Science and Mobile Applications*, 39–44.
Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, research and practice, 70*(4), 231.
Moore, F. O. (2016). Qualitative vs Quantitative Research. [Northcentral University]. https://doi.org/10.13140/RG.2.2.34861.49128
Moosa, F. (2017). Why Do SA Universities Have More Female Graduates But Fewer Academics? *The Daily Vox*. Retrieved from https://www.thedailyvox.co.za/sa-universities-female-graduates-fewer-academics-fatima-moosa/
Morgan, G. A., Leech, N. L., Gloeckner, G. W., & Barrett, K. C. (2004). *IBM SPSS for Introductory*

Statistics: Use and Interpretation (Fourth). New York: Routledge.
Mostafa, M. M. (2007). Gender differences in Egyptian consumers' green purchase behaviour: the effects of environmental knowledge, concern and attitude. *International Journal of Consumer Studies, 31*(3), 220-229. https://doi.org/10.1111/j.1470-6431.2006.00523.x
Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186-209. https://doi.org/10.1016/j.cose.2016.03.004
Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. *2014 Information Security for South Africa*. https://doi.org/10.1109/ISSA.2014.6950510
Munien, R. (2010). *Internet Phishing Hook, Line and Hopefully Not Sunk*--. Westville: University of KwaZulu-Natal.
Musingafi, M. C., Mapuranga, B., Chiwanza, K., & Zebron, S. (2015). Challenges for open and distance learning (ODL) students: Experiences from students of the Zimbabwe Open University. *Journal of Education and Practice, 6*(18), 59-66.
MyBroadband. (2014). South African Internet users: age, gender, and race. Retrieved from https://mybroadband.co.za/news/Internet/109396-south-african-Internet-users-age-gender -and-race.html
Nagarjuna, B., & Sujatha, V. (2013). An innovative approach for detecting targeted malicious E-mail. *International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2*(7), 422-428.
Naidoo, S. (2011). *The impact of the digital divide on information literacy training of Extended Curriculum Programme students at the Durban University of Technology* [Durban University of Technology]. http://er.dut.ac.za/handle/123456789/42
Nami, F., & Vaezi, S. (2018). How ready are our students for technology-enhanced learning? Students at a university of technology respond. *Journal of Computing in Higher Education, 30*(3), 510-529. https://doi.org/10.1007/s12528-018-9181-5
Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches*. London: Pearson Education Limited.
Noguti, V., Singh, S., & Waller, D. S. (2019). Gender differences in motivations to use social networking sites *Gender Economics: Breakthroughs in Research and Practice* (pp. 676-691): IGI Global.
Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in health sciences education, 15*(5), 625-632. https://doi.org/10.1007/s10459-010-9222-y
Norona, J. C., Preddy, T. M., & Welsh, D. P. (2015). How gender shapes emerging adulthood. *The Oxford handbook of emerging adulthood*, 62-86.United Kingdom: Oxford University Press.
Noureddine, M., Keefe, K., Sanders, W. H., & Bashir, M. (2015). Quantitative security metrics with human in the loop. *ACM International Conference Proceeding Series, 21-22-April-2015*. https://doi.org/10.1145/2746194.2746215
Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook. South African Journal of Science. *114*, 1-5.
Okesola, J. O., Onashoga, A., & Ogunbanwo, A. (2016). An investigation into users' information security awareness on social networks in south western Nigeria. *South African Journal of Information Management, 18*(1), 1-7. https://doi.org/10.4102/sajim.v18i1.721
Oltramari, A., Henshel, D. S., Cains, M., & Hoffman, B. (2015). Towards a Human Factors Ontology for Cyber Security. *Proceedings of STIDS*, 26-33.
Panchenko, A., Lanze, F., Pennekamp, J., Engel, T., Zinnen, A., Henze, M., & Wehrle, K. (2016). Website Fingerprinting at Internet Scale. *NDSS*. https://doi.org/10.14722/ndss.2016.23477
Parbanath, S. (2011). *Personal Information Security: Legislation, Awareness and Attitude.* [University of KwaZulu-Natal].
Peltier, T. R. (2005). Information Security Risk Analysis. New York: *Auerbach Publications*. https://doi.org/10.1201/9781420031195
Perrin, A. (2015). Social Media Usage: 2005-2015. *Internet & Technology*. https://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.
Petkovic, M., & Jonker, W. (2007). *Security, Privacy, and Trust in Modern Data Management*: New York: Springer.
Potgieter, P. (2019). The Awareness Behaviour of Students On Cyber Security Awareness by Using

Social Media Platforms: A Case Study at Central University of Technology. *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, *12*, 272–280. https://doi.org/10.29007/gprf

Raber, F., Kosmalla, F., & Krueger, A. (2017). *Fine-Grained Privacy Setting Prediction Using a Privacy Attitude Questionnaire and Machine Learning.* Proceedings of 16th IFIP Conference on Human-Computer Interaction (INTERACT).

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, *421*, 43-69.

Rebovich, D. J., Allen, C. K., & Platt, J. (2015). The New Face of Identity Theft. *Center for Identity Management and Information Protection Utica College.*

Remenyi, D., & Money, A. H. (2012). *Research Supervision for Supervisors and Students* (Second). United Kingdom: Academic Conferences Limited.

Reyns, B. W., & Henson, B. (2016). The Thief with a Thousand Faces and the Victim with None: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119–1139. https://doi.org/10.1177/0306624X15572861

Ritter, J. (2015). Contemporary digital information assets require new look at governance. Retrieved from https://searchcompliance.techtarget.com/tip/Contemporary-digital-information-assets-require-new-look-at-governance

Salehi, M., Khalili, M. N., Hojjat, S. K., Salehi, M., & Danesh, A. (2014). Prevalence of internet addiction and associated factors among medical students from Mashhad, Iran in 2013. *Iranian Red Crescent Medical Journal*, *16*(5). https://doi.org/10.5812/ircmj.17256

Saltzman, J., & Price, M. (2017). Analyzing Neutral Responses to the Maryland Physics Expectation Survey. *Proceedings at the APS March Meeting Abstracts.*

Sattarova Feruza, Y., & Kim, T.-h. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering*, *2*(2), 17-31.

Scott, J. (2017). *Social Network Analysis* (Fourth). London: SAGE Publications.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*: Chichester: John Wiley & Sons.

Sharma, R. (2012). Study of latest emerging trends on cyber security and its challenges to society. *International Journal of Scientific & Engineering Research*, *3*(6), 1.

Shen, G., Yang, F., & Zhou, L. (2015). Usable security of online password management with sensor-based authentication. Washington: U.S. Patent and Trademark Office.

Šincek, D. (2014). Gender differences in cyber-bullying. *Proceedings of International Multidisciplinary Scientific Conference Social Sciences and Arts SGEM2014.* https://doi.org/10.5593/SGEMSOCIAL2014/B11/S1.026

Singh, N., Chandwani, S., Singh, J., & Kumar, D. (2019). Exploration of Level of Computer Anxiety among Veterinary Students. *Library Philosophy and Practice*.

Sinha, A., Li, Y., & Bauer, L. (2013). *What you want is not what you get: predicting sharing policies for text-based content on facebook.* Proceedings of the 2013 ACM workshop on Artificial intelligence and security. https://doi.org/10.1145/2517312.2517317

Siomos, K. E., Dafouli, E. D., Braimiotis, D. A., Mouzas, O. D., & Angelopoulos, N. V. (2008). Internet addiction among Greek adolescent students. *CyberPsychology & Behavior*, *11*(6), 653-657. https://doi.org/10.1089/cpb.2008.0088

Sjoberg, L. (2009). Gender and international security: Feminist perspectives (First). London: Routledge. https://doi.org/10.4324/9780203866931

Slonka, K. J. (2014). *Awareness of malicious social engineering among facebook users*. [Robert Morris University].

Song, Y.-S., Lew, C., Song, A., & Song, V. (2018). Privacy protected anti identity theft and payment network. United States of America: Patent and Trademark Office.

Spence, J. T., & Helmreich, R. L. (1980). Masculine Instrumentality and Feminine Expressiveness: Their Relationships with Sex Role Attitudes and Behaviors. *Psychology of Women Quarterly*, *5*(2), 147–163. https://doi.org/10.1111/j.1471-6402.1980.tb00951.x

Such, J. M., & Criado, N. (2018). Multiparty privacy in social media. *Communications of the ACM, 61*(8), 74-81.https://doi.org/10.1145/3208039

Techophedia (2018). *Multi-Processing.* Retrieved from http://www.techopedia.com/definition/3393/multi-processing.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology, 32*(10), 1014-1023. https://doi.org/10.1080/0144929X.2013.763860

Tewari, A. (2015). *Detection and Classification of Spam and Phishing Emails*. [National Institute of Technology].

Thabethe, N. (2016). *Impact of Internet use on social relationships in teenagers.* [University of Zululand].

Thompson, S. T. C. (2006). Helping the Hacker? Library Information, Security, and Social Engineering. *Information Technology & Libraries, 25*(4), 222-225. https://doi.org/10.6017/ital.v25i4.3355

Tickner, J. A. (1992). *Gender in international relations: Feminist perspectives on achieving global security*. New York: Columbia University Press.

TimesLive. (2017). SA hits 'landmark' as half of adults on internet. Retrieved from https://www.timeslive.co.za/news/sci-tech/2017-07-20-sa-hits-landmark-as-half-of-adults-on-internet/

Tiwari, A. (2018). What Is Social Engineering? What Are Different Types Of Social Engineering Attacks? *Fossbytes*. Retrieved from https://fossbytes.com/what-is-social-engineering-types-techniques/

Trauth, E. M. (2013). The role of theory in gender and information systems research. *Information and Organization, 23*(4), 277–293. https://doi.org/10.1016/j.infoandorg.2013.08.003

Tsarwe, S. (2016). Mobility, connectivity and sociability: the dialectical tension of the mobile phone's prospects for feminist emancipatory politics. *African Journalism Studies, 37*(4), 5-24. https://doi.org/10.1080/23743670.2016.1256055

Twenge, J. M. (1997). Changes in masculine and feminine traits over time: A meta-analysis. *Sex roles, 36*(5-6), 305-325. https://doi.org/10.1007/BF02766650

Van Rensburg, K. S. J. (2017). *The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa.* [Univeristy of South Africa].

Vanderhoven, E., Schellens, T., Valcke, M., & Raes, A. (2014). How safe do teenagers behave on Facebook? An observational study. *PLOS ONE, 9*(8). https://doi.org/10.1371/journal.pone.0104036

Veltri, N., Krasnova, H., Baumann, A., & Kalayamthanam, N. (2014). Gender Differences in Online Gaming: A Literature Review. *AMCIS.* https://doi.org/10.7892/BORIS.68896

Vieraitis, L. M., Copes, H., Powell, Z. A., & Pike, A. (2015). A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior, 20*, 10-18. https://doi.org/10.1016/j.avb.2014.12.008

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

Wakama, A. (2014). South Africa is second most targeted for Phishing Attacks. *IT News Africa*. Retrieved from https://www.itnewsafrica.com/2014/04/south-africa-is-second-most-targeted-for-phishing-attacks/

Walker, C. M., Sockman, B. R., & Koehn, S. (2011). An Exploratory Study of Cyberbullying with Undergraduate University Students. *TechTrends, 55*(2), 31-38. https://doi.org/10.1007/s11528-011-0481-0

Wallace, P. (2014). Internet addiction disorder and youth: There are growing concerns about compulsive online activity and that this could impede students' performance and social lives. *EMBO Reports, 15*(1), 12–16. https://doi.org/10.1002/embr.201338222

Watson, J. (2015). Predicting privacy settings with a user-centered approach. *2015 International Conference on Collaboration Technologies and Systems (CTS).* https://doi.org/10.1109/CTS.2015.7210443

Welsh, A. (2015). *The Identity Theft Protection Guide:*Safeguard Your Family *Protect Your Privacy *Recover a Stolen Identity*. United States of America: St. Martin's Griffin.

Whitman, M., & Mattord, H. (2014). Principles of Information Security (Fifth). Boston, MA: Course Technology.

Wibben, A. T. (2010). *Feminist security studies: A narrative approach*. Canada: Routledge.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72,* 412-421. https://doi.org/10.1016/j.chb.2017.03.002

Wolf, A. (2000). Emotional expression online: Gender differences in emoticon use. *CyberPsychology & Behavior, 3*(5), 827-833. https://doi.org/10.1089/10949310050191809

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674. https://doi.org/10.1002/asi.20779

Wüest, C. (2010). The risks of social networking. *Symantec Corporation*.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311-325.

Yu, S. (2014). Fear of cyber crime among college students in the United States of America: An exploratory study. *International Journal of Cyber Criminology, 8*(1).

Zhang, M. W., Tran, B. X., Hinh, N. D., Nguyen, H. L. T., Tho, T. D., Latkin, C., & Ho, R. C. (2017). Internet addiction and sleep quality among Vietnamese youths. *Asian Journal of Psychiatry, 28*, 15-20. https://doi.org/10.1016/j.ajp.2017.03.025

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742. https://doi.org/10.1002/sec.795

APPENDICES

APPENDIX A: ETHICAL CLEARANCE

21 August 2018

Ms Happyness Nothando Ngwane (210527408)
School of Management, IT & Governance
Pietermaritzburg Campus

Dear Ms Ngwane,

Protocol reference number: HSS/0879/018M
Project Title: Gender Responses Towards Online Social Engineering Attacks amongst Young Adult Students in South Africa, Pietermaritzburg

Approval Notification – Expedited Application

In response to your application received 09 July 2018, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the 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.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....
Professor Shenuka Singh (Chair)

/ms

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Isabel Martins
Cc School Administrator: Ms Debbie Cunynghame

Humanities & Social Sciences Research Ethics Committee
Professor Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** simbaza@ukzn.ac.za / snymanm@ukzn.ac.za / hmohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville

APPENDIX B: NEW ETHICAL CLEARANCE

4 February 2019

Ms Happyness Nothando Ngwane (210527408)
School of Management, IT & Governance
Pietermaritzburg Campus

Dear Ms Ngwane,

Protocol reference number: HSS/0879/018M
New Project Title: Gender Responses Towards Online Social Engineering Attacks amongst Young Adult Students in South Africa.

Approval notification – Amendment Application

This letter serves to notify you that your application for an amendment dated 31January 2019 has now been granted **Full Approval** as follows:

- **Change in Title**

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

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol.

Yours faithfully

.....
Dr Shamila Naidoo (Deputy Chair)
Humanities & Social Sciences Research Ethics Committee

/pm

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Isabel Martins
Cc School Administrator: Ms Debbie Cunynghame

Humanities & Social Sciences Research Ethics Committee
Professor Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** [illegible]
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville

APPENDIX C: QUESTIONNAIRE

Questionnaire
Gender Responses Towards Online Social Engineering Attacks amongst Young Adult Students in South Africa, Pietermaritzburg

Researcher: Happyness Ngwane
Supervisor: Professor Manoj Maharaj

Discipline of Information Systems & Technology
College of Law and Management Studies
University of KwaZulu-Natal
Pietermaritzburg campus

- Please note that there are no correct/incorrect answer.
- Please note that participation in the study is voluntary.
- Please sign the letter of informed consent, giving me permission to use your responses for this research project.
- Please kindly take note of the **"general instruction"** while filling this questionnaire.

GENERAL INSTRUCTION: In all the sections, kindly provide your response by making a tick **(√)** in the appropriate box and fill in the gaps in the case of open-ended questions.

SECTION A: DEMOGRAPHIC INFORMATION

1.	Your gender:	☐ Male	☐ Female			
2.	Your age:	☐ 18 - 20	☐ 21 – 23	☐ 24 - 26	☐ 27 or older	
3.	Your race:	☐ African	☐ Coloured	☐ Indian	☐ White	☐ Do not wish to Answer
4.	Institution:	☐ UKZN	☐ UMgungundlovu FET			
5.	Faculty:	☐ Art/ Drama	☐ Health Sciences	☐ Law / Management	☐ Social Sciences	☐ Science/ Technology

SECTION B: AWARENESS

- Please categorise the following examples
- Please note that there is only **one** category per example

EXAMPLES		**Cyber -crime**	**Phishing attack**	**Malware**	**Email spam**	**Identity theft**	**I do not know**
1.	Emails that usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password						
2.	The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name, and perhaps to the other person's disadvantage or loss						
3.	The below points are all examples of…? - Hacking into computer systems - Introducing viruses to vulnerable networks - Identity theft - Credit card theft						
4.	A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar						

	websites but in fact lead to phishing web sites or sites that are hosting malware						
5.	Any piece of software that was written with the intention of doing harm to information, devices or to people						

6.	**QUESTION**	**OPTIONS**
6.1	Which of the options presented do you believe represents the most important reason behind online privacy on social networks	☐ Prevention of identity theft
6.2		☐ Protection of my information
6.3		☐ Hiding my images and contact information from Unknowns
6.4		☐ I do not know
7.	**QUESTION**	**OPTIONS**
7.1	Which of these actions do you believe can help to safeguard your information on social network sites	☐ Install an antivirus software
7.2		☐ Leave my social network logon active even when I am not at the computer
7.3		☐ Not changing my password
7.4		☐ I do not know

SECTION C: USER'S RESPONSES

1.	I am cautious when opening email attachments	☐ Yes	☐ No
2.	There is no threat in responding to emails which come from a known source (e.g.: friend or lecturer)	☐ Yes	☐ No

		Always (100% of the time)	**Often (75% of the time)**	**Sometimes (50% of the time)**	**Rarely (25%of the time)**	**Never (0% of the time)**	**I do not know how to**
3.	I attend to security alerts that come up at login on social media sites						
4.	I check my privacy controls and settings on my social media sites						
5.	I check for viruses when I download a file from my emails						
6.	I check for viruses when I open an email attachment						

7.	**QUESTION**	**Category**	**Question**	**Received**		**Responded**	
7.1	Have you ever received a	Email message	that you suspect was an attempt to get your personal details?	☐ Yes	☐ No	☐ Yes	☐ No
7.2		Link		☐ Yes	☐ No	☐ Yes	☐ No
7.3		Online pop-up		☐ Yes	☐ No	☐ Yes	☐ No

7.4		Social media message		☐ Yes	☐ No	☐ Yes	☐ No

SECTION D: ATTITUDES

		Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
1.	Online security is important					
2.	Online security is necessary					
3.	Online security is outside the user's control					
		Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
4.	I am not concerned about online security					
5.	I am not concerned about online security when responding to a friend					
6.	I am concerned about online security when responding to an unknown source					
7.	I would like to be taught about information security					

SECTION F: BEHAVIOUR

1.	I reveal my real name on social networks	☐ Yes	☐ No
2.	I reveal my email address on social networks	☐ Yes	☐ No

3.	**QUESTION**	**Category**	**Accepted**	
3.1	Have you ever accepted a friend request on social media from	Someone you do not know	☐ Yes	☐ No
3.2		A friend of a friend	☐ Yes	☐ No
3.3		Someone you have mutual friends with	☐ Yes	☐ No
3.4		Someone you think you know	☐ Yes	☐ No

		Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
4.	Using privacy settings is time consuming					
5.	Privacy settings are complicated					
6.	I consider my information safe on social networks					
7.	Using privacy settings on social networks would require a considerable amount of effort					
8.	There is too much work associated with trying to increase my information protection through the use of privacy settings					

	Daily	**Weekly**	**Monthly**	**Yearly**	**Never**

9.	How often do you change your social network passwords across your social networks					
10.	How often do you check in on social networks					

		Very concerned	**Somewhat concerned**	**Not too concerned**	**Not at all concerned**
11.	How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge				

		Right at the beginning	**After I figured out how to**	**After having a profile for a while**	**I have never changed the settings**	**I do not know how to**
12.	When did you change your privacy settings on social networks since creating your profile					
13.	When did you change your privacy settings on your email (i.e. Gmail) since creating your profile					

QUESTION 15 TO 18:

- Please select the most appropriate option
- Please choose **one** option per question

14.	**QUESTION**	**OPTIONS**
14.1	Which of these do you believe is **NOT** a good way to secure your password	☐ To memorise it
14.2		☐ To write it down (e.g.: paper, notebook)
14.3		☐ Write it down but only in a secured place and with no title information (e.g.: sticky note)
14.4		☐ I do not know
15.	**QUESTION**	**OPTIONS**
15.1	What will you do when somebody close to you (such as your partner) requests your social network's password (e.g.: Facebook password)	☐ Give it to him/her the password
15.2		☐ Give it to him/her by typing it in
15.3		☐ Ask questions and give him/her if you are Convinced
15.4		☐ Say no
16.	**QUESTION**	**OPTIONS**
16.1	Which of these is in line with your belief about privacy on social network	☐ It is necessary and important
16.2		☐ It should be optional depending on what you have to protect
16.3		☐ It is totally outside my control
16.4		☐ I am not concerned about privacy
17.	**QUESTION**	**OPTIONS**

17.1	Which of these describe reasons behind hiding your profile information (e.g.: hometown, cell phone number)	☐ My information might be stolen
17.2		☐ I don't feel secured on social networks generally
17.3		☐ I just choose not to put original personal information on my profile
17.4		☐ I do not hide any personal information

18.	**QUESTION**	**Category**	**Would you verify the caller/ sender**		**Would you respond without verifying the caller/ sender**		**After verifying the caller/ sender would you respond**	
18.1	Under what circumstance would you provide personally identifiable information (e.g.: identity number)	Random telephone call	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
18.2		Random email message	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
18.3		Someone close calling (friend)	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
18.4		Someone close emailing (friend)	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
18.5		Social network direct message	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No

19.	**QUESTION**	**Category**	**Would you verify the caller/ sender**		**Would you respond without verifying the caller/ sender**		**After verifying the caller/ sender would you respond**	
19.1	Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number)	Random telephone	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
19.2		Random email message	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
19.3		Someone close calling (friend)	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
19.4		Someone close emailing (friend)	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No
19.5		Social network direct message	☐ Yes	☐ No	☐ Yes	☐ No	☐ Yes	☐ No

THANK YOU FOR YOUR TIME!!!

☺

APPENDIX D: RELIABILITY TEST

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation
Gender	248.11	131.633	.093
Age	247.58	131.932	.010
Race	248.11	135.063	-.137
Institution	248.40	129.619	.314
Faculty	246.06	133.319	-.063
Emails that usually appear to come from a well-known organization and ask for your personal information - such as credit card number, account number or password	246.12	124.155	.145
The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss	245.29	125.091	.143
The below points are all examples of...? -Hacking into computer systems -Introducing viruses to vulnerable networks -Identity theft -Credit card theft	247.20	116.467	.286
A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware	246.05	125.211	.170
Any piece of software that was written with the intention of doing harm to information, devices or to people	246.25	123.974	.162
Which of the options presented do you believe represents the most important reason behind online privacy on social networks	247.69	128.976	.179
Which of these actions do you believe can help to safeguard your information on social network sites	247.75	127.377	.138
I am cautious when opening email attachments	248.97	132.880	-.014
There is no threat in responding to emails which come from a known source (e.g.: friend or lecturer)	249.04	133.040	-.030
I attend to security alerts that come up at login on social media sites	245.61	129.816	.031
I check my privacy controls and settings on my social media sites	245.50	126.706	.138
I check for viruses when I download a file from my emails	246.03	125.333	.153
I check for viruses when I open an email attachment	246.24	123.499	.213
Have you ever received an email message that you suspect was an attempt to get your personal details	248.40	132.257	.049
Have you ever responded to an email message that you suspect was an attempt to get your personal details	245.88	131.709	.112
Have you ever received a link that you suspect was an attempt to get your personal details	248.32	130.746	.182
Have you ever responded to a link that you suspect was an attempt to get your personal details	245.80	131.478	.169
Have you ever received an online pop-up that you suspect was an attempt to get your personal details	248.30	130.237	.225
Have you ever responded to an online pop-up that you suspect was an attempt to get your personal details	245.78	131.936	.122

Have you ever received an social media message that you suspect was an attempt to get your personal details	248.41	131.854	.091
Have you ever responded to an social media message that you suspect was an attempt to get your personal details	245.99	132.872	-.014
Online security is important	244.85	133.600	-.079
Online security is necessary	245.01	134.153	-.110
Online security is outside the user's control	246.54	129.071	.094
I am not concerned about online security	247.40	129.947	.042
I am not concerned about online security when responding to a friend	246.75	132.152	-.033
I am concerned about online security when responding to an unknown source	245.56	132.941	-.054
I would like to be taught about information security	245.22	133.875	-.083
I reveal my real name on social networks	248.93	132.989	-.024
I reveal my email address on social networks	249.15	132.731	-.003
Have you ever accepted a friend request on social media from someone you do not know	248.82	132.942	-.016
Have you ever accepted a friend request on social media from a friend of a friend	248.76	133.093	-.035
Have you ever accepted a friend request on social media from someone you have mutual friends with	248.73	133.077	-.034
Have you ever accepted a friend request on social media from someone you think you know	248.77	133.279	-.060
Using privacy settings is time consuming	246.55	125.387	.224
Privacy settings are complicated	246.60	126.935	.181
I consider my information safe on social networks	246.80	127.870	.123
Using privacy settings on social networks would require a considerable amount of effort	246.56	126.903	.184
There is too much work associated with trying to increase my information protection through the use of privacy settings	246.42	126.817	.191
How often do you change your social network passwords across your social networks	248.08	130.111	.115
How often do you check in on social networks	245.26	131.976	-.003
How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge	246.48	132.839	-.035
When did you change your privacy settings on social networks since creating your profile	246.30	128.917	.107
When did you change your privacy settings on your email (i.e. Gmail) since creating your profile	246.45	130.259	.046
Which of these do you believe is NOT a good way to secure your password	247.55	130.848	.083
What would you do when somebody close to you (such as your partner) requests your social network's password (e.g.: Facebook password)	246.45	131.704	.013
Which of these is in line with your belief about privacy on social network	248.12	130.498	.090
Which of these describe reasons behind hiding your profile information (e.g.: hometown, cell phone number)	247.72	132.370	-.016
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you verify the caller	248.20	129.741	.260
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	245.72	133.120	-.043
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	244.05	130.161	.228

Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you verify the sender	248.09	129.656	.270
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you respond without verifying the sender	245.72	133.231	-.064
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, after verifying the sender would you respond	243.93	130.645	.207
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you verify the caller	248.20	131.430	.110
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you respond without verifying the caller	245.91	132.772	-.002
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, after verifying the caller would you respond	244.07	130.517	.194
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you verify the sender	248.11	130.713	.174
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	245.88	131.809	.100
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	243.97	130.310	.229
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you verify the sender	248.07	129.631	.273
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	245.80	133.323	-.063
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	243.90	130.212	.261
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you verify the caller	248.17	129.876	.247
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	245.79	133.248	-.054
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	243.98	130.500	.209
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you verify the sender	248.12	128.791	.344
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you respond without verifying the sender	245.78	133.684	-.111
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, after verifying the sender would you respond	243.94	129.872	.279

Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you verify the caller	248.14	131.313	.120
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you respond without verifying the caller	245.92	132.799	-.005
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, after verifying the caller would you respond	244.03	130.843	.168
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you verify the sender	248.13	130.584	.185
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	245.91	133.175	-.042
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	244.00	130.278	.225
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you verify the sender	248.10	129.346	.296
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	245.79	133.607	-.101
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	243.93	129.840	.285

APPENDIX E: NORMALITY TESTS

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Gender	.369	361	.000	.632	361	.000
Age	.270	361	.000	.843	361	.000
Race	.453	361	.000	.593	361	.000
Institution	.464	361	.000	.545	361	.000
Faculty	.202	361	.000	.854	361	.000
Emails that usually appear to come from a well-known organization and ask for your personal information - such as credit card number, account number or password	.199	361	.000	.880	361	.000
The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss	.422	361	.000	.668	361	.000
The below points are all examples of...? -Hacking into computer systems -Introducing viruses to vulnerable networks -Identity theft -Credit card theft	.364	361	.000	.688	361	.000
A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware	.200	361	.000	.895	361	.000
Any piece of software that was written with the intention of doing harm to information, devices or to people	.270	361	.000	.846	361	.000
Which of the options presented do you believe represents the most important reason behind online privacy on social networks	.291	361	.000	.817	361	.000
Which of these actions do you believe can help to safeguard your information on social network sites	.400	361	.000	.659	361	.000
I am cautious when opening email attachments	.438	361	.000	.582	361	.000
There is no threat in responding to emails which come from a known source (e.g.: friend or lecturer)	.402	361	.000	.616	361	.000
I attend to security alerts that come up at login on social media sites	.157	361	.000	.917	361	.000
I check my privacy controls and settings on my social media sites	.177	361	.000	.913	361	.000
I check for viruses when I download a file from my emails	.153	361	.000	.914	361	.000
I check for viruses when I open an email attachment	.189	361	.000	.907	361	.000
Have you ever received an email message that you suspect was an attempt to get your personal details	.463	361	.000	.547	361	.000
Have you ever responded to an email message that you suspect was an attempt to get your personal details	.484	361	.000	.507	361	.000
Have you ever received a link that you suspect was an attempt to get your personal details	.424	361	.000	.597	361	.000
Have you ever responded to a link that you suspect was an attempt to get your personal details	.517	361	.000	.409	361	.000
Have you ever received an online pop-up that you suspect was an attempt to get your personal details	.412	361	.000	.609	361	.000

Have you ever responded to an online pop-up that you suspect was an attempt to get your personal details	.525	361	.000	.372	361	.000
Have you ever received an social media message that you suspect was an attempt to get your personal details	.468	361	.000	.538	361	.000
Have you ever responded to an social media message that you suspect was an attempt to get your personal details	.420	361	.000	.613	361	.000
Online security is important	.486	361	.000	.423	361	.000
Online security is necessary	.423	361	.000	.581	361	.000
Online security is outside the user's control	.193	361	.000	.911	361	.000
I am not concerned about online security	.253	361	.000	.822	361	.000
I am not concerned about online security when responding to a friend	.170	361	.000	.898	361	.000
I am concerned about online security when responding to an unknown source	.298	361	.000	.727	361	.000
I would like to be taught about information security	.372	361	.000	.647	361	.000
I reveal my real name on social networks	.459	361	.000	.554	361	.000
I reveal my email address on social networks	.347	361	.000	.636	361	.000
Have you ever accepted a friend request on social media from someone you do not know	.508	361	.000	.441	361	.000
Have you ever accepted a friend request on social media from a friend of a friend	.530	361	.000	.347	361	.000
Have you ever accepted a friend request on social media from someone you have mutual friends with	.539	361	.000	.268	361	.000
Have you ever accepted a friend request on social media from someone you think you know	.528	361	.000	.357	361	.000
Using privacy settings is time consuming	.179	361	.000	.913	361	.000
Privacy settings are complicated	.204	361	.000	.906	361	.000
I consider my information safe on social networks	.181	361	.000	.908	361	.000
Using privacy settings on social networks would require a considerable amount of effort	.189	361	.000	.913	361	.000
There is too much work associated with trying to increase my information protection through the use of privacy settings	.189	361	.000	.912	361	.000
How often do you change your social network passwords across your social networks	.343	361	.000	.708	361	.000
How often do you check in on social networks	.384	361	.000	.642	361	.000
How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge	.290	361	.000	.804	361	.000
When did you change your privacy settings on social networks since creating your profile	.175	361	.000	.908	361	.000
When did you change your privacy settings on your email (i.e. Gmail) since creating your profile	.160	361	.000	.909	361	.000
Which of these do you believe is NOT a good way to secure your password	.351	361	.000	.784	361	.000

What would you do when somebody close to you (such as your partner) requests your social network's password (e.g.: Facebook password)	.289	361	.000	.759	361	.000
Which of these is in line with your belief about privacy on social network	.380	361	.000	.673	361	.000
Which of these describe reasons behind hiding your profile information (e.g.: hometown, cell phone number)	.242	361	.000	.818	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you verify the caller	.365	361	.000	.633	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	.540	361	.000	.247	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	.396	361	.000	.620	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you verify the sender	.379	361	.000	.629	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you respond without verifying the sender	.540	361	.000	.247	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, after verifying the sender would you respond	.459	361	.000	.554	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you verify the caller	.365	361	.000	.633	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you respond without verifying the caller	.468	361	.000	.538	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, after verifying the caller would you respond	.386	361	.000	.625	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you verify the sender	.367	361	.000	.633	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	.480	361	.000	.515	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	.440	361	.000	.580	361	.000

Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you verify the sender	.385	361	.000	.626	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	.517	361	.000	.409	361	.000
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	.472	361	.000	.531	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you verify the caller	.347	361	.000	.636	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	.519	361	.000	.400	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	.434	361	.000	.587	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you verify the sender	.360	361	.000	.634	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you respond without verifying the sender	.518	361	.000	.403	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, after verifying the sender would you respond	.452	361	.000	.564	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you verify the caller	.349	361	.000	.636	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you respond without verifying the caller	.464	361	.000	.545	361	.000

Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you verify the sender	.357	361	.000	.635	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	.467	361	.000	.540	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	.423	361	.000	.599	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you verify the sender	.372	361	.000	.631	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	.521	361	.000	.391	361	.000
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	.456	361	.000	.558	361	.000

APPENDIX F: DESCRIPTIVE STATISTICS

Item Statistics

	Mean	Std. Deviation	N
Gender	1.55	.498	361
Age	2.07	.896	361
Race	1.55	.951	361
Institution	1.26	.438	361
Faculty	3.60	1.111	361
Emails that usually appear to come from a well-known organization and ask for your personal information - such as credit card number, account number or password	3.54	1.759	361
The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss	4.37	1.628	361
The below points are all examples of...? -Hacking into computer systems -Introducing viruses to vulnerable networks -Identity theft -Credit card theft	2.46	2.014	361
A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware	3.61	1.466	361
Any piece of software that was written with the intention of doing harm to information, devices or to people	3.40	1.691	361
Which of the options presented do you believe represents the most important reason behind online privacy on social networks	1.97	.814	361
Which of these actions do you believe can help to safeguard your information on social network sites	1.91	1.271	361
I am cautious when opening email attachments	.69	.463	361
There is no threat in responding to emails which come from a known source (e.g.: friend or lecturer)	.62	.487	361
I attend to security alerts that come up at login on social media sites	4.05	1.448	361
I check my privacy controls and settings on my social media sites	4.16	1.386	361
I check for viruses when I download a file from my emails	3.63	1.533	361
I check for viruses when I open an email attachment	3.42	1.513	361
Have you ever received an email message that you suspect was an attempt to get your personal details	1.26	.439	361
Have you ever responded to an email message that you suspect was an attempt to get your personal details	3.78	.412	361
Have you ever received a link that you suspect was an attempt to get your personal details	1.34	.474	361
Have you ever responded to a link that you suspect was an attempt to get your personal details	3.86	.346	361
Have you ever received an online pop-up that you suspect was an attempt to get your personal details	1.36	.481	361
Have you ever responded to an online pop-up that you suspect was an attempt to get your personal details	3.88	.321	361
Have you ever received an social media message that you suspect was an attempt to get your personal details	1.25	.433	361
Have you ever responded to an social media message that you suspect was an attempt to get your personal details	3.66	.479	361
Online security is important	4.81	.488	361
Online security is necessary	4.65	.637	361
Online security is outside the user's control	3.12	1.170	361
I am not concerned about online security	2.25	1.317	361
I am not concerned about online security when responding to a friend	2.91	1.342	361
I am concerned about online security when responding to an unknown source	4.10	1.242	361
I would like to be taught about information security	4.43	.938	361
I reveal my real name on social networks	.73	.444	361
I reveal my email address on social networks	.51	.501	361

Have you ever accepted a friend request on social media from someone you do not know	.84	.368	361
Have you ever accepted a friend request on social media from a friend of a friend	.90	.304	361
Have you ever accepted a friend request on social media from someone you have mutual friends with	.93	.249	361
Have you ever accepted a friend request on social media from someone you think you know	.89	.311	361
Using privacy settings is time consuming	3.11	1.212	361
Privacy settings are complicated	3.06	1.147	361
I consider my information safe on social networks	2.86	1.257	361
Using privacy settings on social networks would require a considerable amount of effort	3.10	1.143	361
There is too much work associated with trying to increase my information protection through the use of privacy settings	3.24	1.127	361
How often do you change your social network passwords across your social networks	1.58	.820	361
How often do you check in on social networks	4.40	1.020	361
How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge	3.18	.919	361
When did you change your privacy settings on social networks since creating your profile	3.36	1.129	361
When did you change your privacy settings on your email (i.e. Gmail) since creating your profile	3.21	1.196	361
Which of these do you believe is NOT a good way to secure your password	2.11	.781	361
What would you do when somebody close to you (such as your partner) requests your social network's password (e.g.: Facebook password)	3.20	.973	361
Which of these is in line with your belief about privacy on social network	1.54	.843	361
Which of these describe reasons behind hiding your profile information (e.g.: hometown, cell phone number)	1.94	.969	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you verify the caller	1.45	.499	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	3.94	.234	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	5.61	.489	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you verify the sender	1.57	.495	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, would you respond without verifying the sender	3.94	.234	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a random email message, after verifying the sender would you respond	5.73	.444	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you verify the caller	1.45	.499	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, would you respond without verifying the caller	3.75	.433	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close calling, after verifying the caller would you respond	5.59	.493	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you verify the sender	1.55	.498	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	3.78	.418	361

Under what circumstance would you provide personally identifiable information (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	5.69	.462	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you verify the sender	1.58	.493	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	3.86	.346	361
Under what circumstance would you provide personally identifiable information (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	5.76	.428	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you verify the caller	1.49	.501	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, would you respond without verifying the caller	3.87	.340	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random telephone call, after verifying the caller would you respond	5.68	.467	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you verify the sender	1.54	.499	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, would you respond without verifying the sender	3.88	.333	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a random email message, after verifying the sender would you respond	5.72	.451	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you verify the caller	1.52	.500	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, would you respond without verifying the caller	3.74	.438	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close calling, after verifying the caller would you respond	5.63	.485	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you verify the sender	1.53	.500	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, would you respond without verifying the sender	3.75	.435	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) to someone close emailing, after verifying the sender would you respond	5.66	.475	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you verify the sender	1.56	.497	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, would you respond without verifying the sender	3.87	.334	361
Under what circumstance would you provide personally identifiable information knowing you stand a chance to win something (e.g.: identity number) over a social network direct message, after verifying the sender would you respond	5.73	.447	361

APPENDIX G: CROSS TABULATIONS AND CHI-SQUARE TESTS

Cross tabulation between gender and phishing attack awareness

			Emails that usually appear to come from a well-known organization and ask for your personal information - such as credit card number, account number or password						
			Cyber-crime	**Phishing attack**	Malware	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	22	**42**	3	54	14	26	161
		% within Gender	13.7%	**26.1%**	1.9%	33.5%	8.7%	16.1%	100.0%
	Female	Count	41	**30**	8	56	18	47	200
		% within Gender	20.5%	**15.0%**	4.0%	28.0%	9.0%	23.5%	100.0%
Total		Count	63	**72**	11	110	32	73	361
		% within Gender	17.5%	**19.9%**	3.0%	30.5%	8.9%	20.2%	100.0%

Chi-square tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.513[a]	5	.028
Likelihood Ratio	12.631	5	.027
Linear-by-Linear Association	.609	1	.435
N of Valid Cases	361		

Cross tabulation between gender and identity theft awareness

			The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss						
			Cyber-crime	Phishing attack	Malware	Email spam	**Identity theft**	I do not know	Total
Gender	Male	Count	28	5	2	3	**108**	15	161
		% within Gender	17.4%	3.1%	1.2%	1.9%	**67.1%**	9.3%	100.0%
	Female	Count	29	7	2	7	**117**	38	200
		% within Gender	14.5%	3.5%	1.0%	3.5%	**58.5%**	19.0%	100.0%
Total		Count	57	12	4	10	**225**	53	361
		% within Gender	15.8%	3.3%	1.1%	2.8%	**62.3%**	14.7%	100.0%

	The deliberate use of someone else's name, usually as a method to gain a financial advantage or obtain credit and other benefits in the person's name and perhaps to the other persons disadvantage or loss	Total

			Cyber-crime	Phishing attack	Malware	Email spam	**Identity theft**	I do not know	
Gender	Male	Count	28	5	2	3	**108**	15	161
		% within Gender	17.4%	3.1%	1.2%	1.9%	**67.1%**	9.3%	100.0%
	Female	Count	29	7	2	7	**117**	38	200
		% within Gender	14.5%	3.5%	1.0%	3.5%	**58.5%**	19.0%	100.0%
Total		Count	57	12	4	10	**225**	53	361
		% within Gender	15.8%	3.3%	1.1%	2.8%	**62.3%**	14.7%	100.0%

Chi-square tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.174[a]	5	.147
Likelihood Ratio	8.457	5	.133
Linear-by-Linear Association	1.204	1	.272
N of Valid Cases	361		

Cross tabulation between gender and cyber-crime awareness

			The below points are all examples of...? -Hacking into computer systems -Introducing viruses to vulnerable networks -Identity theft -Credit card theft						
			Cyber-crime	Phishing attack	Malware	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	**110**	7	11	1	11	21	161
		% within Gender	**68.3%**	4.3%	6.8%	.6%	6.8%	13.0%	100.0%
	Female	Count	**106**	9	19	9	14	43	200
		% within Gender	**53.0%**	4.5%	9.5%	4.5%	7.0%	21.5%	100.0%
Total		Count	**216**	16	30	10	25	64	361
		% within Gender	**59.8%**	4.4%	8.3%	2.8%	6.9%	17.7%	100.0%

Chi-square tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.715[a]	5	.026
Likelihood Ratio	13.704	5	.018
Linear-by-Linear Association	7.940	1	.005
N of Valid Cases	361		

Cross tabulation between gender and email spam awareness

			A type of unwanted electronic messages. The messages may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware						
			Cyber-crime	Phishing attack	Malware	**Email spam**	Identity theft	I do not know	Total
Gender	Male	Count	6	37	24	**69**	2	23	161
		% within Gender	3.7%	23.0%	14.9%	**42.9%**	1.2%	14.3%	100.0%
	Female	Count	16	41	31	**67**	3	42	200
		% within Gender	8.0%	20.5%	15.5%	**33.5%**	1.5%	21.0%	100.0%
Total		Count	22	78	55	**136**	5	65	361
		% within Gender	6.1%	21.6%	15.2%	**37.7%**	1.4%	18.0%	100.0%

Chi-square tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.297[a]	5	.199
Likelihood Ratio	7.460	5	.189
Linear-by-Linear Association	.114	1	.736
N of Valid Cases	361		

Cross tabulation between gender and malware awareness

			Any piece of software that was written with the intention of doing harm to information, devices or to people						
			Cyber-crime	Phishing attack	**Malware**	Email spam	Identity theft	I do not know	Total
Gender	Male	Count	20	13	**98**	7	2	21	161
		% within Gender	12.4%	8.1%	**60.9%**	4.3%	1.2%	13.0%	100.0%
	Female	Count	38	20	**55**	18	4	65	200
		% within Gender	19.0%	10.0%	**27.5%**	9.0%	2.0%	32.5%	100.0%
Total		Count	58	33	**153**	25	6	86	361
		% within Gender	16.1%	9.1%	**42.4%**	6.9%	1.7%	23.8%	100.0%

Chi-square tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	43.468[a]	5	.000
Likelihood Ratio	44.507	5	.000
Linear-by-Linear Association	7.633	1	.006

N of Valid Cases	361		

			Which of the options presented do you believe represents the most important reason behind online privacy on social networks				
			Prevention of Identity Theft	Protection of my Information	Hiding my Image and contact info from unknowns	I dont know	Total
Gender	Male	Count	47	89	17	8	161
		% within Gender	29.2%	55.3%	10.6%	5.0%	100.0%
	Female	Count	56	99	31	14	200
		% within Gender	28.0%	49.5%	15.5%	7.0%	100.0%
Total		Count	103	188	48	22	361
		% within Gender	28.5%	52.1%	13.3%	6.1%	100.0%

Cross-tabulationulation between Gender and most important reason behind online privacy on social networks

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.858[a]	3	.414
Likelihood Ratio	2.899	3	.408
Linear-by-Linear Association	1.399	1	.237
N of Valid Cases	361		

Cross-tabulation between Gender and the actions believed can help safeguard information on social network sites

			Which of these actions do you believe can help to safeguard your information on social network sites				
			Install an antivirus	Leave my social network logon active even when I am not at the computer	Not changing my password	I do not know	Total
Gender	Male	Count	107	7	10	37	161
		% within Gender	66.5%	4.3%	6.2%	23.0%	100.0%
	Female	Count	123	6	29	42	200
		% within Gender	61.5%	3.0%	14.5%	21.0%	100.0%
Total		Count	230	13	39	79	361

	% within Gender	63.7%	3.6%	10.8%	21.9%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.627[a]	3	.085
Likelihood Ratio	6.949	3	.074
Linear-by-Linear Association	.476	1	.490
N of Valid Cases	361		

Cross-tabulationulation between Gender and what is believed as not a good way to secure passwords

			Which of these do you believe is NOT a good way to secure your password				
			To memorise it	To write it down (e.g.: paper, notebook)	To write it down but only in a secured place and with no title information (e.g.: sticky note)	I do not know	Total
Gender	Male	Count	32	100	19	10	161
		% within Gender	19.9%	62.1%	11.8%	6.2%	100.0%
	Female	Count	31	124	26	19	200
		% within Gender	15.5%	62.0%	13.0%	9.5%	100.0%
Total		Count	63	224	45	29	361
		% within Gender	17.5%	62.0%	12.5%	8.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.283[a]	3	.516
Likelihood Ratio	2.304	3	.512
Linear-by-Linear Association	2.160	1	.142
N of Valid Cases	361		

Cross-tabulationulation between Gender and response when somebody close requests for your social network password

			What would you do when somebody close to you (such as your partner) requests your social network's password (e.g.: Facebook password)				
			Give it to him/her the password	Give it to him/her by typing it in	Ask questions and give him/her if you are convinced	Say no	Total
Gender	Male	Count	12	17	45	87	161
		% within Gender	7.5%	10.6%	28.0%	54.0%	100.0%
	Female	Count	24	16	67	93	200
		% within Gender	12.0%	8.0%	33.5%	46.5%	100.0%
Total		Count	36	33	112	180	361
		% within Gender	10.0%	9.1%	31.0%	49.9%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.390[a]	3	.222
Likelihood Ratio	4.436	3	.218
Linear-by-Linear Association	1.862	1	.172
N of Valid Cases	361		

Cross-tabulationulation between Gender and How often do you check in on social networks

			How often do you check in on social networks					
			Never	Yearly	Monthly	Weekly	Daily	Total
Gender	Male	Count	3	3	10	30	115	161
		% within Gender	1.9%	1.9%	6.2%	18.6%	71.4%	100.0%
	Female	Count	10	7	26	33	124	200
		% within Gender	5.0%	3.5%	13.0%	16.5%	62.0%	100.0%
Total		Count	13	10	36	63	239	361
		% within Gender	3.6%	2.8%	10.0%	17.5%	66.2%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.852[a]	4	.065
Likelihood Ratio	9.249	4	.055
Linear-by-Linear Association	7.161	1	.007
N of Valid Cases	361		

Cross-tabulationulation between Gender and How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge

			How concerned are you, that some of the information you share on social networking sites might be accessed by third parties, (i.e.: advertisers) without your knowledge				Total
			Not at all concerned	Not too concerned	Somewhat concerned	Very concerned	
Gender	Male	Count	5	33	46	77	161
		% within Gender	3.1%	20.5%	28.6%	47.8%	100.0%
	Female	Count	12	40	52	96	200
		% within Gender	6.0%	20.0%	26.0%	48.0%	100.0%
Total		Count	17	73	98	173	361
		% within Gender	4.7%	20.2%	27.1%	47.9%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.816[a]	3	.612
Likelihood Ratio	1.879	3	.598
Linear-by-Linear Association	.279	1	.598
N of Valid Cases	361		

Cross-tabulationulations between Gender and receiving/responding to an online pop-up message

			Have you ever received an online pop-up that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	125	36	161
		% within Gender	77.6%	22.4%	100.0%
	Female	Count	105	95	200
		% within Gender	52.5%	47.5%	100.0%
Total		Count	230	131	361
		% within Gender	63.7%	36.3%	100.0%

			Have you ever responded to an online pop-up that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	27	134	161
		% within Gender	16.8%	83.2%	100.0%
	Female	Count	15	185	200
		% within Gender	7.5%	92.5%	100.0%
Total		Count	42	319	361
		% within Gender	11.6%	88.4%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	24.383[a]	1	.000		
Continuity Correction[b]	23.308	1	.000		
Likelihood Ratio	25.073	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	24.315	1	.000		
N of Valid Cases	361				

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	7.456[a]	1	.006		
Continuity Correction[b]	6.581	1	.010		
Likelihood Ratio	7.444	1	.006		
Fisher's Exact Test				.008	.005
Linear-by-Linear Association	7.435	1	.006		
N of Valid Cases	361				

Cross-tabulationulations between Gender and receiving/responding to an email message

			Have you ever received an email message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	132	29	161
		% within Gender	82.0%	18.0%	100.0%
	Female	Count	135	65	200
		% within Gender	67.5%	32.5%	100.0%
Total		Count	267	94	361
		% within Gender	74.0%	26.0%	100.0%

			Have you ever responded to an email message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	35	126	161
		% within Gender	21.7%	78.3%	100.0%
	Female	Count	43	157	200
		% within Gender	21.5%	78.5%	100.0%
Total		Count	78	283	361
		% within Gender	21.6%	78.4%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	9.721[a]	1	.002		
Continuity Correction[b]	8.983	1	.003		
Likelihood Ratio	9.958	1	.002		
Fisher's Exact Test				.002	.001
Linear-by-Linear Association	9.694	1	.002		
N of Valid Cases	361				

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.003[a]	1	.956		
Continuity Correction[b]	0.000	1	1.000		
Likelihood Ratio	.003	1	.956		
Fisher's Exact Test				1.000	.528
Linear-by-Linear Association	.003	1	.956		
N of Valid Cases	361				

Cross-tabulationulations between Gender and receiving/responding to an online link

			Have you ever received a link that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	118	43	161
		% within Gender	73.3%	26.7%	100.0%
	Female	Count	121	79	200
		% within Gender	60.5%	39.5%	100.0%
Total		Count	239	122	361
		% within Gender	66.2%	33.8%	100.0%

			Have you ever responded to a link that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	25	136	161
		% within Gender	15.5%	84.5%	100.0%
	Female	Count	25	175	200
		% within Gender	12.5%	87.5%	100.0%
Total		Count	50	311	361
		% within Gender	13.9%	86.1%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	6.523[a]	1	.011		
Continuity Correction[b]	5.964	1	.015		
Likelihood Ratio	6.599	1	.010		
Fisher's Exact Test				.014	.007
Linear-by-Linear Association	6.505	1	.011		
N of Valid Cases	361				

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.685[a]	1	.408		
Continuity Correction[b]	.455	1	.500		
Likelihood Ratio	.682	1	.409		
Fisher's Exact Test				.445	.249
Linear-by-Linear Association	.683	1	.408		
N of Valid Cases	361				

Cross-tabulationulations between Gender and receiving/responding to a social media message

			Have you ever received a social media message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	114	47	161
		% within Gender	70.8%	29.2%	100.0%
	Female	Count	157	43	200
		% within Gender	78.5%	21.5%	100.0%
Total		Count	271	90	361
		% within Gender	75.1%	24.9%	100.0%

			Have you ever responded to a social media message that you suspect was an attempt to get your personal details		
			Yes	No	Total
Gender	Male	Count	39	122	161
		% within Gender	24.2%	75.8%	100.0%
	Female	Count	83	117	200
		% within Gender	41.5%	58.5%	100.0%
Total		Count	122	239	361
		% within Gender	33.8%	66.2%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.820[a]	1	.093		
Continuity Correction[b]	2.424	1	.119		
Likelihood Ratio	2.808	1	.094		
Fisher's Exact Test				.112	.060
Linear-by-Linear Association	2.812	1	.094		
N of Valid Cases	361				

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	11.899[a]	1	.001		
Continuity Correction[b]	11.139	1	.001		
Likelihood Ratio	12.115	1	.001		
Fisher's Exact Test				.001	.000
Linear-by-Linear Association	11.866	1	.001		
N of Valid Cases	361				

Cross tabulation between gender, ethnicity and information security concern

				I am concerned about online security when responding to an unknown source					
Race				Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
African	Gender	Male	Count	8	4	12	24	61	109
			% within Gender	7.3%	3.7%	11.0%	22.0%	56.0%	100.0%
		Female	Count	14	12	13	40	77	156
			% within Gender	9.0%	7.7%	8.3%	25.6%	49.4%	100.0%
	Total		Count	22	16	25	64	138	265
			% within Gender	8.3%	6.0%	9.4%	24.2%	52.1%	100.0%
Coloured	Gender	Male	Count	1		0	1	0	2
			% within Gender	50.0%		0.0%	50.0%	0.0%	100.0%
		Female	Count	1		1	2	1	5

			% within Gender	20.0%		20.0%	40.0%	20.0%	100.0%
	Total		Count	2		1	3	1	7
			% within Gender	28.6%		14.3%	42.9%	14.3%	100.0%
Indian	Gender	Male	Count	4	1	5	13	23	46
			% within Gender	8.7%	2.2%	10.9%	28.3%	50.0%	100.0%
		Female	Count	1	1	2	6	20	30
			% within Gender	3.3%	3.3%	6.7%	20.0%	66.7%	100.0%
	Total		Count	5	2	7	19	43	76
			% within Gender	6.6%	2.6%	9.2%	25.0%	56.6%	100.0%
White	Gender	Male	Count	0		1	0	2	3
			% within Gender	0.0%		33.3%	0.0%	66.7%	100.0%
		Female	Count	1		0	1	7	9
			% within Gender	11.1%		0.0%	11.1%	77.8%	100.0%
	Total		Count	1		1	1	9	12
			% within Gender	8.3%		8.3%	8.3%	75.0%	100.0%
Do not wish to answer	Gender	Male	Count					1	1
			% within Gender					100.0%	100.0%
	Total		Count					1	1
			% within Gender					100.0%	100.0%
Total	Gender	Male	Count	13	5	18	38	87	161
			% within Gender	8.1%	3.1%	11.2%	23.6%	54.0%	100.0%
		Female	Count	17	13	16	49	105	200
			% within Gender	8.5%	6.5%	8.0%	24.5%	52.5%	100.0%
	Total		Count	30	18	34	87	192	361
			% within Gender	8.3%	5.0%	9.4%	24.1%	53.2%	100.0%

APPENDIX H: LANGUAGE EDITING CERTIFICATE

12 The Hill
185 Sherwell Ave
Boskruin
2188

25 May 2020

To whomever it may concern:

This letter serves to confirm that I worked as the proof reader and language editor on Happyness Nothando Ngwane's Master's thesis:

Gender Responses to Online Social Engineering Attacks amongst Young Adult Students in South Africa

In no way did I change the content.

Yours faithfully

Ethel Ross (BA Hons; H Dip Ed)

clanross@icon.co.za

083 954 5412