University of KwaZulu-Natal

Factors that influence young adults' online security awareness

2013

Zahra Bulbulia

Supervisor: Professor Manoj Maharaj

Factors that influence young adults' online security awareness

by

Zahra Bulbulia

Student Number: 202516620

July 2013

Supervisor: Professor Manoj Maharaj

Submitted in fulfillment of the degree of Masters in Commerce (Information Systems & Technology), in the College of Management, IT and Governance, University of KwaZulu-Natal, Durban.

Declaration

I declare that ‘Factors that influence young adults' online security awareness’ is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

Signature:

Name: Zahra Bulbulia

Acknowledgements

I would like to extend my thanks to my family and friends for their consistent support to me on this journey. I would also like to give special thanks to my supervisor whose never ending encouragement and enthusiasm inspired me to produce this research. I would like to also extend thanks to the examiners whose comments enhanced this research study as well as my statistician and language editor. In addition I would like to thank the editors of the Journal of Information Warfare who assisted in getting the results of this research published.

Abstract

The information age presents many fears of security threats to the integrity, confidentiality and availability of information systems and their associated data. Despite the advent of countermeasures, such as antivirus software, firewalls, security patches and password change control systems, amongst others, to protect information systems, online attacks have increased significantly. Vast sums are spent by both the government and business sectors on deflecting mechanisms and on cleaning up after online attacks, which are becoming increasingly sophisticated and diverse (Gartner, 2009). The aim of this exploratory study is to determine the factors that influence online security and the current state of user awareness in South Africa amongst young adults. To guide this approach, Protection Motivation Theory (Rogers, 1983) was used as a conceptual framework.

Significant findings of the study are that gender, race, community, language and employment status affect user awareness of online security. In terms of user awareness of online security it was found that most of the respondents were aware of the dangers of online threats and concerned about the state of online security in South Africa. The reasons why gender, race, community, language and employment status affect online security awareness can be explored in further research.

Table of Contents

List of Figures

List of Tables

List of Acronyms

IS – Information Systems

IT – Information Technology

PMT – Protection Motivation Theory

SNS – Social Networking Websites

UTAUT - Unified Theory of Acceptance and Use of Technology

Chapter 1: Introduction

The September 11 attacks against the United States have prompted many new concerns for physical security and information security. With the advent of the Information age, also known as the computer age, there are increasing fears of security threats to the integrity, confidentiality and availability of information systems. Actions have been taken and measures put in place, however, to prevent these threats from materializing. These include antivirus software, firewalls, password change control systems and security patches, as well as a variety of techniques that are offered to protect information systems (Workman, 2008).

It has been found in research done by Cisco Systems (Cisco Systems White Paper, 2006) regarding online security awareness in the workplace, that isolated end-users seem to possess security awareness but their practices are not consistent with this as they still indulge in risky online behaviour. In this research study, participants believed that they were working securely. What is important here is that, although end-users understand the importance of security, they do not put it into practice. This shows that although users may be aware, they are not properly educated about security threats. So, while users may be aware of security threats, they may not understand the implications of their actions online. Some research states that users are not IT professionals and thus have different priorities (Brush, 2006). While end-users might be aware of the importance of security, this knowledge is not enough to ensure safer habits by them. Just because users think or say they are aware does not mean they know how to be safe. An end-user who is poorly informed about security best practices, yet believes he is working safely, can actually intensify security risks for an organisation.

It is assumed that the younger generation of users are more net-savvy, although a study about how much personal information people reveal online has shown that the student population is not overly concerned about privacy and security issues (Little, 2008). This is due to the fact that 90% of individuals in the study revealed their real names and pictures online (Little, 2008). It was thus concluded in this study that there is a need to develop awareness of personal and professional risks due to the large number of online threats (Little, 2008). According to a recent survey carried out in South Africa, just under 45% of respondents rated online security as a priority. In terms of social networking, 46.32% of respondents share certain information on their social network profile with everyone (Kayle, 2011). This shows that many individuals rate

security as a priority yet do not view sharing certain information on their social networking profiles with everyone as a potential threat. This could be because they are unaware of the potential security threats derived from this practice (i.e. identity theft) or that they are aware but are not overly concerned about privacy, as stated above.

Using the Protection Motivation Theory (Rogers, 1983) this research investigates whether demographic (inclusive of factors like employment status, gender, race, language, community) factors play a role in users' online security awareness.

1.1 Risky Online Behaviour

Recently, attention has been given to the amount of time that some users spend using social networking sites and the risky behaviour of users on these sites (Price 2010). In a study by Sophos (2007) it was found that users are careless when using social networking websites regarding who they invite into their circle of friends. A survey was done in 2007 where a false Facebook profile was created for a character called "Freddi Staur", who sent out 200 friend requests to determine how many people would be willing to accept him as their friend and thus permit a complete stranger to have access to the users' personal details on their Facebook profile (Sophos, 2007). The false friend requests received 87 responses, with 82 responses giving "Freddi" access to private information (Sophos, 2007). This study shows that individuals do not seem to view their actions as possible security threats or are unaware that these actions can result in identity theft.

A survey in the United States found that, regardless of possessing a high level of awareness about threats lurking on the Internet, young adults routinely engage in risky online behaviour. It was found that seven out of ten admitted that they are not always as careful as they should be when posting and accessing information online (TRU Research, 2010). It was also found that, in spite of the incidence of online threats, young adults in the United States are doing very little to protect themselves (TRU Research, 2010). It would be useful to researchers and practitioners involved in developing user education and awareness campaigns to see what the current user awareness of online security of young adults in South Africa is, and whether demographic factors impact on users' security awareness. The reason it would be useful is that these researchers and practitioners will be able to see where the gaps are in terms of the demographic groups who have the knowledge and those who do not and can therefore cater for the ones who have less knowledge by designing their campaigns in such a way that it can be more

understandable to those who lack awareness. Researchers, practitioners and educators could use the findings of this research to generate more effective messages in order to increase online security awareness.

A study in Malaysia showed that demographic factors did impact online shopping behaviour. These factor are gender, age, marital status, employment status and salary (Hashim, Ghani, & Said, 2009). This study looked at whether demographic factors had an impact on users' online security behaviour.

1.2 Protection Motivation Theory

To guide this study, Protection Motivation Theory (PMT) which was conceptualised by Rogers, was considered. The reason for the use of Protection Motivation theory is that, although it is an older model, it has been used in other research over the years and has been effective, particularly in the medical field (Grindley, Zizzi, & Nasypany, 2008). This model has also been adapted and used in the information security arena quite effectively (Acquisti & Gross, 2006, Banks, Onita, & Meservy, 2010, Dwyer, Hiltz, & Passerini , 2007, Herath & Rao, 2009, Johnston & Warkentin, 2010, LaRose, Rifon, & Enbody, 2008, Milne, Labrecque, & Cromer, 2009, Lo, 2012, Pahnile Siponen & Mahmood, 2007, Siponen *et al*., 2010, Youn, 2009, , Young & Quan-Haase, 2009). This theory serves to explain the effect of fear on attitude change and behaviour. Protection Motivation Theory states that an individual's motivations or intentions to protect himself from harm are improved by four critical perceptions: the severity of the risks; the personal vulnerability to the risks; self-efficacy or assurance in one's ability to perform the risk-reducing behaviour; and the response efficacy of the risk-reduction behaviour (Rogers 1983).

Due to the fact that Protection motivation theory was used successfully in the research discussed above, it was applied to this study (More discussion on PMT in online security research is discussed in sections 2.9 and 3.2).

1.3 Applying Protection Motivation Theory to the Online Security Domain

Some research has been done in the information security field using Rogers' Protection Motivation Theory, mostly in empirical studies. It has been used in research to explain information security compliance because it was found to be theoretically solid as well as empirically testable (Pahnile *et al.*, 2006).

Results from one study show that the visibility of a threat has a major effect on users' intentions to observe information security policies (Pahnile *et al*., 2006). This means that information system security must be promoted in the organization in a visible way, through education and campaigns. In other words, the importance is in the visibility of the threats not the exact means by which security matters are promoted in organizations. External information system security visibility also has an effect on the cognitive process of Protection Motivation Theory. Possible sources of external visibility include news or media, such as newspapers, radio, TV, as well as the Internet. This entails reporting security incidents in the media and also making them visible to employees in organizations (Pahnile *et al*., 2006).

Protection Motivation Theory has also been used in a study by Pahnile *et al*., (2007) to find out why users are unmotivated to protect their computers against spyware. It was found in this research that the perceived threat of an online security problem could lead users to protect themselves. Thus Internet users who are highly knowledgeable about the threat of spyware and believe in their ability to cope with a spyware threat are most likely to protect themselves and adopt anti-spyware software. Internet users who are not knowledgeable about the threat of spyware and believe they are incapable of coping with online security threats will most likely engage in unsafe computing behaviour and may appear to be indifferent to taking protective action. In terms of PMT, when Internet users' awareness of an online security threat (i.e., spyware) is high, there is a strong positive relationship between the perceived ability to cope, protection motivation, and behavioural intention to protect oneself. However, when Internet users' awareness of the threat is low, there is a weak relationship between the assessed ability to cope and motivation and behavioural intention to protect oneself (Poston & Stafford, 2010).

A study in the United States has also used Protection Motivation Theory to examine the role of online self-efficacy of non-student respondents. Results of this study showed that demographic factors, such as age, race and employment status, have a differential influence on the type of behaviours taken online (Milne *et al.*, 2009).

1.4 Problem Statement and Research Questions

End-users who are poorly informed about security practices, but who believe they are working safely, present a potential to intensify security risks for IT organizations (Cisco Systems, 2006). According to the 2012 report of security firm RSA, there is a reported number of almost 33,000 phishing attacks globally every month of the year, which results in a total loss of $687 million.

These numbers mark a global increase of 19% when compared with the statistics for the first half of 2011 (RSA, 2012). Cyber crime is a big problem in South Africa according to the latest figures from the South African Anti-Fraud Command Centre (Wolf Pack, 2013). South Africa is the country, after America and Britain, that is experiencing the highest number of phishing attempts. The latest report by the Internet Crime Complaint Centre (Internet Crime Complaint Centre, 2011) states that South Africa is ranked seventh in the top 10 cyber crime perpetrators list (Internet Crime Complaint Centre, 2011). According to a recent report, South Africa has lost more than R1 billion in the past three years due to cyber-crime (Von Solms, 2011).

Online fraud is aggressively threatening individuals and some believe that it can turn into a weapon of electronic warfare in the future (Jakobsson & Srikwan, 2008). One way to ensure online safety is to make use of education and awareness campaigns or provide information to users to increase their awareness levels. Lack of information security awareness is a problem and finding more ways to educate users might be a step in the right direction (Monk 2011, Van Niekerk & Von Solms 2007). True security depends on assistance from the users concerned in the security process (Van Niekerk & Von Solms, 2007). Each user involved in the security process not only needs knowledge relating to what they should do, but also knowledge as to how to perform their security-related functions (Van Niekerk & Van Greunen, 2006).

Despite efforts to generate awareness of online security, research has found that users still indulge in unsafe practices online. Online fraud is actually on the increase (Gartner, 2009) and young adults indulge in risky online behaviour, despite being aware of online security (TRU Research, 2010). These factors gave rise to the problem statement: The identification of factors that influences young adults' awareness of online security.

The main focus of the study is whether the respondents' demographic profiles have an impact on their online security awareness.

1.5 Research Questions

What is the current state of user awareness of online security in South Africa?

Since the subject of user awareness is being researched from the user perspective, what first has to be established is how aware users are of online security threats. This will be done in the form of a survey.

What factors influence online security awareness?

These were derived from the results of the survey when the users' demographic profiles were compared with how they answered the survey. Analyses were performed by a statistician who used SPSS software.

1.6 Research Methodology/Methods

The methodology for the exploratory study was based on assessing the current levels of user awareness of online security and whether demographic factors had an impact on this. The instrument that was used for this research was an online survey.

1.7 Sample and Method

The primary population in this study is young adults.

This online survey will inform the researcher of the following:

- The demographic information of the users
- Current level of online security awareness of users
- Current user fears regarding online security
- Measures users believe will keep them safe if taken
- How much private information they reveal online
- Where the users mainly hear/learn about online security

More detail about the survey and how PMT constructs were measured will be given in chapter three.

1.8 Sampling and Limitations

For this research study, a non-probability sampling method called convenience sampling was used. With this method, the selection of population elements is based on their availability (i.e. because they volunteered). The limitation here is that an unknown portion of the population is excluded (e.g. those who did not volunteer). In this study, a combination of convenience sampling and snowball sampling was used. The convenience sampling technique was used so that the researcher could get a high response rate within the given time frame. This sampling technique was used to get responses from the student population at the University of KwaZulu-Natal.

The snowball sampling technique was used so that the response rate could be expanded to reach people from the target population which would otherwise have been difficult to locate. This sampling technique was used to gain access to young employed adults. These methods were

chosen as they seemed to be the least restrictive in terms of the response rate. Also, other sampling methods require more formal access to lists of people from whom to select for a survey. The researcher did not have the capacity or relevant authority to get access to these types of lists from the University.

Facebook and Twitter were the social networking websites of choice used for this study. The reason that social networking websites were used to conduct this study is that many young adults connect to these websites regularly (Pring, 2012).

1.9 Analysis of Results

Results were analysed by a statistician using SPSS software (See Appendix A for letter from the statistician). To test user awareness, a categorical chi-square goodness of fit test was performed to further validate the results. The researcher used cross tabulations to test the hypotheses to see if the above elements (i.e. gender, race, community, language and employment status) influence online security awareness.

1.10 Chapter Outline

Chapter 1: This contains the introduction. This section provides an overview of the research study motivation section, as well as the study processes that will be followed throughout the research study (This is the above chapter).

Chapter 2: This chapter comprises the literature review of literature relating to the factors influencing users' online security awareness. This chapter also describes current security threat trends and shows some of these statistics. In addition, the conceptual framework and model are described.

Chapter 3: This section describes the research design and methodology that are used and further explains how the model has been adapted to this study.

Chapter 4: This section shows the findings for users' general online security awareness. This section provides answers to the above research questions, namely:

- What factors influence online security awareness?
- What is the current state of user awareness of online security amongst young adults?

Chapter 5: This chapter shows the results of the hypothesis testing for the factors race, language and community.

Chapter 6: This chapter shows the results of the hypothesis testing for gender.

Chapter 7: This chapter shows the results of the hypothesis testing for employment status.

Chapter 8: This chapter gives the conclusions drawn in the study, and the research study evaluation and recommendations for future studies in this area.

Chapter 9: This chapter comprises possible strategies to enhance user awareness of online security.

A bibliography section and appendices follow.

1.11 Conclusion

The results of this study will be relevant to researchers and practitioners involved in developing user education and awareness campaigns. Researchers and designers of online campaigns require information on how they can improve end user observance of information security and, in so doing, improve the security of their information.

Results of this study has been published in the Journal of Information Warfare (April 2013 edition) and an abstract has been accepted for the ISSA 2013 conference (See Appendix E). In addition all chapters of this thesis (Including the abstract) have been language edited (See Appendix B) and results have been analysed by a statistician (See Appendix A). A Turnitin report is also included (Appendix D) and an ethical clearance letter which the research committee has provided to the researcher (Appendix C). This letter was provided after the committee reviewed the research instrument and the motivation for the study and thus allowed the researcher to proceed with the study.

Chapter 2: Literature

2.1 Introduction

Protection of data or electronic information from unauthorized access is known as Information Security (Peltier, 2002). Information Systems are made up of hardware, software and people, and need to be secured against unauthorised access. There are controls in place to ensure security for hardware, software and people. In terms of hardware, devices like firewalls assist in securing information as they control and monitor access between two or more networks. In terms of software programming, standards make sure that developers create software which supports a sufficient level of security. For people, there are policies and rules in place in organisations that users of systems have to follow to ensure that security is maintained. The users of the system are often the main cause of Information Security breaches (Ernst & Young, 2008). Cyber criminals often target the users of the system to gain entry to it as the users are frequently described as the weakest link in the security chain (Allen, 2006). For a system to be secure, it must incorporate the following security goals (Pfleeger & Pfleeger, 2003):

- Integrity: The process of ensuring that the data in the system is not modified, intercepted or deleted illicitly
- Confidentiality: Ensuring that only legitimate parties have access to data. It ensures that computer-related assets are accessed only by authorized parties
- Availability: Ensures legitimate access to the system for authorized parties at appropriate times

Fundamentally, information security can be seen as the protection of assets from threats by launching controls to decrease the risks initiated by vulnerabilities (Monk, 2011). These elements will be discussed in further detail below.

An **asset** is anything which adds value to a business. Assets can be classed into two groups, these being tangible assets and intangible assets. Intangible assets are things like raw data, licences, contracts and policies. Tangible assets, on the other hand, are servers, desktop computers, switches, routers etc. (Alshboul, 2010).

Vulnerabilities are the weaknesses of information systems that provide opportunities for attacks (Monk, 2011). These can be exploited accidentally or intentionally.

Threats exploit vulnerabilities to cause damage or loss (Monk, 2011). Threats with regard to computer systems are when hackers, viruses and destruction to computer and network resources are involved.

A **risk** is the probability that a threat will exploit vulnerability and cause harm to or loss of an asset (Pfleeger & Pfleeger, 2003). When these elements (Assets, Vulnerabilities and Threats) come together, a risk can be recognized and identified.

To mitigate risks, controls or countermeasures have to be implemented so that risks can be reduced. The table below shows examples of all these elements.

Table 1: Examples of an Asset, Threat, Vulnerability and a Control (Adapted)

Asset	Threat	Vulnerability	Control
Data	Firewall enabled to allow guest access	The network	Disable guest access on firewall. Strong authentication measures.
E-mails	Interception of e-mails	The network	Encryption
Password/s	Staff sharing passwords	Unaware and untrained staff	Training programmes
Personal Computers	Theft of Personal Computer	Door	Access control

The information age presents many fears of security threats to the integrity, confidentiality and availability of information systems and their associated data. Despite the advent of countermeasures, such as antivirus software, firewalls and password change control systems, amongst others, to protect information systems online, attacks have increased significantly (RSA 2012, Symantec 2012). Vast sums are spent by both the government and business sectors on deflecting mechanisms and on cleaning up after online attacks which are becoming increasingly sophisticated and diverse. Some of these are discussed further in the sections below.

2.2 Types of Attacks

There are a variety of attacks. These are described in the sections below.

2.2.1 Malware

Malware is code or software that is specially designed to destroy, disrupt, steal, or inflict an illegitimate action on data, hosts, or networks (Cisco Systems, n.d). Viruses, worms, Trojans and bots are all categorized as software called malware (malicious software). According to the Symantec annual report, these attacks continue to increase rapidly, despite efforts to minimise them by the company (Symantec, 2012). Spyware is a type of malicious software (malware) that gathers data or information from a computer system without the user's permission. Spyware can keep track of keystrokes, screenshots, authentication credentials, personal email addresses, web form data, Internet usage habits and additional personal information (US-CERT, 2005).

2.2.2 Phishing and E-mail Scams

There are a large variety of e-mail scams, one of the most popular being phishing attempts. Phishing attacks aim to trick users into exposing personal information like credit card details, usernames, pin codes and passwords for Internet services.

Figure one (below) is an example of a phishing website. One of the typical signs of a phishing website is that the web address in the address bar is unconventional (see below)

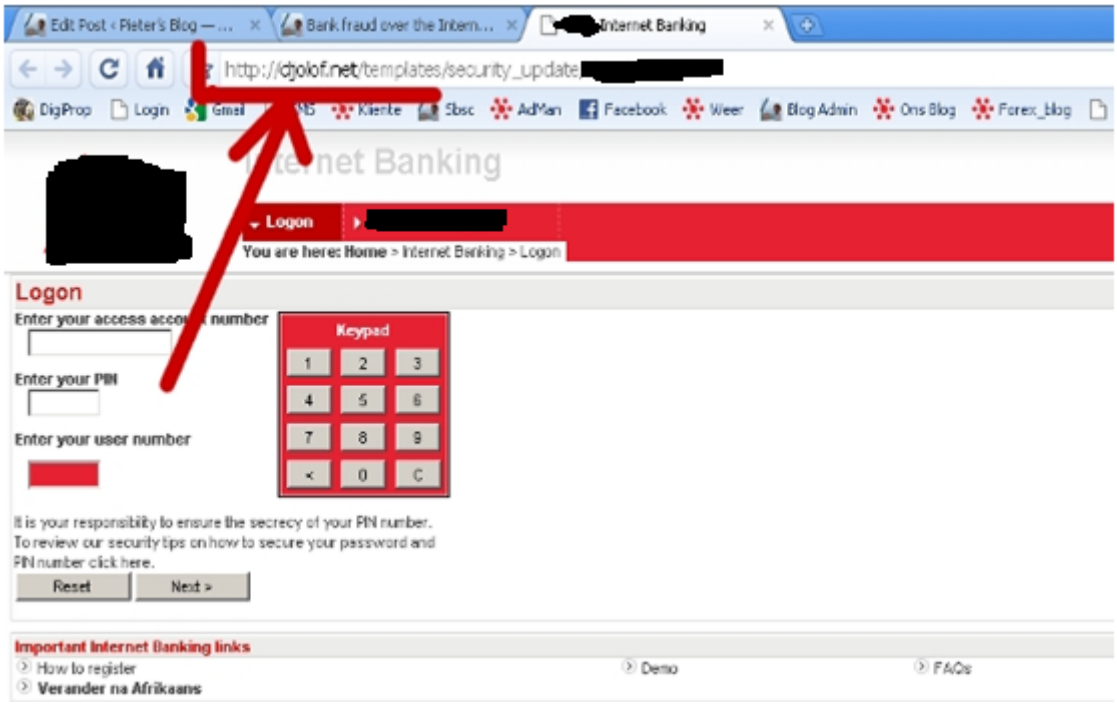

Figure 1: Example of Phishing Attack (Pretorius, 2009)

Other popular types of e-mail scams include 419 scams and spoofing. The term '419' was created from "419" of the Nigerian Criminal Code (Chawki 2009). This scam started with offenders, normally working from Nigeria and targeting victims across the world, usually with letters sent over the postal mail (Smyth and Carelton, 2011). Thereafter, offenders moved to using e-mail. Basically the scam comprises of an unsolicited e-mail that masquerades as a notice from an unknown beneficiary or a request to help with charity or a business proposition (Christensen, 2006). The scam involves a prolonged communication with the victim. The victim becomes progressively drawn into the plot and defrauded by the scammer's skill to form sympathy, rapport and trust while never meeting in person (Smyth and Carleton, 2011). Another common type of attack is called spoofing, which involves the sender of an e-mail altering parts of the e-mail to make it appear as though it was sent by someone else (Gil, 2012).

2.2.3 Web 2.0 Dangers

Web 2.0 is a relatively new technology, which creates a huge opportunity for attackers to exploit online resources. In addition, a number of vulnerabilities can be exploited, like insufficient authentication controls, cross-site scripting, cross-site request forgery, information leakage, injection flaws and insufficient anti-automation (Secure enterprise 2.0, 2009). In terms of incidents, one of the well-publicized ones is the brute force dictionary attack against a

Twitter administrator account that broke into 33 user accounts, including those of Barack Obama and Britney Spears (Secure enterprise 2.0, 2009).

2.3 Controls

For the above attacks, there are controls in place to protect information systems. Anti-Virus software products are designed to defend users' computers against malicious software by recognizing code signatures that are unique to different types of malware (Heyman, 2007). A firewall can be defined as hardware or software that serves as a barrier between networks as well as other functions, such as providing access controls, filtering traffic and other security features (Goertzel, 2011). Personal computer users also use firewalls that are software-based to prevent threats from the Internet. Password control mechanisms are also incorporated into many systems to prevent unauthorised access to information. These can be further categorised or split up into physical controls, technical controls and operational controls (van Niekerk & von Solms 2006, Pfleeger and Pfleeger, 2003) and are discussed below.

- **Physical controls** prevent unauthorised access into a business premises. These include burglar guards, access-controlled entrances and guards.

- **Technical controls**, on the other hand, resolve vulnerabilities that are technology-related. An example of this is forcing a user to authenticate himself before accessing certain information (Whitman & Mattord, 2011). Encryption is another example of a technical control.

- **Operational controls** are controls for threats that occur due to human behaviour, either accidentally or intentionally (Monk, 2011). An example of this type of control would be educating users about online security threats and password mechanisms. These controls are more difficult to regulate than physical and technical controls as they are reliant on users of a system who are the weakest link in the security chain. Physical and technical controls essentially depend on the application of operational controls (van Niekerk & von Solms, 2006; Stephanou & Dagada, 2008). For example, a technical control can force users to use a strong/secure password; however, users are likely to write it down on a piece of paper, which is not secure behaviour.

This study aims to find out what the current level of user awareness is and whether demographic factors play a role in their awareness levels. It therefore focuses on how much the users know about online security. Based on the findings of this research, practitioners and educators can develop awareness campaigns specific to different users' needs and requirements. This would then support the conception that users' behaviour can be transformed to execute controls effectively if they obtain the proper education (Monk, 2011). The next section will show recent online fraud statistics and current user perceptions of online security.

2.4 Cyber Crime and User Perceptions of Online Security

In terms of cyber crime worldwide, viruses, worms and malicious websites are the biggest threats, as shown in figure 2 below (Turbotodd, 2012).

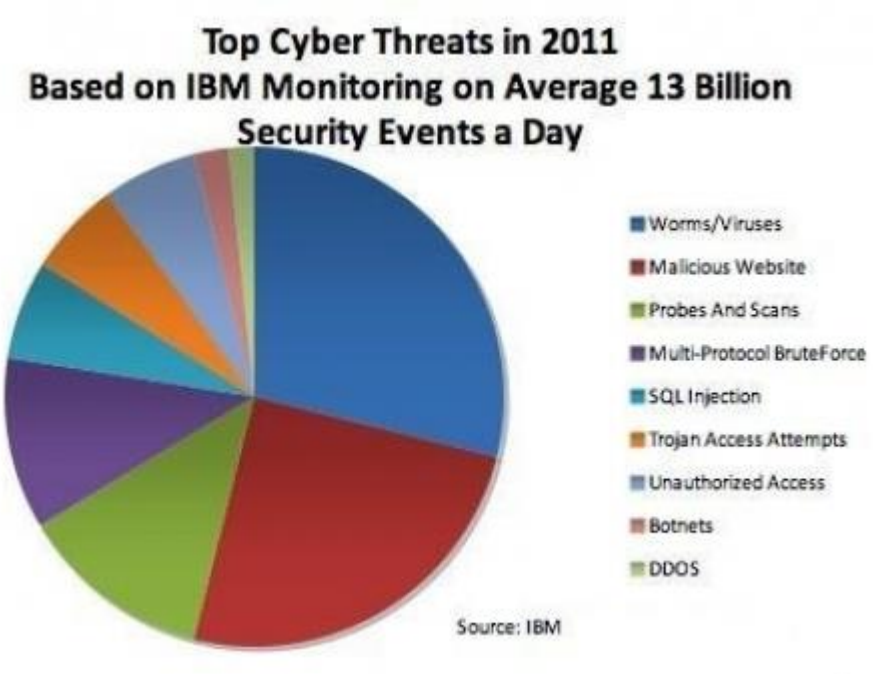

Figure 2: Top Cyber Threats in 2011

Sources show that in the international context, South Africa has a severe cyber crime problem (Internet Crime Complaint Centre 2011, RSA 2012). The most recent figures from the South African Anti-Fraud Command Centre state that South Africa is one of the countries, after America and Britain, undergoing the greatest volume of phishing attempts (Von Solms 2011, RSA 2012). Von Solms (2011) reports that the founder and chairman of the Information Security Group (ISG) of Africa, Craig Rosewarne, stated that the R1 billion reportedly lost in 2011 in South Africa due to cyber crime was a conservative estimate. He further stated that this

was because no law or regulation currently forced companies to report cyber crimes thus the true scope of the situation in South Africa is uncertain. Figure three, below, shows where South Africa is in relation to the rest of the world with regard to phishing attacks.

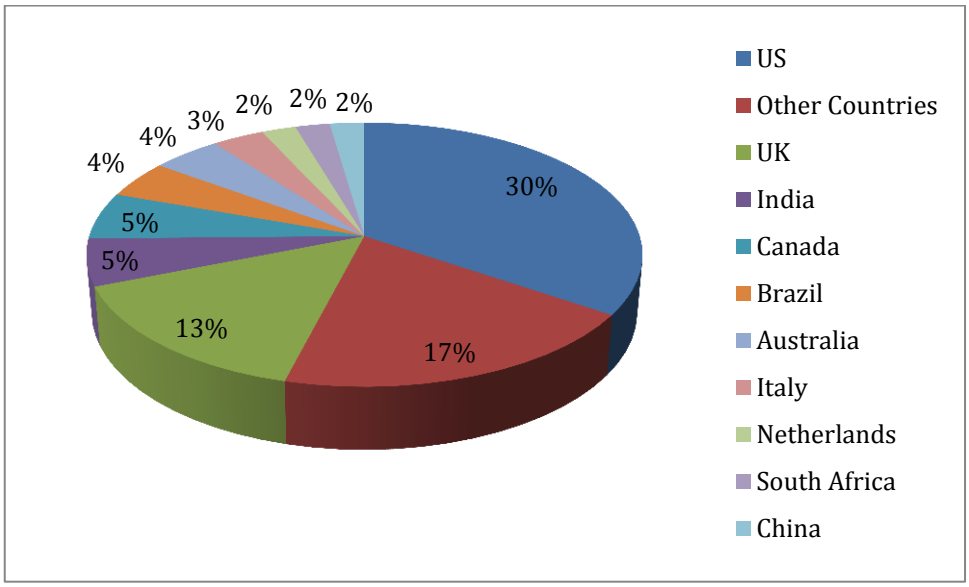

Figure 3: South Africa's High Volume of Phishing Attacks (Grobler, Van Vuuren, Jansen & Zaaiman, 2012)

Online fraud is aggressively threatening individuals and some believe that it can turn into a weapon of electronic warfare in the future (Jakobsson & Srikwan, 2008). One way to ensure online safety is to provide information to users to increase their awareness levels and to make use of education and awareness campaigns. Lack of information security awareness is a problem and investigating more ways to educate users will be a step in the right direction (Monk 2011, Van Niekerk & Von Solms 2007). True security depends on assistance from the users involved in the security process (Van Niekerk & Von Solms, 2007). Each user involved in the security process not only needs knowledge relating to what they should do, but also knowledge as to how to perform their security-related functions (Van Niekerk & Van Greunen, 2006).

Many Internet users at present stay away from buying online, due to fears that their financial information will be stolen (Jahankhani, 2009). In the United Kingdom, 50% of consumers over the age of 16 still do not purchase online (CyberSource, 2010). The study (CyberSource, 2010) indicated that 71% of users were concerned about the level of risk when purchasing online, which is an increase from 66% in 2008. This indicates that users' perception of the safety issues associated with online shopping is not improving.

According to Jahankhani (2009) a primary negative perception revolves around the security involved in electronic payment systems. Consumers are doubtful about providing personal information, including credit card details, over the Internet due to concerns with privacy and fraud (Jahankhani, 2009). Another factor that makes consumers unsure of transacting business online is that e-commerce is borderless. Consumers are therefore unsure of their rights or protection and jurisdiction if something goes wrong (Ong, 2003). The next section will discuss privacy and what it means in the online security context.

2.5 Privacy

In terms of the Internet, privacy refers to the user's opinion on whether or not the online vendor will try to protect the confidential information collected from them during electronic transactions from unauthorized use or disclosure (Kim *et al*., 2008). Thus, for numerous Internet users, privacy loss is the key concern and the protection of information during online transactions is vital (Salleh *et al*., 2012). Examples of privacy abuses on the Internet include spamming, usage tracking and data collection, and the sharing of information to third parties (Salleh *et al.*, 2012). When users feel or recognize that their information privacy has been violated, they will avoid disclosing their personal information on the Internet (Dinev & Hart, 2006).

Several studies have suggested that a large number of Internet users have serious apprehensions concerning privacy on the Internet (Barnard & Wesson, 2003). This leads to the issue of trust. The primary impediment to sustained e-commerce growth is winning public trust. Elevated levels of trust and positive electronic commerce experiences add to the possibility of consumers returning and establishing continuing relationships (Jahankhani, 2009). Trust includes privacy, ease-of-use and credibility of information on the Internet and is as important to consumers as security (Barnard & Wesson, 2003). Trust is found to be an important precursor to perceived risk (Pavlou, 2003).

A study by Salleh *et al.* (2012) found that perceived risk decreases when trust arises. Trust and perceived risk are vital to all types of online transactions, such as e-commerce (Pavlou, 2003), e-governance (Belanger & Carter, 2008), and Internet banking (Casalo *et al*., 2007). In terms of social networking websites, studies show that the majority students in university are more inclined to trust Facebook (FB) than other social networking websites (MySpace, Friendster) (Acquisti & Gross, 2006, Fogel & Nehmad, 2009). There has, however, been some empirical

research that has revealed that while users are occasionally aware of the privacy and security concerns related to social networking websites, they do not have a good understanding of the risks associated with disclosing their information on online social networks (Raynes-Goldie, 2010).

Trust and security are linked. Unlike the real world, consumer trust in e-commerce websites depends on and is influenced by:

- Having secure standard technologies
- Being a reputable, profitable business

To make users aware of the dangers online and to educate them about what they should and should not reveal online, awareness strategies are being put in place. These will be discussed in the section below.

2.6 User Awareness Strategies

Awareness campaigns are important to educate individuals on how to recognize and respond to online attacks. As discussed below, government establishments, online operators and Internet Service Providers are currently developing educational tools for users. In the United States, the Federal Trade Commission (FTC), the Department of Homeland Security, the Department of Commerce, and other government and private sector partners have launched a website and education campaign to help individuals be on guard against Internet fraud. The campaign is called OnGuard Online and is accessible in both English and Spanish. It consists of media as well as articles that aim to help computer users protect themselves against Internet fraud, as well as secure their personal computers and defend their personal information. The materials on OnGuard Online are available to anyone who is interested in using it (OnGuard Online, 2012). This approach can be seen as inadequate as the Federal Trade Commission (FTC) informs people they should forward emails suspected of threats with full headers yet there is no explanation about what a full header is or how to forward it (Jakobsson & Srikwan, 2008). Everyone with access can actually learn what a full header is, yet many may be inadequately motivated to find and read this information (Jakobsson & Srikwan, 2008). This website thus expects users to be more technologically well-informed than they actually are. On the other hand, some initiatives oversimplify the message, for example, financial organizations frequently warn users that they should not click on hyperlinks in email messages.

In 2008, attackers started to adjust to users being cautious of clicking on links in email messages so, in their attacks, actually recommended to targeted users that they should copy and paste

URLs into the address bar (Jakobsson & Srikwan, 2008). Other awareness and advice-giving websites, such as Get Safe Online (Launched by the British Government) and Stay Safe Online (Launched by the Australian Government) also provide good resources for those users that are aware of them. The challenge is that there needs to be a prompt or a trigger so that users look at these websites in the first place (Furnall, 2008). The difficulty with information security education, training and awareness is that most people are usually not motivated to learn on their own. Online security awareness might create employee awareness of a security issue, but it does not guarantee that the employees comprehend how that message should be put into practice (Monk, 2011).

Another view is that users should not be solely responsible for information security. This is due to the fact that ordinary users cannot be expected to keep up with sophisticated attacks launched by career criminals. As stated before, users and IT security professionals have very different priorities and the user should not be expected to understand the complex issues surrounding information security (Cisco Systems White Paper, 2006). In terms of this viewpoint, the solution that is suggested is restructuring the technology as opposed to educating the users (Nielson, 2004). Another solution is to apply more stringent laws regarding information security crime (Nielson, 2004). Both these solutions are logical, but might not be feasible. Changing the technology might be worse as the user might be reluctant to learn a whole new system or technology. Thus, the new technology might be met with resistance. In terms of more stringent laws, different countries have diverse viewpoints regarding online security. The reason for this is possibly because Internet usage in some countries are higher than others (Internet World Stats, 2013), thus more online transactions will be performed by countries with higher Internet usage, thus increasing the susceptibility of these countries (i.e. countries with a higher Internet usage) to attack.

As mentioned above, this study aims to find out what the current level of user awareness is and whether demographic factors play a role in awareness levels. To derive a hypothesis, a review of the literature was performed to see if there was previous literature that showed whether these factors affected online security awareness. These are discussed in the sections below.

2.7 Factors That Influence User Awareness of Online Security

According to recent literature, it has been found that gender, ethnic background, the community in which an individual lives or grew up and employment status do impact online security awareness. Each of these factors is discussed below.

2.7.1 Ethnic Background, Community and Language

The Internet is a dangerous place and users accidentally become victims of cyber criminals. A large segment of the South African population has not had regular contact with technology and broadband Internet access. This fact, in conjunction with the current dangers of cyber threats, make local communities vulnerable to cyber attacks. Poor infrastructure in rural areas limits Internet usage and thus a majority of African Internet users in these areas do not get access to the Internet (Labuschagne & Eloff, 2012). Research done by the Council for Scientific and Industrial Research and the University of Venda shows that local communities are not equipped to deal with cyber threats. As a preventative measure to prevent Internet users from these communities from becoming victims of cyber attacks, a thorough awareness campaign is essential to teach users basic security. According to a recent research study in terms of the South African population (South African citizens from areas within the South African Gauteng, Mpumalanga and Limpopo provinces participated in this study) the results show that only 50% of the population has some level of cyber awareness. This study showed that rural and semi-rural citizens were less aware of cyber threats and should be the focus of online security awareness programmes (Grobler *et al.*, 2012).

In South Africa (where this study had taken place) there are 11 official languages. According to the 2011 census, the most common home language in South Africa is isiZulu with just over 20% of the population speaking it. The second most common language is Xhosa, which is spoken by 16% of the population. This is followed by Afrikaans at 13.5%. and English and Setswana each at 8.2% (SouthAfrica.info, 2013). This research will also look at whether language affects online security awareness. According to previous studies, another factor that influences online security awareness is race (Milne 2009). This research will also look at whether race is an indicator of online security awareness

2.7.2 Internet Usage in South Africa

In other countries, there have been a number of education campaigns and initiatives taken to launch user awareness and. The reason for this is possibly the fact that Internet usage in South Africa is lower than in the United States and Europe (Internet World Stats, 2013). Table two, below, shows the South African population figures and the latest Internet and Facebook usage statistics.

Table 2: Internet Usage in South Africa (Internet World and Population Stats, 2013)

SOUTH AFRICA
ZA - 48,810,427 population (2012) - Country Area: 1,219,090 sq km
Capital City: Pretoria* - population 1,815,889 (2012)
8,500,000 Internet users Dec/12, 17.4% of the population, per WWW.
6,269,600 Facebook subscribers on Dec 31/12, 12.8% penetration rate

Figure four, below, shows the percentages of Internet users in the world.

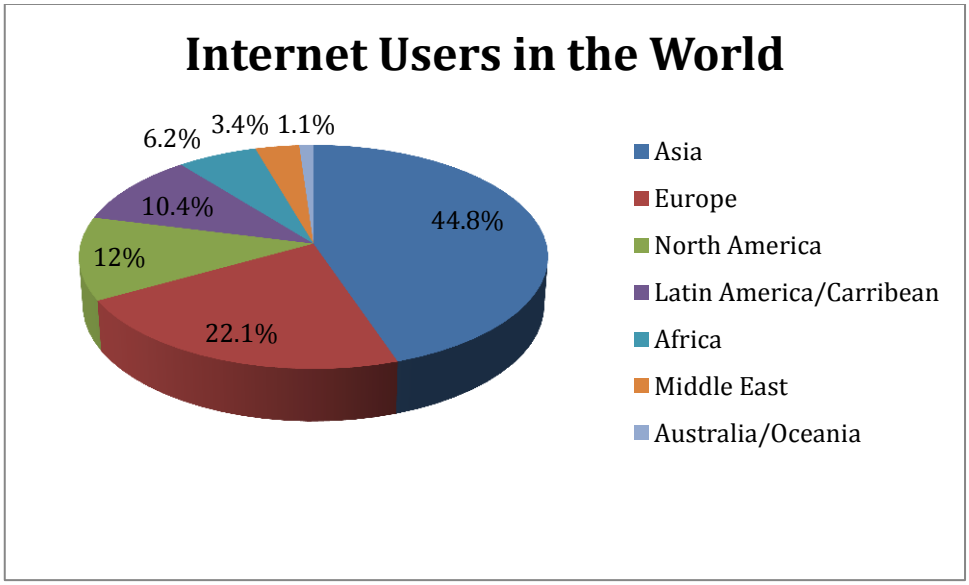

Figure 4: Internet Users in the World, Distribution by World Regions – 2011 (Internet World and Population Stats, 2013)

The data above shows that Africa as a whole, has one of the lowest Internet usage statistics in the world. As shown in figure four, above, North America and Europe both have the highest number of Internet users.

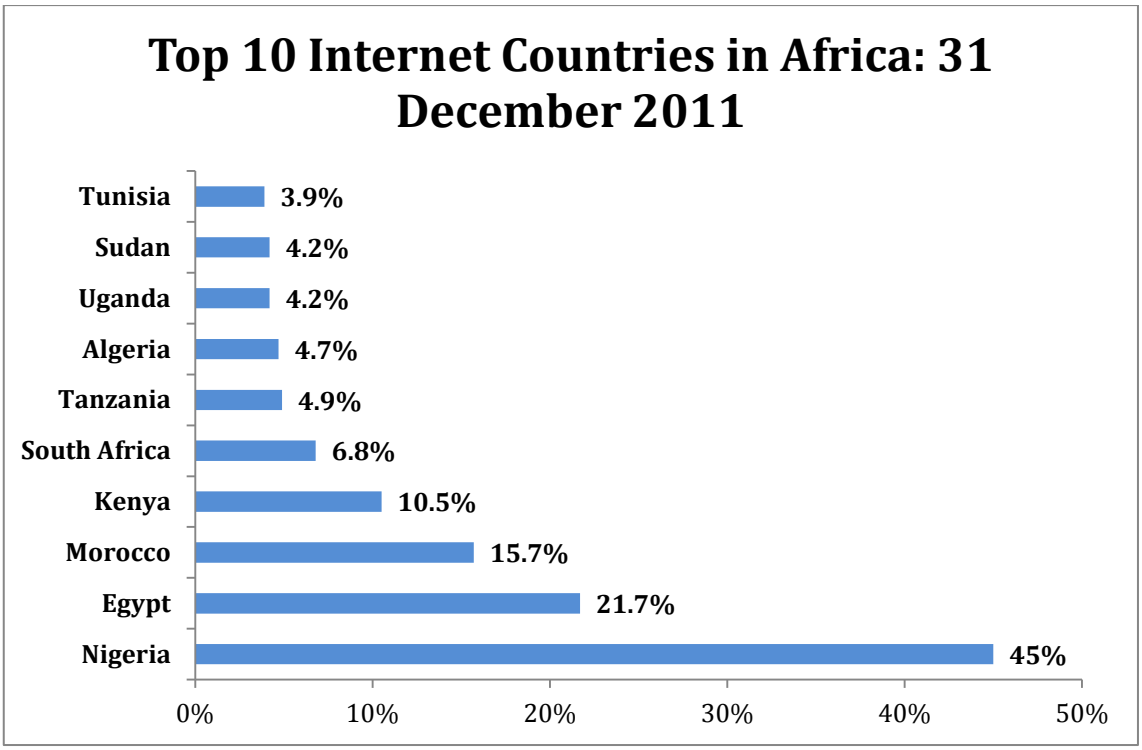

Figure 5: Internet Penetration Africa 2011 (Internet World and Population Stats, 2013)

In terms of Africa, South Africa's Internet usage is only the sixth highest, as shown in the graph (Figure five) above.

2.7.3 Gender Influence on Online Security Awareness

Studies show that gender has an impact on phishing susceptibility. In particular, women, tend to click on links in phishing emails more frequently than men do according to Sheng *et al* (2010). This study speculates that women are more prone because they have fewer opportunities to learn about phishing or are less motivated to learn about phishing. This study also states that issues that would be worth looking at in the future are the difference in the way men and women make use of the Internet as well as the difference in the way men and women make trust decisions.

A study by Fogel & Nehmad (2009) discovered differences between men and women in terms of online privacy. It was found that women are reassured about privacy protection on social networking websites (SNS) and are less likely to reveal real information about themselves when compared with men. Another study was done at the University of Indiana that aimed to show whether participants would fall for a phishing website by providing their personal details on it (Jagatic *et al.*, 2007). This study found that 77% of female students fell for the phishing attack as opposed to 65% of male students who fell for these attacks. Similarly, results from another

study show that men are more likely to correctly differentiate between phishing websites and legitimate websites than women (Kumaraguru *et al.*, 2007). The above studies show that gender does have an effect on online security awareness.

2.7.4 Employment Status Influence on Online Security Awareness

Siponen (2001) identified five dimensions of information security awareness. These are the organisational dimension, the general public dimension, the socio-political dimension, the computer ethical dimension and the institutional educational dimension.

The organisational dimension refers to the different categories of employees who need to be aware of different aspects of information security. These categories include: top management, Information Technology/Information Systems management, information security staff, computing/Information Systems professionals, end-users of various types (e.g., casual end-users, parametric end-users, sophisticated end-users and stand-alone users). For example, IT management should be responsible for implementing and creating information security policies, while end-users need to be responsible for following these policies. More security training takes place here than in the other dimensions. This study also looked at whether these users were more aware of online security awareness (i.e. employed individuals) than student users; thus, looking at whether organisational dimension users are more aware of online security.

Results of a study by Hashim *et al.* (2009) show that employment status does affect online shopping behaviour. The results indicate that respondents who had a higher income per month and were in top management level jobs were more likely to do online shopping compared with those employed at lower levels. A reason for this, at as stated in the study, could be that these respondents have easier access to credit cards which allowed them to do online shopping.

To guide this study, an appropriate framework had to be considered. The theory that was considered was a fear appeals model known as Protection Motivation Theory by Rogers. The next section will discuss what fear appeal strategies are. This will be followed by sections describing the model used for this research study.

2.7.5 Fear Appeals

One way to guide this study is to see whether "fear appeals" impact user awareness of online security. There have been over 50 years of research on fear appeals in many different subjects and these studies have collectively gathered mixed results (Ruiter *et al.*, 2001). Fear appeals are

commonly used in health campaigns that are designed to change behaviour, for example these would include campaigns against drug use, drinking and driving, and unsafe sexual practices. In terms of the health context, fear appeal messages have been used regarding condom use (Witte, 1992), the spread of sexually transmitted diseases (Witte *et al.*, 1998), AIDS (Dillard, *et al.*, 1996), skin cancer (Stephenson & Witte, 1998), and breast cancer (Kline & Mattson, 2000).

Fear appeals normally begin with the appearance of the negative consequences of certain behaviour, followed by a recommendation in which a solution to the health risk is offered. The majority of empirical studies investigating the effects of fear appeals on persuasion have established that more fear leads to more persuasion (Das, 2001).

Fear appeal strategies essentially are made up of two components (Dillard and Anderson, 2004):

- A threat is posed which is aimed at causing a negative awareness by way of showing susceptibility and severity of aversive consequences to the receiver of the message who is connected with a particular behaviour or belief.

- Immediately following the threat is a suggestion of substitute action or belief that, if followed, is perceived by the receiver of the message to result in the decline of the perceived threat.

2.7.6 Model of Fear Appeal Strategies

This model is made up of three main components.

- The problem: which is a fear provoking statement to a certain behaviour.
- The reaction: which essentially is the target audience who experiences anxiety
- The solution: which is a suggestion designed to reduce fear through an alternative behaviour or attitude (Dillard and Anderson, 2004).

Figure six, below, shows the relationship between these components.

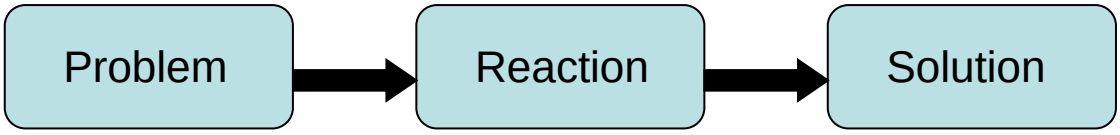

Figure 6: Fear Appeal Strategies (Dillard and Anderson, 2004)

Most fear appeal strategies have a dialogue structure. There are essentially three components that make up this dialogue. These are:

- The argument, in which proponent P actually engages in communication with the respondent R, who is the audience.
- The purpose of the dialogue is to get P to get R to carry out a particular action A.
- This means of getting the conformity centres on a danger which is D, which is a very bad outcome from R's perspective, which generally represents a potential loss of R's continued safety or well-being. (Wilson, 2004).

The characteristic of D in the fear appeals argument is that P thinks that D is particularly fearful of R. The basic dialogue structure for this argument would be:

If you get (P) to engage with (R) to carry out (A), then D will not occur (Wilson, 2004).

The next section will discuss the fear appeals strategy used in this study, this model is called Protection Motivation Theory (PMT).

2.8 Protection Motivation Theory

To guide this study, the model considered was Protection Motivation Theory (PMT) developed by Rogers. This theory serves to explain the effect of fear on attitude change and behaviour. Protection motivation theory states that an individual's motivations or intentions to protect himself from harm are improved by four critical perceptions: the severity of the risks, personal vulnerability to the risks, self-efficacy or confidence in one's ability to perform the risk-reducing behaviour, and the response efficacy of the risk-reduction behaviour (Rogers 1983). Application of these constructs in terms of this study is discussed further in Chapter three.

Protection Motivation Theory postulates that a fear appeal will provide a drive for the individual to measure the severity of an event, the likelihood of the event's incidence, and confidence in the efficacy of the message's suggestion. These factors provoke "protect motivation" which presents the reason for change (Keller, 1999). On the other hand, there could be a boomerang effect, that is, if individuals feel threatened but have no useful way to protect themselves, then intentions to change behaviour are expected to be very low. In this instance, the individual will resort to denial, avoidance and wishful thinking (Roser and Thompson, 1995). Researchers established that self-efficacy, which is basically an individual's confidence in their ability to perform a certain task, plays a significant role in the explanation of protective behaviour

(LaRose *et al.*, 2008, Youn, 2009). Protection Motivation theory has been used in other information security research, as discussed below.

2.9 Protection Motivation Theory Used in Other Information Security Research

Protection Motivation Theory has been used to observe users' protective behaviour in online transactions (LaRose *et al.*, 2006; Youn, 2009). Youn's (2009) study showed that perceived vulnerability and information revelation benefits affect online privacy protection behaviour. This theory was also used to observe employees' awareness of organizational information security policies (Herath & Rao, 2009; Siponen *et al.*, 2010). This model was also used to examine individuals' use of security software (Johnston & Warkentin, 2010). A number of studies used constructs from Protection Motivation Theory and incorporated them with other factors connected to information disclosure behaviour, like privacy concerns (Young & Quan-Haase, 2009; Acquisti & Gross, 2006), locus of control (Lo, 2010), and trust (Dwyer *et al.*, 2007).

Banks *et al*. (2010) observed information-sharing behaviour in Social Networking Websites by using Protection Motivation Theory and the theory of social influence as a framework. This study investigates how Social Networking users have made a mental calculation by trading-off the possible vulnerability and severity of the threat with the rewards related to risky online behaviour. The results of this study show that rewards offset the effect of perceived severity and vulnerability which resulted in a lower threat assessment, which, in turn, led to elevated motivation to employ the risky behaviour. Protection Motivation Theory was also used in research that examined users' attitudes towards password mechanisms. Results show that users are currently not motivated to adopt proper password practices. Users do not believe that they can stop a hacker from getting into the system. They also believe that somebody getting in could not cause them any serious personal harm.

2.10 Conclusion

Security technology may be getting more sophisticated, but that does not mean users are more aware of security and they are often the last line of defence against viruses and other potentially costly security threats (Mitnick, 2002).

Security is improved more effectively by designing for how users actually behave. In order to achieve this, a process of user education in online behaviour could possibly assist to improve online security. This chapter discussed the factors that influence online security awareness and discussed the model of choice for this study. This research will investigate whether or not demographic (inclusive of factors like employment status, gender, race, language, community) play a role in determining online security awareness. The next chapter describes the research design and methodology of this study.

Chapter 3: Research Design and Methodology

3.1 Introduction

This exploratory study is based on assessing what the current levels of user awareness of online security are and whether demographic factors have an impact on this. The instrument that was used for this research was an online survey.

3.2 Protection Motivation Theory

The reason for the use of Protection Motivation theory is that, although it is an older model, it has been used in other research over the years and has been effective, particularly in the medical field (Grindley *et al.*, 2008). According to the Protection Motivation Theory, there are two sources of information. These are: environmental and intrapersonal. Environmental sources refer to verbal influence and learning by observing. Intrapersonal sources refer to information obtained due to prior experience. This information is either an 'adaptive' coping response (i.e. the intention to improve one's online security practices) or a 'maladaptive' coping response (e.g. avoidance, denial "Online threats do not affect me") (Rogers 1983). Protection Motivation Theory (PMT) was originally developed for communicating fear in people. It was later used to motivate people to avoid unhealthy behaviour and it is thus applicable to any attitude-change behaviour (Rogers 1983).

Information systems research has theories relating to technology adoption. To guide this approach, an appropriate framework had to be considered. In the Information Systems discipline, there are theories such as Technology Acceptance Model (Davis, 1989), Unified Theory of Acceptance Use of Technology (UTAUT) (Venkatesh *et al.*, 2003), and Diffusion of Innovation Theory (amongst others) (Rogers, 1995). The Technology Acceptance Model states that perceived usefulness and perceived ease of use determine an individual's intention to use a system (Davis, 1989). Online security behaviour comprises more than just technology adoption. Online security behaviour also includes other behaviours, such as choosing strong passwords, identifying and avoiding placing details on phishing websites and being cautious with suspicious email attachments. These actions do not involve the adoption of any technology but require the user to decide to perform the right actions to prevent data from being lost or compromised. For this type of research, Information System theories like the Technology Acceptance Model, are not suitable as the primary focus of these models is the adoption of technology by users. There has, however, been new research which has showed that there are considerable differences between positive technologies (used for designed utilities) and

protective technologies (used to avert negative occurrences) (Boon Yuen, Kankanhalli, & Xu, 2009). Security technologies belong to the category of protective technologies as they are used to prevent incidents, such as virus attacks.

The above argument gives the motivation to look for theories that are more suitable for the study of the usage of protective technologies. According to recent research, there are similarities between protective security behaviour and preventive healthcare behaviour (Boon Yuen *et al.*, 2009). An example of protective security behaviour would be the use of an alpha-numeric password (or a strong password) to prevent someone from accessing a user's account. In terms of preventative healthcare behaviour, an example would be avoiding smoking to prevent lung diseases. Preventive healthcare refers to actions that will extend an individual's healthy life or decrease the risk of diseases (Jayanti & Burns, 1998). Protective security behaviour refers to actions that will decrease the risk of security occurrences (Boon-Yuen *et al.*, 2009). Both involve taking action to prevent an undesirable situation. Success, in terms of protective online security, will be achieved when users take action to prevent their information systems being compromised. Success, in terms of preventative healthcare, can be regarded as individuals taking actions to ensure that they stay healthy and thus avoid diseases. Basically, diseases interrupt the normal functioning of an individual's body; in the same way, the incidence of security threats also interrupt the normal functioning of an individual's information system. Similarly, computer viruses interrupt the normal functioning of a computer system and preventative behaviour will avoid computers getting viruses (i.e. by installing antivirus and/or anti spyware software).

Research in the online security domain has made use of Protection Motivation Theory (See Chapter 1). In a study by Youn (2005) high school students were surveyed to establish teenagers' willingness to provide information on the Internet. The study found that the greater the perception of risk of information exposure, the less willing students were to provide information. What was also found was that when teenagers perceived that the information would be more beneficial, they were more likely to disclose information about themselves. In another study, Lee and Larsen (2009) applied Protection Motivation Theory to virus protection. The findings show that perceived vulnerability, response efficacy and coping self-efficacy projected intentions to use virus protection, with self-efficacy being the most powerful variable influencing the results. Perceived severity and response efficacy did not influence safety intentions. Another study, which involved undergraduate student computer users, showed that perceived vulnerability, perceived severity, response efficacy, and response cost impacted upon

users' behavioural intention to use anti-spyware software as a protective technology (Chenoweth *et al*., 2009).

3.3 Elements of PMT

Figure seven, below, shows that each of the elements would result in individuals taking action to ensure protective behaviour. Severity looks at the level of harm of the particular unhealthy behaviour. Vulnerability refers to the probability that an individual will experience harm from the specific behaviour. Response efficacy and self-efficacy come from a coping appraisal, which is a component of Protection Motivation Theory (Rogers 1983; Rogers and Prentice-Dunn, 1997). Response efficacy refers to the belief that carrying out the coping action removes the threat. Self-efficacy is the belief that the individual can successfully perform the coping response (Rogers 1983). Coping appraisal consists of the individual's review of the response efficacy of the suggested behaviour (Rogers and Prentice-Dunn, 1997).

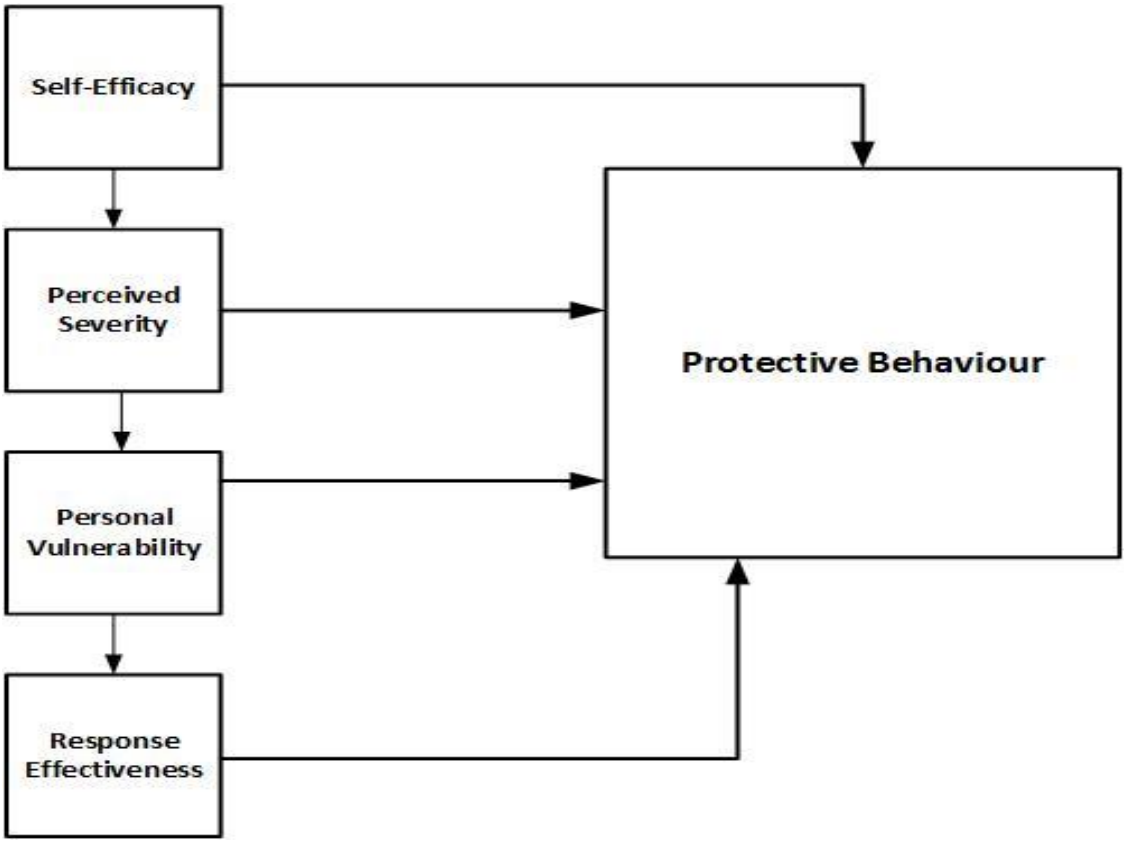

Figure 7: Protection Motivation Theory (Rogers 1983)

An adaptation of the PMT to the study at hand yields the following variables:

- Self-efficacy (e.g. 'I am confident that I can change my behaviour online so that my information is more secure')
- Severity (e.g. 'Online threats are dangerous')
- Vulnerability (e.g. 'the chances of my information being stolen/modified/used
- against my will are high').
- Response effectiveness (e.g. 'changing my online behaviour would help protect my information resources')

Figure eight, below, shows the effect of the above constructs on fear, on attitude and on behaviour change.

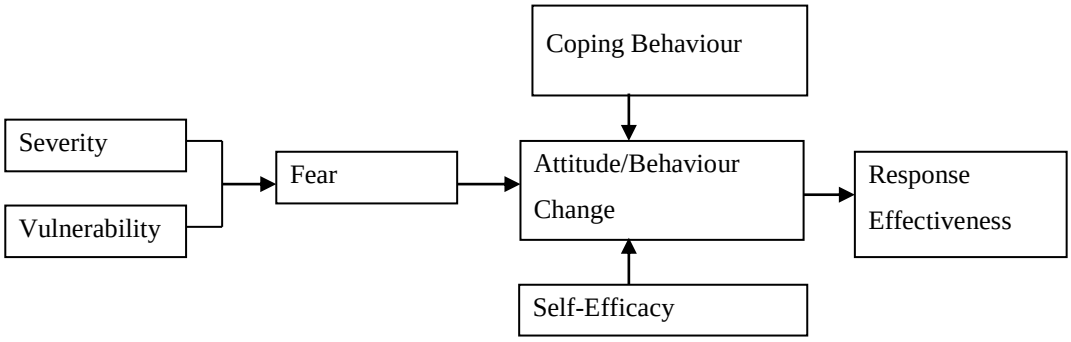

Figure 8: Conceptual Framework of PMT (Rogers 1983) (Adapted)

In terms of this research, Protection Motivation will be adapted to help determine whether users' demographic factors, particularly gender, home language, community and employment status, has an impact on their online security awareness. The choice of these factors was based on findings of previous studies that showed that they had affected online security awareness. Below is a table that shows which studies these are, as well as the demographic factor/s that impacted online security awareness.

Table 3: Literature of Factors That Impact Online Security Awareness

Study	**Demographic factor affected**
Sheng *et al.*, 2010	Gender, Age
Milne *et al.*, 2009	Gender, Race, Age, Employment status
Grobler *et al.*, 2012	Community

Jagatic *et al.*, 2007	Gender
Kumaraguru *et al.*, 2007	Gender, Age
Hashim *et al.*, 2009	Gender, Employment status

The level of user online security awareness will also be determined in this research. Figure nine, below, is the model based on Protection Motivation Theory that has been adapted for this research study.

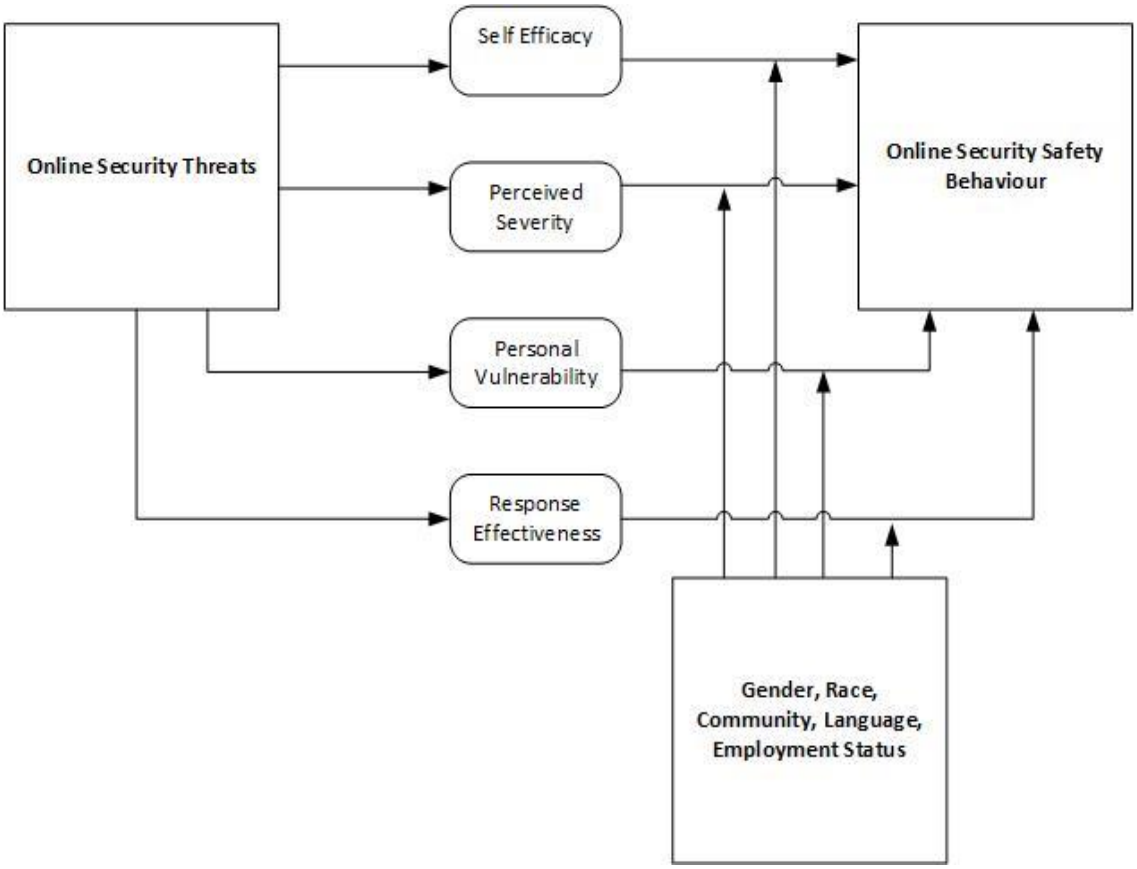

Figure 9: Conceptual Framework of PMT (Rogers 1983) (Adapted)

3.4 Hypotheses

Based on the model depicted above (Figure 9) the following hypotheses were derived. The variables in these cases were the demographic factors, i.e. race, language, community, gender, employment and physical security awareness. The constructs of the model are as stated above: self-efficacy, risk severity, vulnerability and response effectiveness. The effects that the variables have on the constructs will determine users' awareness of online security.

If a positive relationship exists between the constructs and the variables, then it can be concluded that online security awareness is higher. If there is a negative relationship between the constructs and the variables, then it can be concluded that online security awareness is lower. According to the literature (Section 2.7.1) race or ethnic background was found in studies to be a factor in influencing online security awareness, thus the constructs of protection motivation theory will be used to test this variable. Linked to this variable, however, are language and community.

H_{10}: Users' race does not influence their online security awareness

H_{1A}: Users' race influences their online security awareness

H_{20}: Users' language does not influence their online security awareness

H_{2A}: Users' language influences their online security awareness

H_{30}: Users' community does not influence their online security awareness

H_{3A}: Users' community influences their online security awareness

Similarly, according to the literature (Section 2.7.3) gender was found in studies to be a factor in influencing online security awareness, thus the constructs of protection motivation theory were also used to test this variable.

H_{40}: Users' gender does not influence their online security awareness

H_{4A}: Users' gender influences their online security awareness

It was also found that employment status did influence online security awareness, according to literature (Section 2.7.4). The constructs of protection motivation theory were used to test this variable.

H_{50}: Users' employment status does not influence their online security awareness

H_{5A}: Users' employment status influences their online security awareness

3.5 Sample and Method

The primary sample group for this research is students and young employed adults. Earlier, it was mentioned that the younger generation of users were more net-savvy, although it was revealed in a study by Little (2008) that the student population is not overly concerned about privacy and security issues. This study concludes that there is a need to develop awareness of personal and professional risks due to the huge number of online threats. This age range was

chosen for this study because students' perceptions were being measured as well as young employed adults. Also, this population was chosen to see if privacy concerns of students at the University of KwaZulu-Natal were similar to those in Little's (2008) study.

The primary population in this study consisted of young adults from the University of KwaZulu-Natal as well as the researcher's Facebook and Twitter friends (as well as their friends). The target group was young adults. In the South African context, the national youth policy defines youth as people between the ages of 14 and 35 years old (National Youth Policy, 2009). This sample consisted of people in this age range. The method that was used was surveying, which is the process of performing a study from samples of specific populations. In terms of this research, the sample consisted of young adults.

The questionnaire was e-mailed to prospective participants at the University of KwaZulu Natal where they could submit it electronically. This survey was mailed to all students, not just students with an IT background. For the snowball sample, the survey was sent to the researcher's Facebook friends and Twitter followers who fitted the criteria. The reason for the snowball sample was so that the researcher could gain access to young employed adults.

3.6 How Snowball Sampling through Facebook was Achieved

According to research, Facebook is a valuable tool for snowball sampling due to its size (Bhutta, 2012). Other studies state that the average adult user has 229 friends on their profiles (Hampton *et al.*, 2011). When person A posts on person B's wall, this post is available to all person B's friends. In terms of this research, the survey was posted on the researcher's wall and then shared by people from the researcher's friends list on their walls, thus people that the researcher did not know had access to the survey. Figure 10, below, shows a post that a friend on the researcher's Facebook friends list put up. As can be seen, the researcher was tagged in the post, thus people from both the individual's friends lists would be able to see the post. Figure 11, below, shows a post that the researcher put on Facebook that was shared by another person on the researcher's friends' list to their friends. This created a snowball effect. People on the researcher's Facebook page also posted the survey link on various group pages.

Figure 10: Survey Distributed to Researcher and Researcher's Friends' Friends on Facebook

Figure 11: Survey Distributed to Researcher's Friends on Facebook and Shared

3.7 How Snowball Sampling through Twitter was Achieved

Twitter was also used to gather data. In this case, the researcher put up the link of the survey on the respective Twitter profile thus allowing one of the followers to see it and respond. The post with the link was then re-tweeted by the researcher's followers on Twitter to all the people on their follower lists. This is shown in both figure 12 and figure 13 below.

Figure 12: Survey Distributed by Researcher's Twitter Followers

Figure 13: Survey Distributed by the Researcher to Her Twitter Followers

3.8 Questionnaire

The questionnaire was an online questionnaire. Thus, the users that did not fit the criteria (young adults) were not used in the sample and were thus not reflected in the results. This was done by excluding the respondents who did not fit the criteria from the spread sheet that was imported into SPSS for statistical analysis. This was ensured by not including these responses in the analyses, when running the data through SPSS. The questionnaire was e-mailed to prospective participants, where they could submit it electronically.

The table below shows the constructs that make up the questionnaire in detail.

Table 4: Questionnaire Constructs

Contructs	**Question**
Demographic information	Questions 1-10
Internet usage questions	Questions 11 – 16
Perceived severity	Email attachments may contain viruses or other malware and care must be taken when opening them
Perceived severity	I am concerned about the current state of online security in South Africa
Personal vulnerability	I feel safe about placing my credit card details online
Personal vulnerability	I have had my credit card details stolen and used in an online transaction
Personal vulnerability	Do you know of anyone else who may have had their credit card or card number stolen and used in an online transaction
Personal vulnerability	I keep my property locked at all times as I fear being a victim of crime
Personal vulnerability	I take significant precautions to ensure that my family does not become a victim of a crime
Response effectiveness	I feel that installing anti-virus software will keep my computer safe
Response effectiveness	I feel that installing anti-Spyware software will keep my computer safe
Self efficacy	Under certain conditions I will give my username and password to a friend
Self efficacy	Under certain conditions I will give my username and password to a stranger
Self efficacy	I know the difference between a virus and a Trojan
Self efficacy	I would be able to tell if my computer was hacked or infected
User Awareness	I feel that my computer is very secure
Self efficacy	Is the firewall on your computer enabled?

Self efficacy	Is your computer configured to be automatically updated?
Self efficacy	I know what an email scam is and how to identify one
Self efficacy	My computer has no value to hackers, they do not target me
Self efficacy	I would be comfortable using the Internet to conduct business
User Awareness	How often do you change the password on your computer?
User Awareness	A phishing attack is...
User Awareness	An example of an e-mail scam is....
User awareness	What it is that you fear most with regards to online banking?
User awareness	What is it that you fear with regard to making online purchases? Select all those that apply to you
User Awareness	What is it that you fear with regard to social networking?
User Awareness	I get most of my information about online security from
User Awareness	What is your perception of online security training?
User Awareness	I would like to learn about online security
User Awareness (Privacy)	Tick each that apply, I provide the following information on social networking websites:

3.9 Pilot Study

The pilot study was carried out during a practical session for a first year module (ISTN100). The total number of respondents to the survey was 46. The students were directed to a website that allowed them to access the online survey. The pilot was used to test the questionnaire for omissions and/or inconsistencies. Those that were found were corrected, before sampling proper was started. The pilot results were not used in the final analysis.

3.10 Limitations and Strengths of Design

There were some limitations that, if eliminated, could have meant that more accurate results would have been provided. The major disadvantage of these sampling methods was that there was a possibility that the population being studied was not represented accurately. This however, would not have impacted the results significantly as this exploratory study's primary population group was young adults. The strength of the convenience sampling technique was that it enabled the researcher to attain a high response rate in the given time frame.

Also, due to the fact that the researcher was primarily using participants from their friends' lists, this could have causes bias in the response rate. That stated, the strengths of using the snowball sample via Facebook and Twitter made it possible to reach a larger segment of the population that the researcher would otherwise not have had access to.

Chapter 4: Results and Discussion

4.1 Introduction

The aims of this exploratory study are to discover the factors that play a role in influencing user awareness of online security and the current state of user awareness of online security. These results are presented in this chapter as well as chapters five to seven.

This chapter will firstly show the age range of respondents and response rate. This will be followed by sections on the tests that were used as well as how analysis was performed. This will then be followed by a section on how respondents answered, generally, and how the model was used. Thereafter, sections on fears regarding online purchasing, online banking and social networking will follow. All results for this study were analysed by a statistician (See Appendix A).

4.2 Response Rate

The online survey ran from April 2012 to June 2012 with a total of 323 respondents. The sample included people from a diversity of backgrounds spread evenly across gender and race.

4.2.1 Age

The majority of respondents fell into the 18-22 age range; this is due to the fact that most individuals who participated in the survey were students. This does have an impact on the study as most respondents in this age range are undergraduate students and will not be expected to have the knowledge that other age ranges in the sample would have, regarding online security.

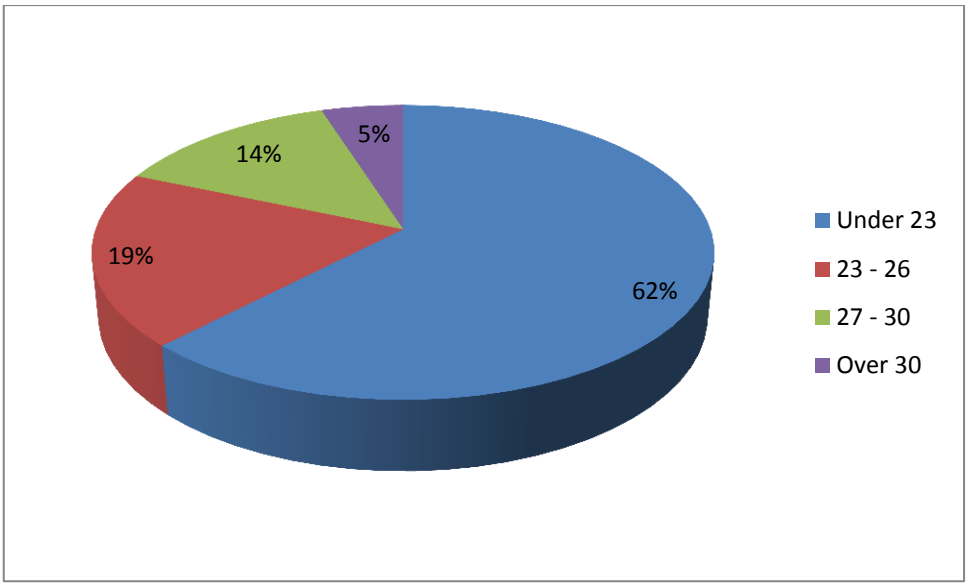

Figure 14: Age Range of Respondents

4.3 How Analyses Were Performed

As the questions required categorical responses, normality does not apply. Thus normality tests and t tests were not performed on the sample. With regard

to questions dealing with online security awareness, where the options were 'strongly agree' to 'strongly disagree' a categorical chi-square goodness of fit test was performed as it was more appropriate than a t-test if the distribution of the responses is not normal. This test was performed to show whether options were selected equally or not. The chi square goodness of fit test is often used by researchers to determine the goodness of fit between theoretical and experimental data (Centre for Innovation in Mathematics teaching. n.d).

To view the options presented by the questions discussed refer to the survey provided in Appendix F. For all statistical tables refer to Appendix G.

4.4 General Online Security Awareness

This section shows the results for the respondents' user awareness as a whole. For the question "How often do you change your password on your computer?" the results from a chi-square goodness-of-fit test show that the response options have not been selected equally (χ^2 (N = 323, 4) = 276.489; p < .0005). Specifically significant was that more of the respondents indicated that they seldom change the password on their computers. Twelve per cent of respondents stated that they change their passwords regularly, 28% of respondents stated that they

sometimes change their passwords, 36% of respondents stated that they seldom change their passwords and 25% of respondents stated that they did not change their passwords at all. From this result, it can be deduced that the majority of respondents do not change their passwords regularly (Appendix F, question 11). Good password practices include changing one's password regularly; the general rule of thumb is to change it once every three months (Hartley & Abrams, 2009). Therefore, most respondents in this study are not following this practice.

In terms of respondents feeling that their computers were secure, the chi-square shows that significantly ($p<.0005$) most respondents agree or are neutral and fewer are in disagreement (Appendix F, question 17). Forty seven per cent of respondents agreed with this statement, 37% neither agreed nor disagreed and 16% of respondents disagreed with this statement. Thus, more respondents believe that their computers are very secure.

The responses to the user awareness question regarding phishing attacks showed that most respondents are not aware of what a phishing attack is as most of them chose the wrong answer for it. The question for "a phishing attack is…" had the following three options:

- is an email masquerading as a message from a trusted source
- is an attempt to make a computer resource available to its intended users
- is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques

The first option is the correct definition of phishing, namely, that it is an email masquerading as a message from a trusted source (Mailfrontier 2004, Dell Sonicwall 2008, Club Norton 2013). The second option is the definition of a denial of service attack, which is an attempt to make a computer resource available to its intended users (Solari 2009, Al Islam & Sabrina 2009). The third option is the definition for social engineering, which is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques (Hall 2012, Apau 2011).

The chi-square showed that, significantly, ($p<.0005$) most respondents chose the third option, which is the wrong answer to the question. Twenty nine per cent respondents chose the first option (which is the correct answer to the question), 17% chose the second option and 54% chose the third option. This shows that the majority of respondents are not aware of what a phishing attack is.

The majority of respondents know what an anti-virus is and have it installed on their computers. The chi-square showed that significantly ($p<.0005$) more respondents selected 'yes' to knowing what an anti-virus is and having it installed on their personal computers of respondents stated that they have anti-virus software installed on their computers, thirteen per cent stated that they do not have anti-virus software installed on their computers, 6% stated that they do not know how to tell if anti-virus is installed or not and 2% of respondents stated that they do not know what anti-virus software is (Appendix F, question 22).

4.5 Self-Efficacy of Respondents

For the question "Under certain conditions I will give my username and password to a friend?" the results of the chi-square test show that the selection of response options is not equal. Disagreement responses were selected significantly more often than expected ($p<.0005$). Twenty per cent of respondents agreed that they would give their username and password to a friend under certain conditions, 20% neither agreed nor disagreed, 60% of respondents disagreed with this statement (Appendix F, question 12).

Similarly, strong disagreement was shown for the question "Under certain conditions I will give my username and password to a stranger?" The chi square result indicates a significant strong disagreement ($p<.0005$). Three per cent of respondents stated that they would give their username and password to a stranger under certain conditions, 1% of respondents neither agreed nor disagreed, and 96% of respondents disagreed (Appendix F, question 13). This shows that in terms of password security users are more net-savvy as they claim to protect their passwords. In terms of Protection Motivation theory, the construct to which these questions are related in these instances is self-efficacy, since the users' were in strong disagreement. They recognize that revealing their password could result in negative consequences and therefore refrain from it.

Respondents were also confident in their ability to tell if their computer is hacked or has a virus. This showed in the results of the question "I would be able to tell if my computer is hacked or infected?" which showed a significantly ($p<.0005$) strong agreement (Appendix F, question 16). Forty eight per cent of respondents agreed with this statement, 27% neither agreed nor disagreed and 25% of respondents disagreed with this statement. This question shows that users' self-efficacy is high as most of them are confident that they would be able to tell if their computer is hacked or infected.

The majority of respondents know what a firewall is and have it installed on their personal computers (Appendix F, question 18). Sixty one per cent stated that they knew what a firewall is and have it installed on their personal computers, 13% did not have it installed on their personal computers and 20% did not know what a firewall is. This shows that users' self-efficacy is high as most of them are aware of what a firewall is and make use of it to prevent online threats.

In terms of automatic updates, the chi-square test showed that significantly ($p<.0005$) more than expected respondents stated that they have automatic updates configured on their personal computers (Appendix F, question 19). Fifty nine per cent of users stated that they have automatic updates configured on their personal computers, 22% stated that they did not have automatic updates configured on their personal computers and 19% of users did not know what automatic updates were. This shows that users' self-efficacy as a whole was high as most of them are aware of automatic updates.

There was strong agreement for the question "I know what an email scam is and how to identify one." The chi-square showed that significantly ($p<.0005$) most of the respondents agreed with this statement. Sixty three per cent of respondents claimed to know what an e-mail scam is and how to identify one, 19% neither agreed nor disagreed with this statement and 18% disagreed with this statement (Appendix F, question 21). This showed that users' self-efficacy was high as most of them claimed that they are aware of what an e-mail scam is and how to protect themselves and identify such threats.

The majority of respondents stated that they would be comfortable using the Internet to conduct business, with 65% agreeing with this statement, 21% neither agreed nor disagreed and 14% disagreed with this statement (Appendix F, question 24). The chi square test shows the result as significant as ($p<.0005$).

4.6 Perceived Severity

With regard to the question "Email attachments may contain viruses or other malware and care must be taken when opening them" results showed significance ($p<.0005$) for agreement, which indicates that most respondents selected 'agreement' as an option. Seventy six per cent of respondents showed agreement with this statement, 16% neither agreed nor disagreed and 9% were in disagreement (Appendix F, question 15). This indicates that users do have a level of awareness of e-mail viruses and malware. The construct to which this is related in the Protection

Motivation Theory model is perceived severity. In this instance, users do realise that care must be taken when opening e-mails. This awareness of online threats shows that their perception of the severity of these threats is high.

Perceived severity amongst the majority of respondents was high, with 53% of respondents being concerned about the state of online security in South Africa and 32% stating that they were somewhat concerned. Sixteen per cent of respondents stated that they were not concerned with the state of online security in South Africa (Appendix F, question 28). The chi square test shows the result as significant as ($p<.0005$), with most respondents stating that they are concerned with the state of online security in South Africa.

4.7 Personal Vulnerability

Personal vulnerability was found to be high in one question as the majority of respondents did not feel safe about placing their credit card details online. Sixty two per cent of respondents stated that they do not feel safe about placing their credit card details online, 18% of respondents stated that they did feel safe about putting their credit card details online and 20% neither agreed nor disagreed (Appendix F, question 25). The chi-square shows this result to be significant as ($p<.0005$), with more respondents stating that they do not feel safe about placing their credit card details online. On the other hand, the majority of respondents stated that they would be comfortable using the Internet to conduct business, with 65% agreeing with this statement (Appendix F, question 24). So, although they have an interest in using the Internet to conduct business, they do not place their credit card details online, possibly due to fears of losing their money through online fraud. Another point to note is that the majority of respondents are students and therefore might not have access to credit cards.

For the question "I have had my credit card stolen and used in an online transaction", the majority of respondents chose 'no' (97%) (Appendix F, question 26). The chi square showed this to be significant as ($p<.0005$). The number increases, though, when looking at the results of the next question. The results for the question "Do you know of anyone else who may have had their credit card or card number stolen and used in an online transaction?" showed that 35% of respondents said 'yes' and 65% said 'no' (Appendix F, question 27). The chi square showed this to be significant as ($p<.0005$).

4.8 Response Effectiveness

Response Effectiveness was shown to be significantly high ($p<.0005$) in both questions regarding this construct as 69% of respondents agreed that installing anti-virus software will keep their computers safe and 56% of respondents agreed that installing anti-spyware software will keep their computers safe (Appendix F, question 32 & 33). A possible reason for this discrepancy is that respondents possibly did not know what anti-spyware software is. Figure 17, below, is a diagram showing a holistic picture of the relationship between the variables and the constructs of the model.

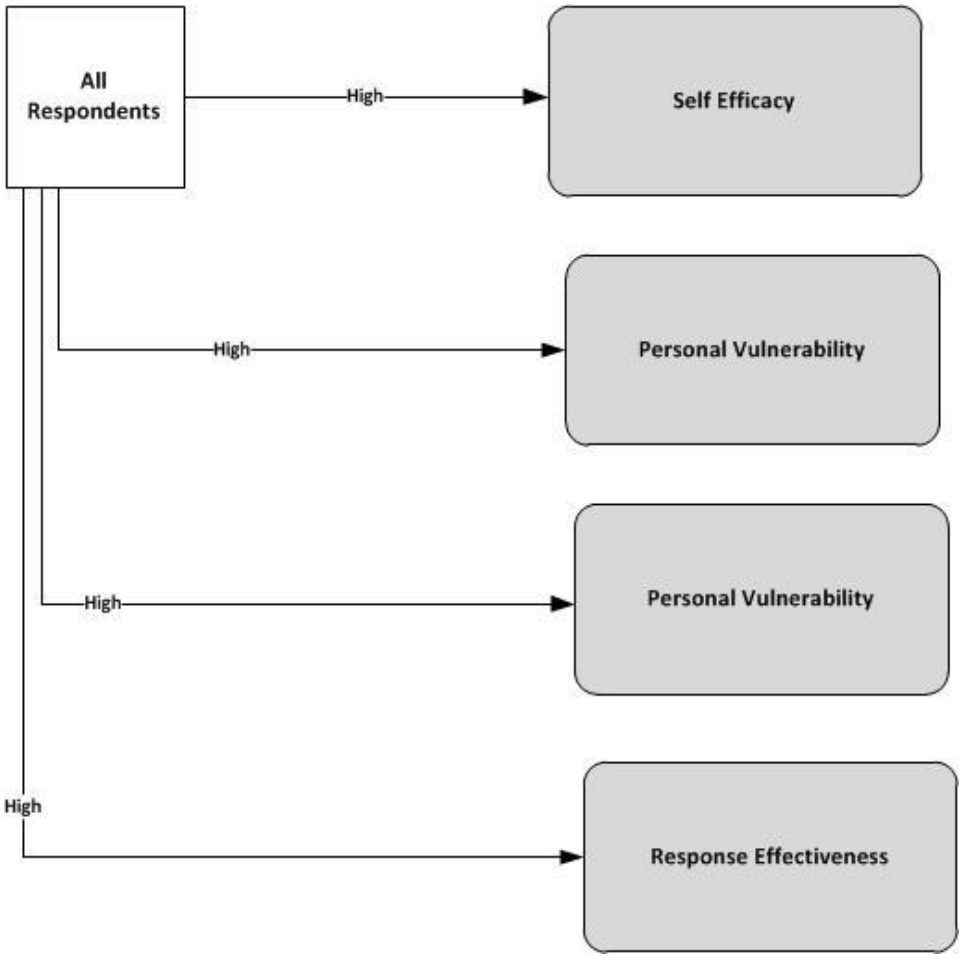

Figure 15: Protection Motivation Theory Applied to General Online Security Awareness (Adapted)

4.9 Fears Regarding Online Purchasing

In terms of online purchasing fears, the following were found by the chi square test to be significant (See Appendix G for p values):

- Money will be "lost" with no record of where it is and how it got there
- In the event that a problem arises, you will experience great difficulty proving that you paid for a product or a service
- The Internet might be new to you so there is fear of the unknown
- Fear of identity theft
- I have no fears

Seventy two per cent of respondents stated that they feared that " money will be "lost" with no record of where it is and how it got there. Forty three per cent of respondents stated that they feared that "In the event that a problem arises, you will experience great difficulty proving that you paid for a product or a service." Fifty four per cent of respondents stated that they had fear of identity theft.

Just 12% of respondents stated that "The Internet might be new to you so it is fear of the unknown" and only 8% of respondents stated that they had no fears. What was significant here was how low the percentages were in terms of users stating that they have no fears (To view all the options for this question refer to Appendix F, question 30).

4.10 Fears Regarding Online Banking

In terms of fears regarding online banking, it was found through the chi square test that there were some significant fears (See Appendix G for p values). These are:

- An outsider will be able to access my account details and steal my money
- The Internet might be new to you so there is fear of the unknown
- Fear of identity theft
- Fear of being unsure of your rights or protection if something goes wrong
- If there is a problem, there will be no way to trace where your money went
- I have no fears

Fifty eight per cent of respondents stated that one of their fears regarding online banking was "An outsider will be able to access my account details and steal my money". Evidently these respondents are wary of hackers accessing their accounts and committing fraud. Forty eight per cent of respondents chose the option "If there is a problem there will be no way to trace where

your money went". The respondents who chose this option are not confident about the systems in place, for securing their transactions. Thus their fear is directed more towards the systems in place than possible outsiders accessing their accounts. Forty three per cent of respondents stated that they feared that "In the event that a problem arises you will experience great difficulty proving that you paid for a product or a service." Thirty three per cent of respondents stated that they had fear of identity.

For the question "The Internet might be new to you so there is fear of the unknown" just 9% of respondents chose this option. This makes sense as everyone in the sample is young adults and will have been exposed to the Internet. Just 9% of respondents chose the option "I have no fears". What was significant here was how low the percentages were in terms of users' stating that they have no fears theft (To view all the options for this question refer to Appendix F, question 29).

4.11 Fears Regarding Social Networking

In terms of social networking, the following were found through the chi square test to be significant (See Appendix G for p values):

- Fear of identity theft
- Fear of my account being compromised
- I have no fears

It was found that 44% of respondents were afraid of their account being compromised. Thirty eight per cent of respondents have fear of identity theft. Twenty five per cent stated that they have no fears (To view all the options for this question refer to Appendix F, question 31).

As can be seen from the results above, respondents feared identity theft more in terms of online purchasing than social networking. This makes sense as an individual would be at a greater risk if their identity was being used fraudulently during an e-commerce transaction than if one of their social networking accounts was hacked. An individual is in danger of losing money in an online transaction, whereas the individual would not lose any money if their social networking account is compromised. Respondents' main fears were where they could potentially lose their money. Thus, the percentage of respondents who stated that they have no fears regarding online banking and online purchasing was much smaller than the percentage of respondents who stated that they have no fears in terms of social networking.

4.12 Privacy on Social Networking Websites

It was found that respondents did reveal a significant amount of personal information on social networking websites, as shown in table five below. The chi square test found all to be significant (See Appendix G for p values).

Table 5: Privacy on Social Networking Websites

My real name and surname	My real pictures	My phone number	My address	My e-mail	My work information	My interests and hobbies	My education information	My relationship status	I do not have any social networking accounts
81%	75%	35%	12%	67%	23%	67%	64%	43%	7%

Cross-tabulations were then performed against this data to show whether demographic factors influenced privacy on social networking websites. These results are shown in the chapters that follow.

In terms of where respondents got information on online security, the following were found to be significant (See Appendix G for p values):

- The media
- Government websites
- Social networking websites

Sixty two per cent of respondents stated that they got their online security information from the media. Only 10% of respondents got information on online security websites via government websites (Appendix F, question 35). In other countries, Government establishments, online operators and Internet Service Providers are currently developing educational tools for users. The United States, the FTC, the Department of Homeland Security, the Department of Commerce, and other government and private sector partners have launched a website and education campaign called ‘OnGuard’ to help individuals be on guard with regards to Internet fraud. The Australian government has also launched an awareness campaign called ‘StaySmartOnline’ and is a website that offers advice to online users about security issues. The website offers practical advice and tips on e-security for home users as well as small businesses

and families. (StaySmartOnline, 2010). The challenge is that there needs to be a prompt or a trigger so that the users look at these websites in the first place (Furnall, 2008).

What was also found was that 34% of respondents got information on online security via social networking websites. Many government establishments mentioned above (Stay Smart Online and OnGuard), also have pages on Facebook and Twitter. The issue again is that users need to know where to go to find this information, thus a prompt or a trigger would be needed to direct them to these websites.

In terms of how respondents rated online security training, it was shown that significantly fewer respondents rated it as not important ($p<.0005$). Fifty seven per cent of respondents stated that online security training was important, 37% of respondents stated that it was very important and 7% stated that it was not important (Appendix F, question 36).

4.13 Conclusion

This chapter showed the responses of respondents as a whole. The results in this chapter show that respondents have high self-efficacy, which means that the majority of individuals in this study have high user awareness. The results also show that users' personal vulnerability and perceived severity is high, which means that they are aware that they should be cautious and should refrain from risky online behaviour. Response effectiveness was also shown to be high, which means that users do realise that they should take the relevant precautions to be safe online. The chapters that follow will show what impact the variables (in this study the variables are demographic factors) have on the constructs of the Protection Motivation Theory model.

Chapter 5: Race, Language and Community Affect Online Security Awareness

This chapter will firstly show the race demographics of respondents. This will be followed by a section on the tests which were used as well as how analysis was performed. This will then be followed by a section on how the hypothesis was addressed and how the model was used.

Race demographics are shown in the figure 15, below.

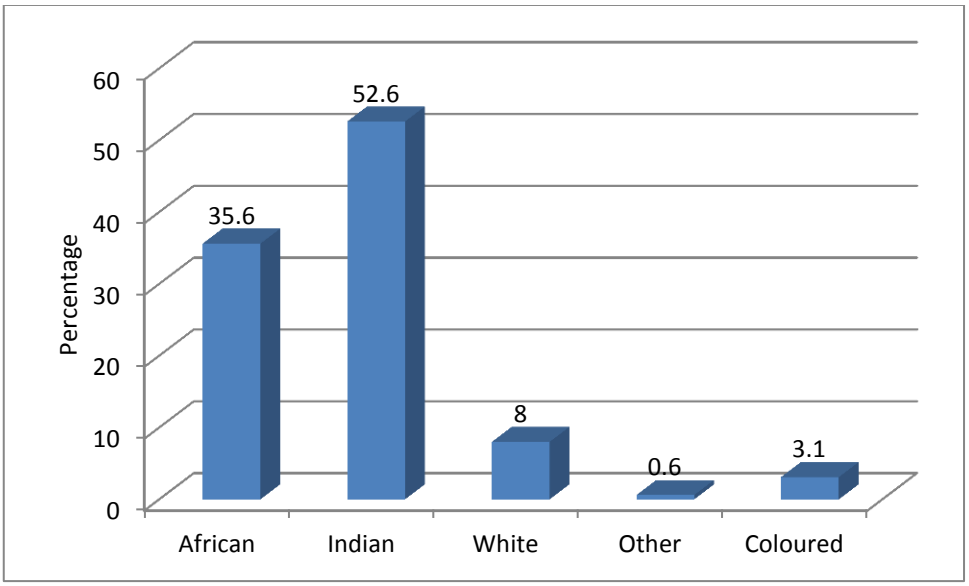

Figure 15: Race Demographics of Respondents

5.1 Addressing the Hypothesis

The main objective of this study is to determine what factors affect users' online security awareness. According to previous studies, one of these factors is race (Milne 2009). Using the constructs of the Protection Motivation theory model, it will be shown whether or not this variable (race) influences online security awareness. The following hypothesis was derived:

H_{10}: Users' race does not influence their online security awareness

H_{1A}: Users' race influences their online security awareness

5.2 How Analyses Were Performed

With regard to analysis between the demographic variables and constructs of the model, cross-tabulations were performed. The chi-square test of independence, which tests whether a significant relationship exists between the two variables, was used for cross-tabulations. Under the null hypothesis, the variables are independent (i.e. no relationship). When the conditions for a chi-square were not met (e.g. >20% of cells with expected values <5), then Fisher's exact test was applied. For Fisher's exact test the hypothesis of independence is evaluated between two categorical random variables (Springer, 2013). In this chapter, the demographic variable that was tested was race.

5.3 Self-Efficacy (Race)

In terms of Protection Motivation theory, the results show that self-efficacy was the determining factor in users' online security awareness for race. In terms of race, there were also differences in self-efficacy in a few of the questions.

- I know the difference between a virus and a Trojan (Appendix F, question 14)
- I would be able to tell if my computer is hacked or infected (Appendix F, question 16)
- I feel that my computer is very secure (Appendix F, question 17)
- Is the firewall on your computer enabled? (Appendix F, question 18)
- Is your computer configured to be automatically updated? (Appendix F, question 19)
- I know what an email scam is and how to identify one (Appendix F, question 21)

Results for the question "I know the difference between a virus and a Trojan", showed that 35% of Africans stated that they knew the difference, 65% of Indians also responded 'yes' for this question, 85% of whites responded 'yes' and 60% of coloureds responded 'yes'. This result shows that the difference between the gaps in knowledge of the African respondents is much higher than in other groups. The chi square test results indicate that significantly ($p<.0005$) most Africans responded 'no' and Indians and Whites responded 'yes'. This indicates that Indians and Whites are more aware of the difference between a virus and a Trojan than Africans.

Results for the statement "I would be able to tell if my computer is hacked or infected" show that 46% of Africans were in agreement, 50% of Indians are in agreement, 65% of Whites are in agreement and 10% of Coloureds are in agreement. The chi square test indicates that significantly ($p<.0005$) most Africans strongly disagree; most Indians, Coloureds and Other

disagree and Whites agree. This indicates that Whites and Indians are more confident than Africans and Coloureds about being able to tell whether their computer is hacked or has a virus.

In terms of the responses for the question "Is the firewall on your computer enabled?" the chi square test indicated that significantly ($p<.0005$) most Africans responded 'don't know' and the others (Whites and Indians in particular) responded 'yes'. This indicates that Whites and Indians have an idea of what a firewall is and possibly have it enabled on their computers. Similarly, for the question "Is your computer configured to be automatically updated?" the chi square test showed that significantly ($p<.0005$) most Africans responded "don't know" and Indians responded "yes". This indicates that more Indians know what this is and recognize the importance of it. It was found that, when comparing both these results, if respondents know what a firewall is, their response to the question "Is your computer configured to be automatically updated?" was "yes".

The results show that for the statement "I know what an email scam is and how to identify one" significantly ($p<.0005$) most Africans are either neutral or in disagreement; results for the other groups showed significant agreement (Indians, Whites and Other). This indicates that Whites and Indians are more confident than Africans and Coloureds about knowing what an e-mail scam is and identifying one.

5.4 Perceived Severity (Race)

In terms of race, the questions on perceived severity did not yield any significant results. Therefore, it can be deduced that this construct did not play a role in determining user security awareness.

5.5 Personal Vulnerability (Race)

Personal vulnerability was found to be low amongst all race groups. Most respondents stated that they would be comfortable to use the Internet to conduct business, although the results show that Whites are the most comfortable with conducting business online compared with all the other race groups (Appendix F, question 24). The chi square test shows that significantly ($p<.0005$) most Whites agree.

Personal vulnerability was shown to be high in some cases. For the question "I feel safe about placing my credit card details online" (Appendix F, question 25), most respondents do not feel safe about placing their credit card details online, as can be seen in the table below. Thirty one

per cent of whites were in agreement, followed by 26% of Indians, 23% coloureds and 8% Africans. This shows that personal vulnerability amongst Africans is the highest compared with all other race groups. The chi square test shows that significantly ($p<.0005$) most Africans strongly disagree. A possible reason for this could be that their user awareness is lower than the other groups, as stated in the results above. Also, for the question "Do you know of anyone else who may have had their credit card or card number stolen and used in an online transaction?" (Appendix F, question 27), Whites and Indians responded "yes" more than Africans and Coloureds. Forty two per cent of White respondents responded "yes", 45% of Indian respondents responded "yes", 20% of Coloured respondents responded "yes" and 21% of Africans responded "yes". This result could be attributed to the fact that the Indian and White respondents have had more exposure to online purchasing than the African respondents in the sample and, therefore, were more aware of online crime incidents. The chi square test shows that significantly ($p<.0005$) fewer than expected Africans selected "yes".

5.6 Response Effectiveness (Race)

Although all race groups had high response effectiveness, some were much higher than others. Eighty per cent of African and Coloured respondents agreed that installing anti-virus software will keep their computers safe (Appendix F, question 32). Sixty five per cent of Indians agreed that installing antivirus software will keep their computers safe while 50% of Whites agreed that installing antivirus software will keep their computers safe. Interestingly, 46% of white respondents neither agreed nor disagreed that installing anti-virus software will keep their computers safe. This is marginally higher than all the other groups' responses for this option. This could be because the respondents in this group do not want to commit to giving an answer to this question or do not really see installing anti-virus software as a fool-proof method for protecting their personal computers.

5.7 Discussion of PMT Model on Race

Figure 16, below, shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy was found to be high amongst Indian and White respondents, whilst Africans and Coloureds had low self-efficacy. The difference in user awareness, in this case, could be attributed to the differences in socio-economic conditions for all groups. African and Coloured respondents could have a lower knowledge base due to less exposure to technology than the other two groups, and thus have lower confidence. Personal vulnerability amongst all groups was low, as respondents stated that they felt comfortable with using the Internet to conduct business. Response effectiveness was found to be high amongst all

race groups, but lower amongst white respondents. Why this is the case can be further investigated in another study.

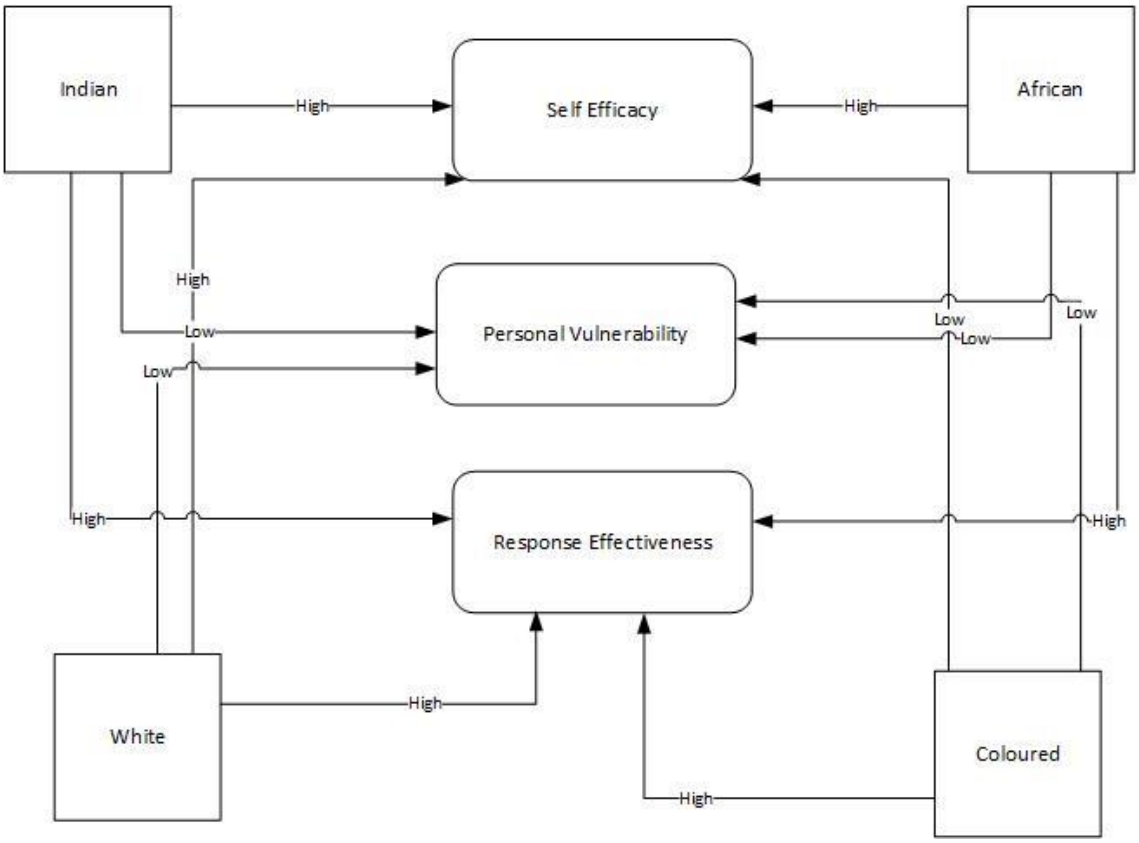

Figure 16: Protection Motivation Theory Constructs Affect Race (Adapted)

The results of this study show that race does affect online security awareness. The results of these questions show that Indians and Whites have higher self-efficacy than African respondents. Therefore, race does affect online security awareness as Indians and Whites were found to be more aware of online security than Africans. Thus the null hypothesis was rejected.

5.8 Fears Regarding Online Purchasing (Race)

In terms of online purchasing, it was found that most Indian and White respondents had fears that "someone else will gain the benefit of the money deposited." Fifty four per cent of Indians answered "yes" to this question, 46% of whites answered "yes", 37% of Africans answered "yes" and 30% of coloureds answered "yes". Another fear that was identified as significant was "In the event that a problem arises you will experience great difficulty proving that you paid for a product or a service." Fifty per cent of Indians responded "yes" to this question, 42% Whites

responded “yes”, 33% Africans responded “yes” and 30% of Coloureds responded “yes”. The chi square showed significance for both these questions (p<.0005). There was marked disagreement from all the respondents for the statement: “The Internet might be new to you so there is fear of the unknown” with 100% of White and Coloured respondents answered “no” to this question, 93% of Indian respondents answered “no” and 84% of Africans answered “no” as well (To view all the options for this question refer to Appendix F, question 30).

In terms of where respondents got information on online security awareness, numerous respondents chose the option “the media”. Fifty seven per cent of African respondents chose this option, 69% of Indian respondents chose this option, 42% of Whites chose this option and 50% of coloureds chose this option (Appendix F, question 35). The chi square showed significance for this question (p<.0005).

5.9 Privacy on Social Networking Websites (Race)

In terms of privacy on social networking websites, it was found that significantly fewer Indian respondents place their phone numbers on social networking websites than the other race groups. Forty four per cent of Africans stated that they have put their phone numbers on social networking websites, 47% of Whites stated that they have put their phone numbers on social networking websites, 80% of Coloureds stated that have had put their phone numbers on social networking websites and 25% of Indians stated that they have put their phone numbers on social networking websites. The chi square showed significance for this question (p<.0005).

Most respondents stated that they would not place their addresses on social networking websites, 19% of African respondents responded “yes” to this question, 8% of Indians responded “yes” to this question, 8% of Whites responded “yes” to this question and 20% of Coloured responded “yes” to this question. Many respondents also stated that they would place their e-mail addresses on social networking websites, 56% of Africans responded “yes” to this question, 72% of Indians responded “yes” to this question, 81% of Whites responded “yes” to this question and 80% of coloureds responded “yes” to this question. As can be seen from this result, Africans seem to be more wary about placing their e-mail addresses on social networking websites than the other groups. Most of the groups did not want to reveal their work information on social networking websites, with 11% of African respondents responding “yes” to this question, 28% of Indians responding “yes” this question, 35% of Whites responding “yes” to this question and 40% of Coloureds responding “yes” to this question. As can be seen, Africans

seem to be the most reluctant about revealing their work information compared with the other groups. The chi square showed significance for this question as (p<.0005).

There were varying responses for the question about whether respondents placed their relationship status on social networking websites. Twenty six per cent of African respondents stated that they would place their relationship status on social networking websites, 49% of Indians stated that they would place their relationship status on social networking websites, 62% of whites stated that they would place their relationship status on social networking websites and 90% of Coloureds stated that they would place their relationship status on social networking websites. The chi square showed significance for this question as (p<.0005). As can be seen from all the above questions, the African respondents were less likely to place information about themselves on social networking websites. This could mean that they value privacy more than the other race groups do (To view all the options for this question refer to Appendix F, question 34).

5.10 Language Effect on Online Security Awareness

This section will show the language demographics of respondents. Thereafter, the results of the analysis of this variable will be presented. The analysis for language was performed in the same way that it was performed for the race variable.

Figure17, below, shows the language demographics of the respondents. As can be seen from the figure, the majority of the respondents were English speaking.

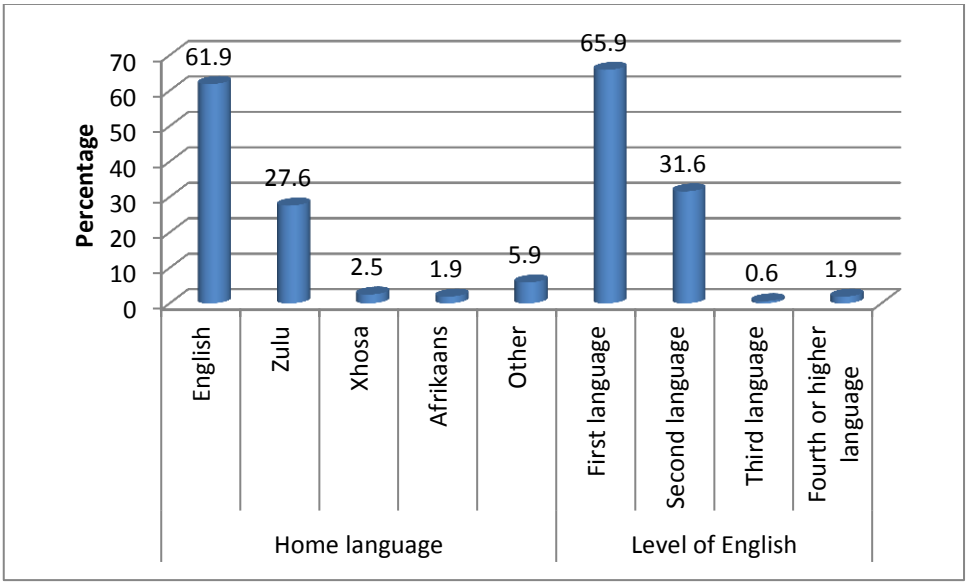

Figure 17: Language Demographics of Respondents

5.11 Self-Efficacy (Language)

In terms of language it was shown that English and Afrikaans speaking people had the highest self-efficacy from all of the groups. Although this was found for this exploratory study and the numbers of Afrikaans and Xhosa speaking people in the sample were too small to draw adequate conclusions. This was shown for the following questions:

- I know the difference between a virus and a Trojan (Appendix F, question 14)
- Is the firewall on your computer enabled? (Appendix F, question 18)
- Is your computer configured to be automatically updated? (Appendix F, question 19)
- I know what an email scam is and how to identify one (Appendix F, question 21)

The results for the question "I know the difference between a virus and a Trojan", show that 65% of English speaking people stated that they knew the difference, 30% of Zulu speaking respondents also answered "yes" for this question, 38% of Xhosa speaking people answered "yes" and 83% of Afrikaans speaking respondents answered "yes". This result shows that the difference between the gaps in knowledge of the Zulu and Xhosa speaking respondents is much higher than other groups. The chi square test results indicate that, significantly ($p<.0005$) most Zulu and Xhosa speaking people answered "no" and English and Afrikaans speaking people responded "yes". This indicates that English and Afrikaans speaking respondents are more aware of the difference between a virus and a Trojan than the Zulu and Xhosa speaking groups.

In terms of the responses for the question "Is the firewall on your computer enabled?" the chi square test indicated that significantly ($p<.0005$) most Zulu and Xhosa respondents responded "don't know" and the other groups (English and Afrikaans speaking) responded "yes". This indicates that the English and Afrikaans speaking groups know what a firewall is and have it enabled on their computers. Similarly, for the question "Is your computer configured to be automatically updated?" the chi square test showed that significantly ($p<.0005$) most Zulu and Xhosa respondents responded "don't know" or "no", while English and Afrikaans speaking respondents answered "yes". This indicates that more English and Afrikaans speaking respondents knew what this was and recognized the importance of it. It was found that when comparing both these results that, if respondents knew what a firewall is, their response to the question "Is your computer configured to be automatically updated?" was "yes".

The results show that for the question "I know what an email scam is and how to identify one" that significantly ($p<.0005$) more English and Afrikaans speaking people are in agreement than Zulu and Xhosa speaking respondents. This indicates that English and Afrikaans speaking

respondents were more confident than Zulu and Xhosa speaking respondents about knowing what an e-mail scam is and identifying one.

5.12 Perceived Severity (Language)

Perceived severity was shown to be significantly high amongst all language groups ($p<.0005$). As shown in the question "Email attachments may contain viruses or other malware and care must be taken when opening them", 81% of English speaking respondents agreed with this statement, 61% of Zulu speaking respondents agreed with this statement, 63% of Xhosa speaking people agreed with this statement, 100% of Afrikaans speaking people agreed with this statement and 89% of respondents from the "Other" group agreed with this statement (Appendix F, question 15)..

5.13 Personal Vulnerability (Language)

Personal vulnerability was shown to be high in some cases. For the question "I feel safe about placing my credit card details online", most respondents did not feel safe about placing their credit card details online. Twenty four per cent of English speaking respondents were in agreement, followed by 9% of Zulu speaking respondents, 13% of Xhosa speaking respondents and 33% Afrikaans speaking respondents (Appendix F, question 25). This shows that personal vulnerability amongst Zulu and Xhosa speaking respondents was the highest compared with all the other language groups. The chi square test shows that significantly ($p<.0005$) most Zulu and Xhosa speaking respondents strongly disagree. A possible reason for this could be that their user awareness is lower than the other groups, as stated in the results above. Also, for the question "Do you know of anyone else who may have had their credit card or card number stolen and used in an online transaction?" significantly ($p<.0005$) more English and Afrikaans speaking people answered "yes" than Xhosa and Zulu speaking people. Forty two per cent of English speaking respondents answered "yes", 83% of Afrikaans speaking respondents answered "yes", 13% of Xhosa speaking respondents answered "yes" and 22% of Zulu speaking respondents answered "yes" (Appendix F, question 27). This result could be attributed to the fact that the English and Afrikaans speaking respondents had more exposure to online purchasing than the Zulu and Xhosa speaking respondents in the sample and therefore were more aware of online crime incidents.

5.14 Response Effectiveness (Language)

All language groups had high response effectiveness. The results show that 64% of English speaking respondents agreed that installing antivirus software will keep their computers safe. Eighty per cent of Zulu speaking respondents agreed that installing antivirus software will keep their computers safe. Seventy five per cent of Xhosa speaking respondents agreed that installing anti-virus software will keep their computers safe while 67% of Afrikaans speaking respondents agreed that installing antivirus software will keep their computers safe (Appendix F, question 32). Interestingly, a higher number of Zulu and Xhosa respondents agreed with this statement than English and Afrikaans speaking respondents. This could be because some of these respondents do not really see installing anti-virus software as a fool-proof method for protecting their personal computers.

5.15 Discussion of PMT model on Language

Figure 18, below, shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy was found to be high amongst the English and Afrikaans speaking respondents, whilst Zulu and Xhosa speaking respondents had low self-efficacy. The difference in user awareness in this case could be attributed to the differences in socio-economic conditions for all groups. Zulu and Xhosa speaking respondents could have a lower knowledge base due to less exposure to technology than the other two groups, and thus have lower confidence. Personal vulnerability and perceived severity amongst all groups was high, which means that they were wary of placing their information online. Response effectiveness was found to be high amongst all language groups, meaning that respondents from all groups did realise that they should take the relevant precautions to be safe online.

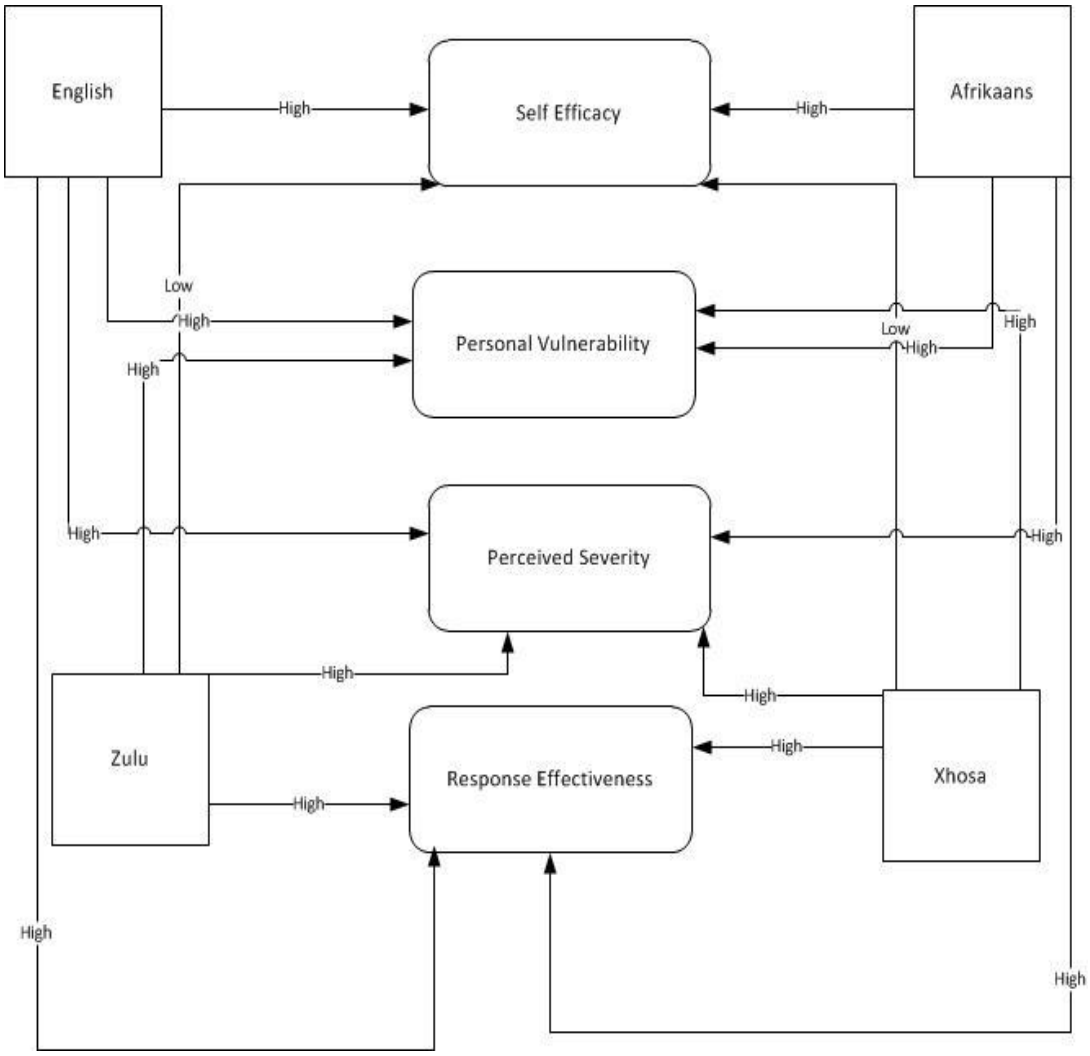

Figure 18: Protection Motivation Theory Constructs Effect Language (Adapted)

5.16 Fears Regarding Online Purchasing (Language)

In terms of online purchasing, it was found that one of the most significant fears was "In the event that a problem arises you will experience great difficulty proving that you paid for a product or a service". Forty seven per cent of English speaking respondents responded "yes" to this question, 50% of Afrikaans speaking respondents responded "yes" to this question, 31% of Zulu speaking respondents responded "yes" to this question and 38% of Xhosa speaking respondents responded "yes" to this question. There was marked disagreement from all the respondents for the statement: "The Internet might be new to you so there is fear of the unknown" with 100% of White and Coloured respondents answering "no" to this question, 94% of English speaking respondents answering "no", 86% of Zulu speaking people answering "no",

88% of Xhosa speaking people answering “no” and 100% of Afrikaans speaking respondents answering “no” as well (To view all the options for this question refer to Appendix F, question 30). The chi square showed significance for both these questions (p<.0005).

5.17 Privacy on Social Networking Websites (Language)

In terms of privacy on social networking websites, it was found that significantly (p<.0005) fewer English and Xhosa speaking respondents place their phone numbers on social networking websites than the other language groups. Twenty nine per cent of English speaking respondents stated that they had put their phone numbers on social networking websites, 49% of Zulu speaking respondents stated that they had put their phone numbers on social networking websites, 13% of Xhosa speaking respondents stated that they had put their phone numbers on social networking websites and 50% of Afrikaans speaking respondents stated that they had put their phone numbers on social networking websites. The chi square showed significance for this question (p<.0005).

Most respondents stated that they would not place their addresses on social networking websites. Nine per cent of English speaking respondents answering “yes” to this question, 22% of Zulu speaking respondents answering “yes” to this question, 25% of Xhosa speaking respondents answering “yes” to this question and 0% of Afrikaans speaking respondents answering “yes” to this question. Many respondents also stated that they would place their e-mail addresses on social networking websites. Seventy one per cent of English speaking respondents responded “yes” to this question, 58% of Zulu speaking respondents responded “yes” to this question, 25% of Xhosa speaking respondents responded “yes” to this question and 100% of Afrikaans speaking respondents responded “yes” to this question. As can be seen from this result, Zulu and Xhosa speaking respondents seem to be more wary about placing their e-mail addresses on social networking websites than the other groups. The chi square showed significance for both these questions as (p<.0005).

Most of the groups did not want to reveal their work information on social networking websites, with 72% of English respondents stating no to this question, 89% of Zulu speaking respondents answering “no” this question, 88% of Xhosa speaking respondents answering “no” to this question and 67% of Afrikaans speaking respondents answering “no” to this question. As can be seen, Zulu and Xhosa speaking respondents seem to be the most reluctant about revealing their work information compared to the other groups. The chi square shows significance for this as (p<.0005). There were varying responses for the question about whether respondents placed

their relationship status on social networking websites. Fifty two per cent of English speaking respondents stated that they would place their relationship status on social networking websites, 25% of Zulu speaking respondents stated that they would place their relationship status on social networking websites, 38% of Xhosa speaking respondents stated that they would place their relationship status on social networking websites and 50% of Afrikaans speaking respondents stated that they would place their relationship status on social networking websites. The chi square showed significance for this question as ($p<.0005$). As can be seen from all the above questions, the Zulu and Xhosa speaking respondents were less likely to place information about themselves on social networking websites. This could mean that they value privacy more than the other language groups do (To view all the options for this question refer to Appendix F, question 34) .

5.18 Community Effect on Online Security Awareness

This section will show the community demographics of respondents. Below are the definitions of each community segment:

- Urban areas: Can be defined in the South African context as places that have some system of local authority (Demographic Yearbook, 2005).
- Semi urban areas: Exhibits characteristics of both rural and urban areas (Collins, 2013).
- Rural areas: These are areas outside of cities and towns (Worldnetweb, 2013).

Thereafter, the results of the analysis of this variable will be presented. The analysis for the community variable was performed in the same way that it was performed for the race and language variables.

Figure 19, below, shows the community demographics of the respondents. As can be seen from the figure, the majority of respondents were from urban areas.

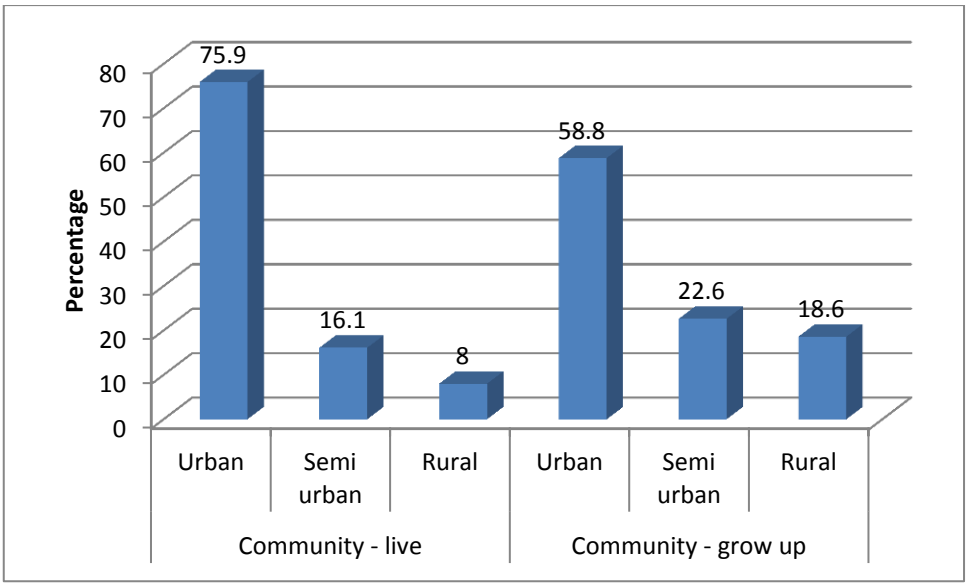

Figure 19: Community Demographics of Respondents

5.19 General Online Security Awareness (Community)

This section shows the results for the respondents' user awareness as a whole. Specifically significant was that more of the respondents indicated that they seldom change the password on their computers. Fourteen per cent of respondents from urban communities stated that they change their passwords regularly, 6% of respondents from semi urban communities stated that they change their passwords regularly and 4% of respondents from rural communities stated that they regularly change their passwords (Appendix F, question 11). From this result it can be deduced that the majority of respondents do not change their passwords regularly. The chi square shows significance for this as ($p<.0005$).

The user awareness question regarding phishing attacks showed that most respondents were not aware of what a phishing attack is, as most of them chose the wrong answer for it. Although it was found that more respondents from urban communities chose the right answer for it than the other two communities. The chi-square showed that significantly ($p<.0005$) most respondents chose the third option, which is the wrong answer to the question. Twenty nine per cent of respondents from urban communities chose the first option (which is the correct answer to the question), 23% of respondents from semi-urban communities chose the first option and 31% of respondents from rural communities chose the first option (Appendix F, question 20/Chapter 4, Pg. 42). This shows that the majority of respondents are not aware of what a phishing attack is,

although it is interesting to note that more respondents from rural areas knew what a phishing attack was than respondents from urban and semi urban communities.

5.20 Self-Efficacy (Community)

In terms of community lived in, it was shown that respondents from urban areas had the highest self-efficacy from all of the groups. This was shown for the following questions:

- I know the difference between a virus and a Trojan (Appendix F, question 14)
- Is the firewall on your computer enabled? (Appendix F, question 18)
- Is your computer configured to be automatically updated? (Appendix F, question 19)
- I know what an email scam is and how to identify one (Appendix F, question 21)

The results for the question "I know the difference between a virus and a Trojan", show that 60% of respondents who live in urban areas knew the difference, 54% of respondents who live in semi-urban areas also answered "yes" for this question, 23% of respondents living in rural areas answered "yes". This result shows the difference between the gaps in knowledge of respondents who live in rural areas compared with respondents in the other groups. The chi square test results indicate that significantly ($p<.0005$) respondents from rural areas answered "no" and respondents from urban and semi urban areas responded "yes". This indicates that respondents from urban and semi-urban areas were more aware of the difference between a virus and a Trojan than respondents from rural areas. When this question was cross-tabulated with "a phishing attack is…", results showed that 80% of respondents from urban communities who did not know the difference between a virus and a Trojan, chose the wrong answer for the question "a phishing attack is…".

In terms of the responses for the question "Is the firewall on your computer enabled?" the chi square test indicated that significantly ($p<.0005$) most respondents from rural areas responded "don't know" and the other groups (urban and semi urban) responded "yes". This indicates that the respondents from urban and semi-urban areas know what a firewall is and have it enabled on their computers. Similarly, for the question "Is your computer configured to be automatically updated?" the chi square test showed that significantly ($p<.0005$) most respondents from rural communities responded "don't know" or "no", while respondents from urban and semi urban communities answered "yes". This indicates that more respondents from urban and semi-urban communities know what this is and recognized the importance of it. It was found that, when

comparing both these results, that if respondents know what a firewall is, their response to the question “Is your computer configured to be automatically updated?” was “yes”.

The results show that for the question “I know what an email scam is and how to identify one” that significantly ($p<.0005$) more respondents from urban and semi-urban communities are in agreement than respondents from rural communities. This indicates that respondents from urban and semi-urban communities were more confident than respondents from rural communities about knowing what an e-mail scam is and identifying one.

5.21 Perceived Severity (Community)

The questions on perceived severity in terms of community did not yield any significant results. Therefore, it can be deduced that this construct did not play a role in determining user security awareness in terms of community.

5.22 Personal Vulnerability (Community)

Personal vulnerability was shown to be high in some cases. For the statement “I feel safe about placing my credit card details online”, most respondents did not feel safe about placing their credit card details online. Twenty two per cent of respondents from urban communities were in agreement, followed by 8% of respondents from semi-urban communities and 4% of respondents from rural communities (Appendix F, question 25). This shows that personal vulnerability amongst respondents from semi-urban and rural communities was higher than amongst respondents from urban communities. The chi square test shows that significantly ($p<.0005$) most respondents from semi-urban and rural communities disagree.

5.23 Response Effectiveness (Community)

Although all groups had high response effectiveness, some were much higher than others. Sixty six per cent of respondents from urban areas agreed that installing anti-virus software will keep their computers safe. Sixty four per cent of respondents from urban areas agreed that installing anti-virus software will keep their computers safe, while 83% of respondents from rural communities agreed that installing anti-virus software will keep their computers safe (Appendix F, question 32).

5.24 Discussion of PMT model on Community

Figure 20, below, shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy was found to be high amongst the respondents from urban and semi-urban communities, whilst respondents from rural communities have low self-efficacy. The difference in user awareness in this case could be attributed to the differences in socio-economic conditions for all groups. Respondents from rural communities could have a lower knowledge base due to less exposure to technology than the other two groups, and thus have lower confidence. Personal vulnerability was found to be high among respondents from semi-urban and rural communities, which means that they were wary of placing their information online. Response effectiveness was found to be high amongst all community groups, meaning that respondents from all these groups did realise that they should take the relevant precautions to be safe online.

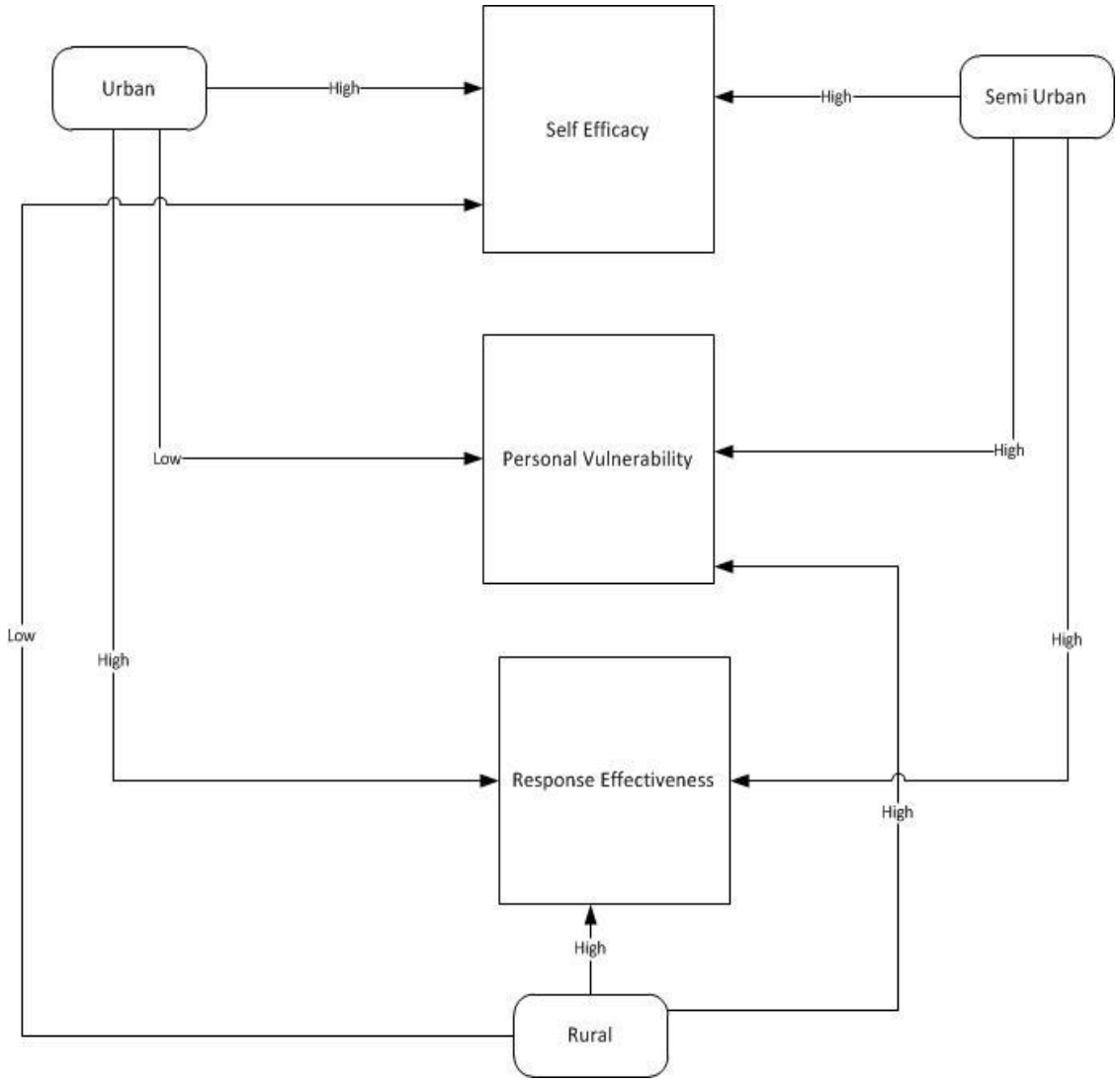

Figure 20: Protection Motivation Theory Constructs Effect Community (Adapted)

5.25 Fears Regarding Online Purchasing (Community)

In terms of online purchasing, a fear that was identified as significant was "In the event that a problem arises, you will experience great difficulty proving that you paid for a product or a service". Forty four per cent of respondents from urban communities answered "yes" to this question, 52% of respondents from semi-urban communities responded "yes" to this question and 20% of respondents from rural communities responded "yes" to this question. Interestingly, respondents from rural communities did not seem to fear this. The chi square showed significance for this question ($p<.0005$). There was marked disagreement from all the respondents for the statement "The Internet might be new to you so there is fear of the

unknown" with 94% of respondents from urban communities answering "no" to this question, 90% of respondents from semi urban communities answered "no" and 81% of respondents from rural communities answered "no" as well (To view all the options for this question refer to Appendix F, question 30).

5.26 Privacy on Social Networking Websites (Community)

In terms of privacy on social networking websites, it was found that most respondents from all groups placed their real names and surnames on social networking websites. Eighty eight per cent of respondents from urban communities stated that they place their real names and surnames on social networking websites. Eighty seven per cent of respondents from semi-urban communities stated that they would place their real names and surnames on social networking websites and 62% of respondents from rural communities stated that they would place their real names and surnames on social networking websites. This result shows that respondents from rural communities are more reluctant to place their real names and surnames on social networking websites than the other groups. The chi square showed significance for this question ($p<.0005$).

Most respondents stated that they would not place their addresses on social networking websites. Ten per cent of respondents from urban communities answered "yes" to this question, 14% of respondents from semi urban areas answered "yes" to this question and 22% of respondents from rural areas answered "yes" to this question. Many respondents also stated that they would place their e-mail addresses on social networking websites. Seventy per cent of respondents from urban communities responded "yes" to this question, 63% of respondents from semi-urban communities responded "yes" to this question and 46% of respondents from rural communities responded "yes" to this question. As can be seen from this result, respondents from rural communities seem to be more wary about placing their e-mail addresses on social networking websites than the other groups.

Most of the groups did not want to reveal their work information on social networking websites, with 26% of respondents from urban communities answering "yes" to this question, 14% of respondents from semi-urban communities answered "yes" this question and 8% of respondents from rural communities answered "yes" to this question. As can be seen, respondents from rural communities seem to be the most reluctant about revealing their work information on social networking websites compared with the other groups. The chi square showed significance for this question as ($p<.0005$).

In terms of education information on social networking websites, respondents from urban and semi-urban communities revealed their education information on social networking websites. Sixty six per cent of respondents from urban communities stated that they would reveal their education information on social networking websites. 67% of respondents from semi-urban communities stated that they would reveal their education information online and 38% of respondents from rural communities stated that they would reveal their education information online. As can be seen, respondents from rural communities seem to be the most reluctant about revealing their education information on social networking websites, compared with the other groups. The chi square showed significance for this question as ($p<.0005$).

There were varying responses for the question about whether respondents placed their relationship status on social networking websites. Forty seven per cent of respondents from urban communities stated that they would place their relationship status on social networking websites, 38% of respondents from semi-urban communities stated that they would place their relationship status on social networking websites and 20% of respondents from rural communities stated that they would place their relationship status on social networking websites. The chi square showed significance for this question as ($p<.0005$). As can be seen from all the above questions, the respondents from rural communities were less likely to place information about themselves on social networking websites. This could mean that they value privacy more than the other communities (To view all the options for this question refer to Appendix F, question 34) .

5.27 Conclusion

The above results show that race, community and possibly language have an effect on online security awareness. Thus, the null hypotheses were rejected in all these cases. The results of the study show that the awareness level of the African population group, in terms of online security awareness, is not as high as it was for other sectors. It was also found that language and community play a role in determining online security awareness. It is recommended that this type of study be expanded to determine reasons why this might be the case for all the above elements. The next chapter will look at the effect of gender on online security awareness.

Chapter 6: Gender Affect Online Security Awareness

This chapter will show the gender demographics of respondents. This will be followed by a section on the tests which were used as well as how the analysis was performed. This will then be followed by a section on how the hypothesis was addressed and how the model was used.

The results of this study show that 58% of respondents were male and 42% were female.

6.1 Addressing the Hypothesis

The main objective of this study was to determine what factors affected users' online security awareness. From previous studies, one of the factors that were shown to influence online security awareness is gender (Kumaraguru *et al.*, 2007, Jagatic *et al.*, 2007, Milne 2009, Sheng, 2009). Using the constructs of the Protection Motivation theory model, it will be shown whether or not this variable (gender) influences online security awareness. The following hypothesis was derived:

H_{40}: Users' gender does not influence their online security awareness

H_{4A}: Users' gender influences their online security awareness

6.2 How Analyses Were Performed

With regard to analysis between the demographic variables and constructs of the model, cross-tabulations were performed. The chi-square test of independence was used for cross-tabulations. It tests whether a significant relationship exists between the two variables. Under the null hypothesis, the variables are independent (i.e. no relationship). When the conditions for a chi-square were not met (e.g. >20% of cells with expected values <5), then Fisher's exact test was applied. In this chapter, the demographic variable tested was gender.

6.3 General Online Security Awareness

The user awareness question "A phishing attack is…", showed that females and males answered similarly, with slightly more male respondents getting the answer to this question correct (Appendix F, question 20/Chapter 4 Pg. 42). The chi square test shows that significantly ($p<.0005$) more than expected females and males selected the third option. The third option is the wrong option, which indicates that both genders in the study are not aware of what a phishing attack is. The majority of respondents answered this question incorrectly, with just 32% of male respondents choosing the correct answer and 24% of females choosing the correct answer.

6.4 Self-Efficacy

The results of the questions related to self-efficacy, in terms of the Protection Motivation Theory Model, show that self-efficacy amongst males is higher than among females. This links to the literature where some studies found that females were more susceptible to online attacks than males (Sheng *et al.*, 2010).

In terms of Protection Motivation theory, results showed that self-efficacy is the determining factor in users' online security awareness for gender. In this study, self-efficacy refers to a user's knowledge regarding online security, which works as a factor in determining his/her online security awareness. In terms of gender, in at least five instances, males showed higher self-efficacy than females. This was in terms of the following questions:

- I know the difference between a virus and a Trojan (Appendix F, question 14)
- I would be able to tell if my computer is hacked or infected (Appendix F, question 16)
- Is the firewall on your computer enabled? (Appendix F, question 18)
- Is your computer configured to be automatically updated? (Appendix F, question 19)
- I know what an email scam is and how to identify one (Appendix F, question 21)
- My computer has no value to hackers, they do not target me (Appendix F, question 23)

In terms of the significance results for the question "I know the difference between a virus and a Trojan", the chi square test showed that significantly ($p<.0005$) more males responded "yes" and females responded "no". Sixty nine per cent of males claimed to know the difference between a virus and a Trojan as opposed to 37% of females who stated that they knew the difference. This indicates that more males than females are confident about knowing the difference between the two.

In terms of the next question "I would be able to tell if my computer is hacked or infected?" The chi square test shows that significantly ($p<.0005$) more males are in agreement than females who are not in agreement. Sixty one per cent of males agreed with this statement as opposed to 31% of females who agreed with this statement. This again indicates that males are more confident than females about being able to tell whether their computer is hacked or has a virus.

When asked “Is the firewall on your computer enabled?” 73% of males answered “yes” while 60% of females answered “yes”. Fourteen per cent of males answered “no”, while 12% of females answered “no”. Thirteen per cent of males stated that they do not know what a firewall is, while 28% of females stated that they do not know what a firewall is. There is a big gap between male respondents knowing what a firewall is and female respondents knowing what a firewall is. Also, when compared with the question “Is your computer configured to be automatically updated?” 64% of male respondents answered “yes”, while 53% of females answered “yes”. Twenty six per cent of males answered “no”, while 17% of females answered “no”. Ten per cent of male respondents chose the option “don’t know”, while 30% of female respondents chose this option. What can be seen, when looking at the results of these two questions, is that if respondents knew what a firewall was then generally they seemed to be aware of automatic updates. For the question “Is the firewall on your computer enabled?” the chi square test showed that significantly ($p<.0005$) more than the expected number of females do not know what a firewall is. This indicates that more males know what a firewall is and have it enabled on their computers.

For the question “Is your computer configured to be automatically updated?” the chi square test showed that significantly ($p<.0005$) more than the expected number of females do not know if their computers are configured to be automatically updated. This indicates that more males know what this is and recognize the importance of it.

A significantly higher number of male respondents stated that they know what an e-mail scam is and how to identify one. Seventy five per cent of males claimed that they know what an e-mail scam is and how to identify one, compared with 47% of females who claimed that they know what an e-mail scam is and how to identify one. The chi square test shows that significantly ($p<.0005$) more males are in agreement than females who are not in agreement.

There was significant disagreement ($p<.0005$) amongst males shown for the question “My computer has no value to hackers; they do not target me”. Forty per cent of males disagreed with this statement as opposed to 24% of female respondents. Twenty nine per cent of males neither agreed nor disagreed, while 46% of females neither agreed nor disagreed. Thirty one per cent of males agreed with the statement and 30% of females agreed with the statement.

For all the above questions, males answered in the affirmative in more instances than female respondents. This showed that they are more confident in their ability to identify e-mail scams

and tell whether their computers have been hacked or infected. Also, more males know what the difference between a Virus and a Trojan is and are aware of what a phishing attack is. A further cross-tabulation between these two questions showed that 57% of males in the sample who know the difference between a virus and a Trojan also (60%) know what a phishing attack is. These results show that the male respondents in this study showed a higher self-efficacy than the female respondents.

6.5 Perceived Severity

Perceived severity amongst both males and females was high. Forty nine per cent of males stated that they were concerned with the current state of online security in South Africa, 21% of males were not concerned about the current state of online security in South Africa and 30% stated that they were somewhat concerned about the current state of online security in South Africa. Fifty eight per cent of females stated that they were concerned with the current state of online security in South Africa, 8% of females were not concerned about the current state of online security in South Africa and 34% stated that they were somewhat concerned about the current state of online security in South Africa (Appendix F, question 28). Thus, perceived severity seemed to be higher amongst the female respondents than the male respondents. This means that more female respondents were concerned about the current state of online security in South Africa than male respondents. This shows that, although females have a lower self-efficacy, their perceived severity is higher. With the male respondents, their self-efficacy is higher but their perceived severity is lower than the female respondents.

6.6 Personal Vulnerability

Personal vulnerability was higher amongst female respondents than male respondents. Seventy per cent of males agreed that they would be comfortable to use the Internet to conduct business, while 58% of females agreed that they would be comfortable to use the Internet to conduct business. Seventeen per cent of males neither agreed nor disagreed, while 27% of females neither agreed nor disagreed. Thirteen per cent of males disagreed, while 11% of females disagreed (Appendix F, question 24). The chi square test shows that significantly ($p<0.005$) more males are in agreement and females are not in agreement.

6.7 Response Effectiveness

The questions on response effectiveness in terms of gender did not yield any significant results. Therefore, it can be deduced that this construct did not play a role in determining user security awareness in terms of gender.

6.8 Discussion of PMT Model on Gender

Figure 21, below, is a diagram that shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy amongst males was high, whilst it was low amongst females. It was found that self-efficacy linked directly to user awareness, as it seemed that respondents who had knowledge regarding online security also seemed to possess a higher self-efficacy than users who did not. Personal vulnerability was found to be high in females; this could be attributed to the fact that their awareness and knowledge level was lower than the male respondents. Thus their fear regarding online security would be greater as they do not possess the ability to secure themselves online. Personal vulnerability amongst male respondents was low; this could be attributed to the fact that they are confident about being able to protect themselves as they believe that they possess the knowledge to do so. Perceived severity was high amongst both males and females.

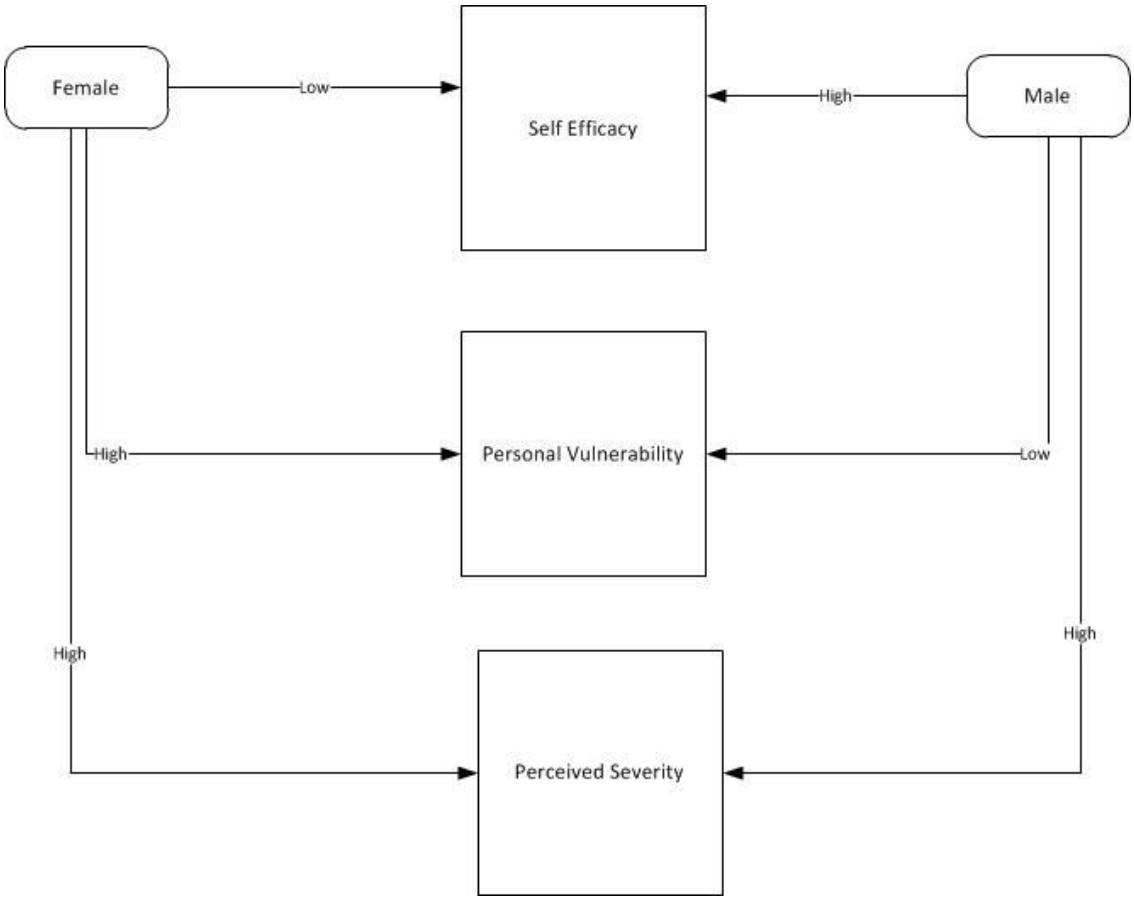

Figure 21: Protection Motivation Theory Constructs Affect Gender (Adapted)

6.9 Privacy on Social Networking Websites

In terms of privacy on social networking websites it was found that significantly more males placed their phone numbers on these websites than females. 43% of males stated that they had placed their phone numbers on these websites, while 27% females stated that they had placed their phone numbers on these websites. The chi square test shows that significantly ($p<0.005$) more males than females have answered yes to this question (To view all the options for this question refer to Appendix F, question 34).

6.10 Online Security Information and Training Importance

In terms of where respondents got their information on online security, 72% of females named "the media" compared with 54% of males who chose this option. The chi square test showed that significantly ($p<0.005$) more females than males chose this option. With regard to online

security training, it was found that both males and females found it important. Fifty one per cent of males stated that it was important while 67% of females stated that it was important. Forty per cent of males stated that it was very important, while 32% of females stated it was very important. The chi square showed that significantly ($p<0.005$) few male and female respondents view online security training as "not important". Ten per cent of males stated that it was not important and 2% of females stated that it was not important (Appendix F, question 36).

6.11 Conclusion

The above results show that males are more aware of online security than females, thus gender does affect online security awareness. Thus, the null hypothesis is rejected. As shown in the results, male respondents had high self-efficacy, thus having higher awareness of online security than female respondents. In addition, female respondents had higher personal vulnerability than male respondents, which showed that male respondents, who had a higher awareness of online security, were less cautious online than female respondents. The next chapter will look at the effect of employment status on online security awareness

Chapter 7: Employment Status Affect Online Security Awareness

This chapter will show the employment demographics of respondents. This will be followed by a section on the tests which were used as well as how the analysis was performed. This will then be followed by a section on how the hypothesis was addressed and how the model was used.

Employment demographics are shown in the figure below. As can be seen, the majority of respondents were students. The employed respondents were obtained from the snowball sampling technique through Facebook and Twitter. Although this was found for this exploratory study and the numbers of self-employed and unemployed respondents in the sample were too small to draw adequate conclusions.

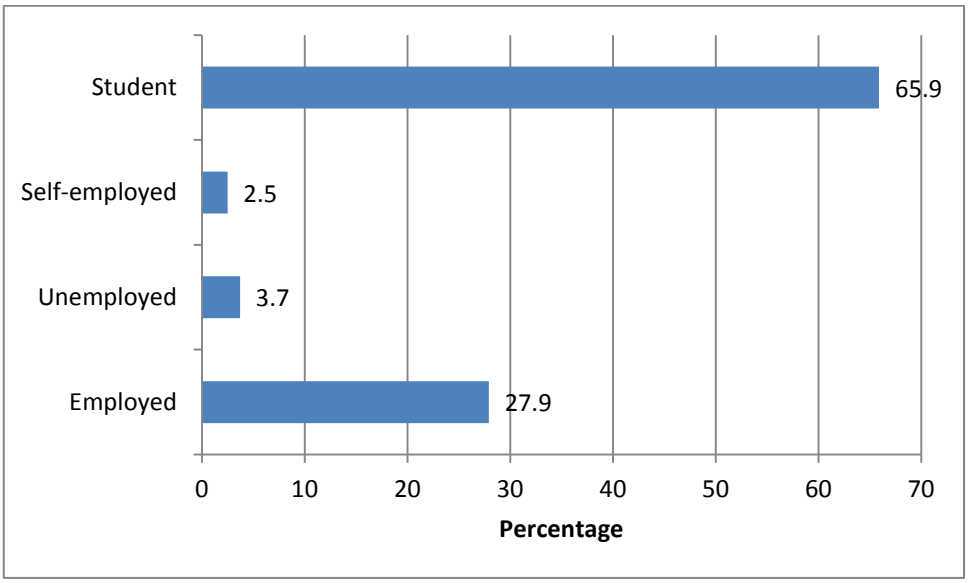

Figure 22: Employment Demographics of Respondents

7.1 Addressing the Hypothesis

The main objective of this study was to determine what factors affect users' online security awareness. From previous studies, one of the factors that were shown to influence online security awareness is employment status (Milne *et al*., 2009). Using the constructs of the Protection Motivation theory model, it will be shown whether or not this variable (employment status) influences online security awareness. The following hypothesis was derived:

H_{10}: Users' employment status does not influence their online security awareness

H_{1A}: Users' employment status influences their online security awareness

H_{10}: Users' employment status does not influence their online security awareness

H_{1A}: Users' employment status influences their online security awareness

7.2 How Analyses Were Performed

The results of this study show that employment status does affect online security awareness. This was to be expected as the literature states that most security training is done in the organizational dimension (Siponen, 2001). In order to address the hypotheses, cross-tabulations have been made and the chi-square test of independence was performed.

When the conditions for a chi-square were not met (e.g. >20% of cells with expected values <5), then Fisher's exact test was applied. In this chapter, the demographic variable that was tested was employment status.

7.3 User Awareness

The password protection question showed a difference in response rates between employed respondents and student respondents. As can be seen from the table below, employed respondents changed their passwords a great deal more often than all other respondents. This could, however, be due to these respondents having to change their passwords regularly with the systems they work with. The chi square shows that this result is significant as ($p<.0005$).

Table 6: Employment Status Effects Password Change Behaviour

	How often do you change the password on your computer?				
	Regularly	Sometimes	Seldom	Not at all	Total
Employed	26%	29%	29%	16%	100%
Unemployed	8%	0%	33%	58%	100%
Self-employed	0%	25%	38%	37%	100%
Students	7%	29%	38%	26%	100%

In terms of knowing what a phishing attack is, most respondents from all categories chose the wrong option. The correct option was option one, although the majority of respondents chose option three (Appendix F, question 20/Chapter 4, Pg. 42). The chi square test shows that significantly ($p<.0005$) more employed respondents knew what a phishing attack was than student respondents. Thirty nine per cent of employed respondents chose the correct option, 25% of unemployed respondents chose the correct option, 50% of self-employed respondents chose the correct option and 23% of student respondents chose the correct option. This shows that more employed and self-employed respondents know what a phishing attack is compared with students in the sample. Although the big concern here is that user awareness across all groups in terms of this question is still low.

7.4 Self-Efficacy

In terms of Protection Motivation theory, the results show that self-efficacy is the construct that was a determining factor in users' online security awareness for employment status. Similarly, employment status also showed differences in self-efficacy in the following questions.

- I know the difference between a virus and a Trojan (Appendix F, question 14)
- Is the firewall on your computer enabled? (Appendix F, question 18)
- Is your computer configured to be automatically updated? (Appendix F, question 19)
- I know what an email scam is and how to identify one (Appendix F, question 21)

The employed people in the sample answered in the affirmative to the above questions and thus had a higher self-efficacy than the student respondents.

In terms of knowing the difference between a virus and a Trojan, 74% of employed respondents answered "yes" to this question, 88% of self-employed respondents answered "yes", 58% of unemployed respondents answered "yes" and 46% of students answered "yes". Thus, for the question "I know the difference between a virus and a Trojan" the chi square test shows significantly ($p<.0005$) that more than expected employed people say 'yes'; students say 'no'. This indicates that employed people are more aware of the difference between a virus and a Trojan than students. In addition, more employed respondents knew what a firewall was than student respondents. Seven per cent of employed respondents stated that they did not know what a firewall was, 17% of unemployed respondents stated that they did not know what a firewall was and 26% of students stated that they did not know what a firewall was. In terms of having a firewall installed on their personal computers, 84% of employed respondents stated that a firewall was installed on their personal computers, 100% of self-employed respondents stated

that a firewall was installed on their personal computers, 75% of unemployed respondents stated that a firewall was installed on their personal computers and 57% of student respondents stated that a firewall was installed on their personal computers. The chi square shows that this result is significant as (p<.0005).

As can be seen when comparing these two questions, it seems that, if respondents knew the difference between a Virus and a Trojan, they also knew what a firewall was and had it installed on their personal computers. Similarly, for the question "Is your computer configured to be automatically updated?" 8% of employed respondents stated that they "don't know", 8% of unemployed respondents stated that they "don't know" and 24% of students stated that they "don't know". The chi square test shows that significantly (p<.0005) more employed respondents answered 'yes'; unemployed answered 'no'; students answered 'don't know'. This indicates that more employed people know what this is and recognize the importance of it.

For the question "I know what an email scam is and how to identify one", the chi square test indicates that significantly (p<.0005) more employed respondents were in agreement; students were either neutral or strongly disagreed. Seventy seven per cent of employed respondents agreed that they know what an e-mail scam is and how to identify one, 83% of unemployed respondents agreed that they know what an e-mail scam is and how to identify one, 100% of self-employed respondents agreed that they know what an e-mail scam is and how to identify one and 55% of student respondents agreed that they know what an e-mail scam is and how to identify one. This indicates that employed people are more confident than students about knowing what an e-mail scam is and identifying one and that their self-efficacy and awareness is much higher than the student respondents.

All groups seemed to believe that their computers have no value to hackers, the majority of respondents chose to either agree or neither agree nor disagree. Twenty three per cent of employed respondents were in agreement with this statement, 83% of unemployed respondents were in agreement with this statement, 25% of self-employed respondents were in agreement and 31% of student respondents were in agreement. This is a potentially dangerous mindset in the sense that these respondents are possibly not aware of how hackers can potentially use their information to commit fraud. The chi square shows significance as (p<.0005).

7.5 Perceived Severity

Perceived severity amongst students and unemployed respondents was found to be significantly (p<.0005) high. Fifty three per cent of unemployed respondents stated that they were concerned

about the state of online security in South Africa, and 58% of student respondents stated that they were concerned about the state of online security in South Africa. Forty per cent of employed respondents stated that they were concerned about the state of online security in South Africa and 38% of self-employed respondents stated that they were concerned about the state of online security in South Africa (Appendix F, question 28). This shows that perceived severity is highest amongst student respondents, followed by unemployed respondents. Self-efficacy was the highest amongst employed respondents, yet their perceived severity is the lowest. Students' self-efficacy was lower than employed people's, yet their perceived severity was high. A possible reason why students' perceived severity is high could be because this group is less educated about online security, thus being less aware of online security awareness.

7.6 Personal Vulnerability

Personal vulnerability was found to be low amongst all groups. Most respondents stated that they would be comfortable to use the Internet to conduct business, although results showed that employed, self-employed and unemployed respondents were more comfortable with conducting business online than student respondents. Seventy six per cent of employed respondents stated that they would be comfortable using the Internet to conduct business, 67% of unemployed respondents stated that they would be comfortable using the Internet to conduct business, 88% of self-employed respondents stated that they would be comfortable using the Internet to conduct business and 59% of student respondents stated that they would be comfortable using the Internet to conduct business (Appendix F, question 24). The chi square shows significance as ($p<.0005$).

Personal vulnerability was found to fluctuate in all categories in terms of credit card transactions in online environments. Self-employed respondents seemed to feel safe about placing their credit card details online. In terms of employed, the distribution of responses seemed to be equal in terms of all responses. For the unemployed respondents and the student respondents, the majority in these categories seemed to disagree, indicating that personal vulnerability was high in these cases. Seventy five per cent of self-employed respondents felt safe about placing their credit card details online. Thirty three per cent of employed respondents felt safe about placing their credit card details online, 8% of unemployed respondents felt safe about placing their credit card details online and 10% of student respondents felt safe about placing their credit card details online (Appendix F, question 25). A possible reason for the majority of students choosing "disagree" over the other options could be attributed to the fact that most students are unlikely to have a credit card or access to one. The chi square shows significance as ($p<.0005$)

In terms of the question “I have had my credit card details stolen and used in an online transaction”, the majority of respondents in all categories chose “no”. Ninety three per cent of employed respondents answered “no”, 100% of unemployed respondents answered “no”, 88% of self-employed respondents answered “no” and 94% of students answered “no” (Appendix F, question 26). The reason why the number is lower in terms of employed and self-employed respondents could be attributed to the fact that these respondents are likely to have credit cards and thus there is a higher chance of their being exposed to credit card fraud. The chi square shows significance as ($p<.0005$).

7.7 Response Effectiveness

The questions on response effectiveness, in terms of employment status, did not yield any significant results. Therefore, it can be deduced that this construct did not play a role in determining user security awareness in terms of race.

The diagram below shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy was shown to be high amongst all respondents, except the student respondents. This could be attributed to students not having the same level of knowledge of security as the other groups, thus a lower level of user awareness. Personal vulnerability was high amongst all groups, except the self-employed respondents. This could be because the self-employed respondents within the sample often placed their credit card details online and thus felt comfortable doing this. Perceived severity was neither high amongst student and unemployed respondents, and neither high nor low for employed and self-employed respondents. Student respondents perceived online threats as more dangerous than the other groups; the reason for this could be their lower awareness levels of online security. Response effectiveness was high amongst all groups, except self-employed respondents. This could be because these respondents do not believe that the controls in place to prevent online attacks or to keep their personal computers safe are adequate.

7.8 Discussion of PMT model on Employment Status

Figure 23, below, shows a holistic picture of the relationship between the variables and the constructs of the model. Self-efficacy was shown to be high amongst all respondents except the student respondents. This could be attributed to students not having the same level of knowledge of security as the other groups, thus a lower level of user awareness. Personal vulnerability was low amongst all groups. Perceived severity was low amongst all groups,

except unemployed respondents. More student respondents perceived online threats as dangerous, than the other groups; the reason for this could be the lower awareness levels of online security.

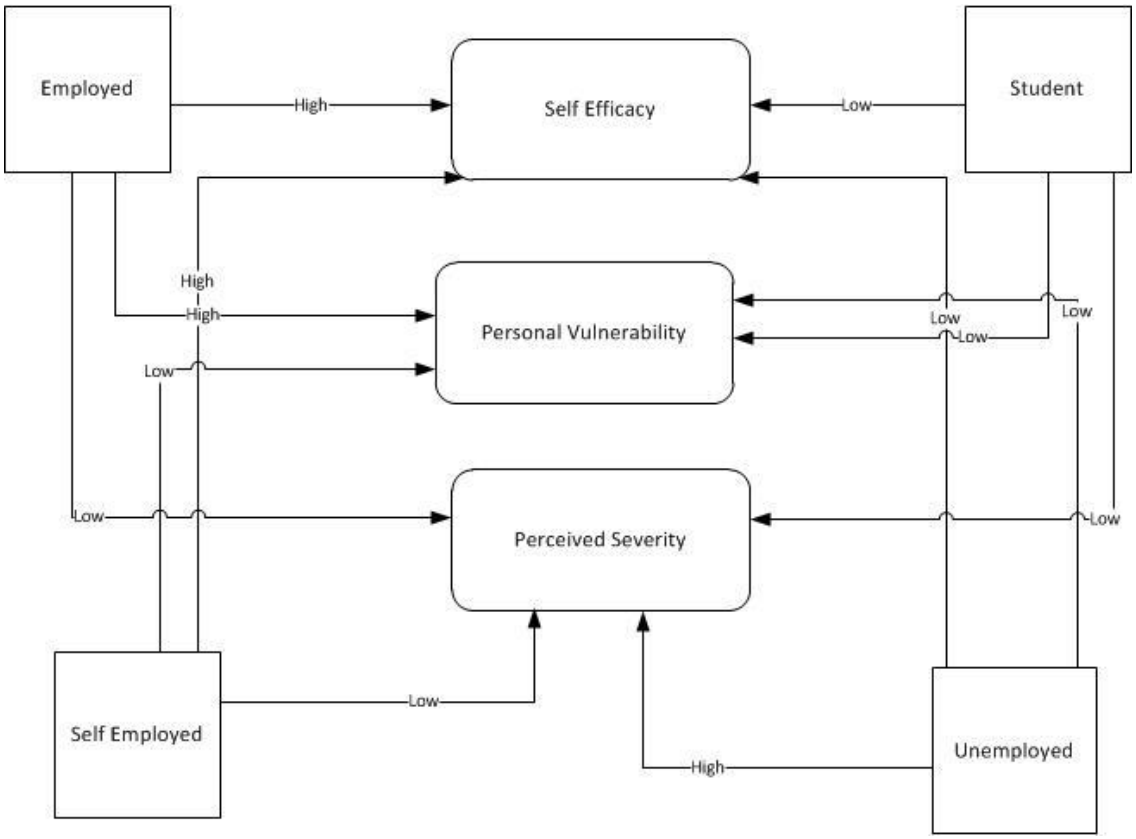

Figure 23: Protection Motivation Theory Constructs Effect Employment Status (Adapted)

7.9 Fears Regarding Online Banking

In terms of online banking, the vast majority of respondents did indeed have fears in this regard as very few respondents chose the option "I have no fears". Twelve per cent of employed respondents stated that they had no fears, 50% of self-employed respondents stated that they had no fears, 8% of unemployed respondents stated that they had no fears and 4% of students stated that they had no fears regarding online banking theft (To view all the options for this question refer to Appendix F, question 29). As can be seen from this result, a higher percentage of self-employed and employed respondents have no fears as opposed to student respondents. This could be due to the fact that these groups make more use of online banking than do student respondents and thus view it as relatively safer than students would. The chi square shows significance as ($p<.0005$).

7.10 Fears Regarding Online Purchasing

In terms of online purchasing fears, one of the significant ones were "Money will be 'lost' with no record of where it is and how it got there". Fifty six per cent of employed respondents stated that they feared this, 33% of unemployed respondents stated that they feared this, 25% of self-employed respondents stated that they feared this and 62% of student respondents stated that they feared this well (To view all the options for this question refer to Appendix F, question 30).

In addition, the vast majority of respondents did indeed have fears as very few respondents chose the option "I have no fears". Eleven per cent of employed respondents stated that they had no fears, 50% of self-employed respondents stated that they had no fears, 8% of unemployed respondents stated that they had no fears and 6% of students stated that they had no fears regarding online banking. As can be seen from this result, a higher percentage of self-employed and employed respondents have no fears compared with student respondents. This could be due to the fact that these groups make more use of online purchasing than student respondents and thus view it as relatively safer than the students would. Looking at the above two questions, there is a slight shift in terms of there being 3% of students who stated that they had no fears regarding online banking, while 6% stated that they had no fears regarding online purchases. Thus, more students fear online banking than they fear online purchasing. The chi square shows significance as ($p<.0005$).

7.11 Privacy on Social Networking Websites

In terms of privacy on social networking websites, it was found that significantly more employed respondents put work information online than the other respondents. In terms of "work information on social networking websites", 40% of employed respondents stated that they placed their work information on websites, 25% of unemployed respondents stated that they placed their work information on websites, 38% of self-employed respondents stated that they placed their work information on websites and 15% of students stated that they placed their work information on websites. The chi square shows significance as ($p<.0005$). The above result shows that all the other respondents (students, unemployed and self-employed) are more reluctant to put their work information on social networking websites than employed respondents.

In terms of the question on "relationship status on social networking websites", 60% of employed respondents stated that they would put their relationship status online, 33% of unemployed respondents stated that they would put their relationship status online, 75% of self-

employed respondents stated that they would put their relationship status online and 36% of students stated that they would put their relationship status online. The chi square shows significance as ($p<.0005$). This result shows that significantly fewer students are willing to place their relationship status online than any of other groups. Another theory is that both these groups use social networking websites for different purposes and thus the information they put up differs (To view all the options for this question refer to Appendix F, question 34).

7.12 Conclusion

The above results show that employment status does have an effect on online security awareness. Thus the null hypothesis was rejected. Results of the study show that the awareness levels of the student respondents are not as high as those of the employed respondents. This result was to be expected as the literature stated that most security training is done in the organizational dimension (Siponen, 2001).

The next chapter concludes this study and discusses how the model can be used in similar future studies in this area. Strategies to improve online user awareness of online security are also suggested.

Chapter 8: Discussion

8.1 Introduction

The purpose of this exploratory study is to determine the factors influencing online user security awareness using Protection Motivation Theory as a theoretical framework and to determine the current state of user awareness of online security. The context was specifically limited to young adults. The study aimed to find out whether race, language, community, gender and employment status influence online security awareness. To this end, the following hypotheses were formed and tested:

H_{10}: Users' race does not influence their online security awareness

H_{1A}: Users' race influences their online security awareness

H_{20}: Users' language does not influence their online security awareness

H_{2A}: Users' language influences their online security awareness

H_{210}: Users' level of English does not influence their online security awareness

H_{21A}: Users' level of English influences their online security awareness

H_{30}: Users' community does not influence their online security awareness

H_{3A}: Users' community influences their online security awareness

H_{40}: Users' gender does not influence their online security awareness

H_{4A}: Users' gender influences their online security awareness

H_{50}: Users' employment status does not influence their online security awareness

H_{5A}: Users' employment status influences their online security awareness

This chapter will discuss the framework and how it was used to interpret the results and draw conclusions. Thereafter, the hypotheses and research questions will be discussed. The chapter will conclude with limitations and further research suggestions for user awareness of online security.

8.2 Protection Motivation Theory and its application to this study

The above hypotheses assisted in providing answers to the research questions, which were:

- What factors influence online security awareness?
- What is the current state of user awareness of online security in South Africa?

This study used Protection Motivation theory to determine the hypotheses. Results showed that respondents' self-efficacy proved to be the determining factor in showing differences in users' awareness levels. The results indicate that constructs behaved differently, depending on the variables being tested. It was found that there were lower self-efficacy levels amongst certain groups of respondents who had a higher perceived severity. Thus, respondents who had less online security awareness feared online fraud more than respondents who were aware and more knowledgeable about online security. This was seen to be the case with gender, race and employment status. In addition, it was found that, generally, respondents who had a lower self-efficacy had higher personal vulnerability. This indicates that users with lower self-efficacy felt more vulnerable to online threats than users with higher self-efficacy.

When gender was tested, it showed that females had a low self-efficacy and their perceived severity and personal vulnerability was higher than male respondents. Thus, their lower self-efficacy (hence lower awareness) was a factor in making them feel more vulnerable regarding online security and had a higher level of concern about online security than the male respondents. There were marked differences when race, community and language were tested, as low/high self-efficacy did not affect users' perceived severity and personal vulnerability. Likewise, with regards to employment status, low/high self-efficacy did not affect users' perceived severity and personal vulnerability.

As described in chapters five to seven, the results show that gender, race, community, language and employment status affected online security awareness. In certain cases, self-efficacy of male respondents was higher than female respondents'. Self-efficacy also proved to be higher in Indian and White respondents than in African respondents.

Similarly, self-efficacy amongst English and Afrikaans speaking respondents was higher than among the Zulu and Xhosa speaking respondents. In addition, respondents from urban and semi-urban communities showed higher self-efficacy than respondents from rural areas. Employment status also influenced self-efficacy with results showing that employed people had a higher self-efficacy than student respondents. This study can be expanded to explore the reasons why these individuals have a higher self-efficacy and user awareness than the other groups and, in future, can possibly investigate how to educate groups that are not as aware as others.

On the whole, user awareness of online security was low (See Appendix G for all statistical analyses), as only 29% of respondents in the sample actually knew what a phishing attack was. To increase user awareness, user education strategies are recommended. This section is expanded in chapter nine.

8.3 Limitations

In terms of limitations emerging from the study, there were some weaknesses shown in the model itself. One of these was that the model did not account for social factors that could have influenced online security awareness. For example, the way an individual's friend/s behave/s could influence the way the individual would behave online. In addition, the model did not take into account environmental factors. For example, an individual could be less aware of online security because he/she has been less exposed to technology than others. This being stated, one of the aims of the study was to find if individuals with different demographic backgrounds had different awareness levels of online security, and the results showed that this was the case (i.e. individuals from rural areas where shown to have lower user awareness levels than individuals from urban areas). So, in this sense, this limitation of the model did not affect the results of the study.

Since this was an exploratory study, there was no need to show any representative population groups. The focus group of this study was young adults and the majority of respondents did fit within the relevant age range.

8.4 Further Research

This was largely an exploratory study to determine whether the issues needed further examination. The study could now be extended to incorporate larger areas of the country.

Other specific issues to explore might be the determination of reasons for the lower awareness and self-efficacy levels of females compared with males in terms of online security. In terms of social networking and privacy, results showed that more males than females place their phone numbers online. A study could be done to investigate the difference between online privacy perceptions between males and females using Protection Motivation Theory as a possible framework.

Other issues to explore might be the reasons why self-efficacy and awareness amongst Whites and Indians are higher than in the African population. Other factors that were found to influence online security awareness were language and community. This means that security awareness programs should target rural areas as well as users who do not speak English as a first language. The results showed that White respondents had lower response effectiveness than all the other groups. The reasons for this can be investigated further.

In terms of privacy on social networking websites, it was found that significantly fewer Indian respondents place their phone numbers on social networking websites than other race groups. Also, there were varying responses for the question about whether respondents placed their relationship status on social networking websites. This section could be expanded to investigate the differences between online privacy perceptions of all the race groups in South Africa.

In terms of language and community, there were varying responses in terms of what information different respondents placed online. These users also had varying fears regarding online purchasing. These can be further examined by performing a study regarding privacy and trust in online environments.

In terms of employment status, the varying self-efficacy and awareness levels can be further investigated. It was found that employed respondents were more likely than all the other groups to put up their relationship status. A comparative study can be done showing the differences in attitudes on privacy behaviour on social networking websites of employed individuals and students.

It was found that respondents feared online banking and online purchasing more than social networking. Specific fears regarding each of these have been discussed in chapters five to seven and an investigation can be done probing respondents about exactly what they fear regarding each of these (online purchasing, online banking and social networking) and possible reasons. Protection Motivation Theory can be used as a theoretical framework for this investigation.

The next chapter will focus on possible strategies to improve user awareness.

Chapter 9: Recommended Strategies to Improve User Awareness of Online Security

This chapter explores the strategies that are available to assist in raising user awareness of online security. Two of these are discussed in this chapter. These are:

- Using Web 2.0 to improve online security awareness
- Use of games to improve online security awareness

These two areas are recommended strategies for improving online security awareness. Section 2.6 in the literature chapter discusses strategies used by other countries to promote user awareness of online security. This chapter serves as an extension of this discussion.

9.1 User Awareness Strategy Using Web 2.0

Web 2.0 can be used as an avenue to increase online security awareness as it has worked well in the e-learning domain. Essentially, the drivers are the users due to the fact that the users can produce the content, individually or together (Hamburg & Hall, 2008). By using Web 2.0 tools (Wikis, social networking, bookmarking tools, blogs etc.) everyone can be a learner or a teacher as the barriers to conventional ICT-based training are removed (Hamburg & Hall, 2008). Web 2.0 makes a new level of communication possible which allows easier collaboration and sharing of information. It was found in a study that clear communication between members of a learning group is vital for success in training programmes, regardless of whether the communication was of a formal nature or informal (i.e. between colleagues). The tools and structures that aided the communication in this study were Web 2.0 tools. At the present time, it seems that younger people have greater knowledge with these technologies than older people. Due to this, it is assumed that the younger generation of users are more net-savvy, although a study about how much personal information people reveal online has shown that the student population are not overly concerned about privacy and security issues (Little, 2008). This is due to the fact that 90% of individuals in the study revealed their real names and pictures online (Little, 2008). It was thus concluded in this study that there is a need to develop awareness of personal and professional risks due to the huge number of online threats (Little, 2008).

Web 2.0 tools combine both visibility and interaction; both these elements work very well in terms of education. This can be seen by looking at the top 20 learning tools for 2009 (Hart, 2009). YouTube is one of the websites that offers a visual way of learning (by watching videos).

Teampedia, StudyStack and many others provide an interactive way of learning. Awareness campaigns using these tools can possibly be very strong as they appeal to the visibility element as well as the interactive one. In terms of information security, it makes sense to use these Web 2.0 tools to raise awareness as the user interacts with them in the appropriate spaces (i.e. the user interacts with them on a computer). There are currently many videos on YouTube that cover online security awareness, as well as various groups on Facebook that discuss it. A suggested strategy to help increase online security awareness using Web 2.0 can be derived simply by creating a group on Facebook and sharing videos and articles on it and inviting users to participate. The success of this group would be seen by the number of users that decide to join as well as seeing how much activity there would be in the group on a daily basis. An experimental version of this type of strategy was carried out in 2010, as can be seen by the screenshot below. The researcher posted up a video on a Web 2.0 e-learning website called Edmodo, and invited a group of students to a group called "Online Security". As can be seen in figure 24, below, after watching the video, students provided comments and created a discussion around the topic.

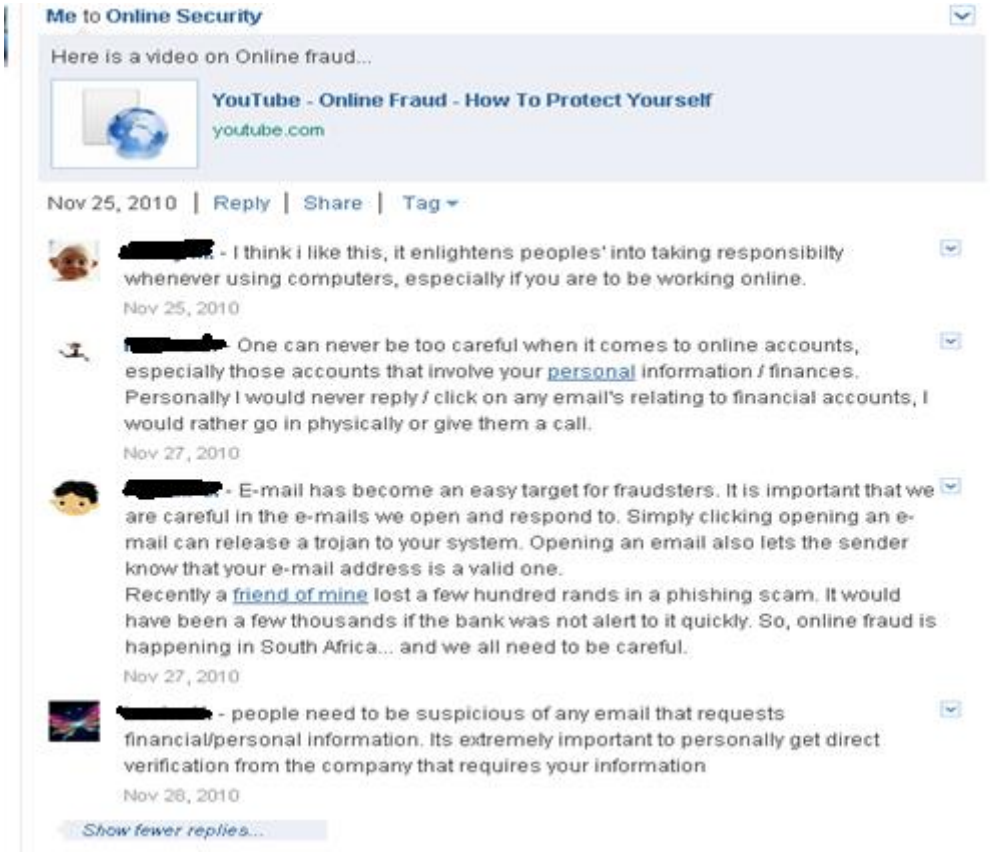

Figure 24: Suggested Online Awareness Strategy Using Web 2.0

A possible framework to use, to investigate whether a Web 2.0 platform would be adequate for user security awareness, is UTAUT.

The UTAUT model consists of 4 constructs: Performance expectancy, effort expectancy, social influence and facilitating conditions (Venkatesh, Morris, Davis, & Davis, 2003). It also deals with variables, such as age, gender, experience and voluntariness of use.

The elements that will be measured are listed below:

Performance expectancy (PE) is defined as the degree to which an individual believes that using new technology will help with improving working performance. It will be measured by the investigating the participant's perceptions of using different educational platforms in terms of the benefits, speed, usefulness and productivity.

Effort expectancy (EE) is the degree of ease associated with the use of the system and is measured by the perceptions of ease of using or understanding the operations of the different educational platforms.

Social influence (SI) refers to the degree to which an individual perceives how significant it is that others believe he or she should use the technology. In this case, it would be the degree of importance with which the respondents view each platform.

Facilitating condition (FC) refers to the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system and is measured by the perception of having the required resources or facilities knowledge to use each of the platforms (Venkatesh *et al*., 2003).

The above elements are shown in figure 25, below.

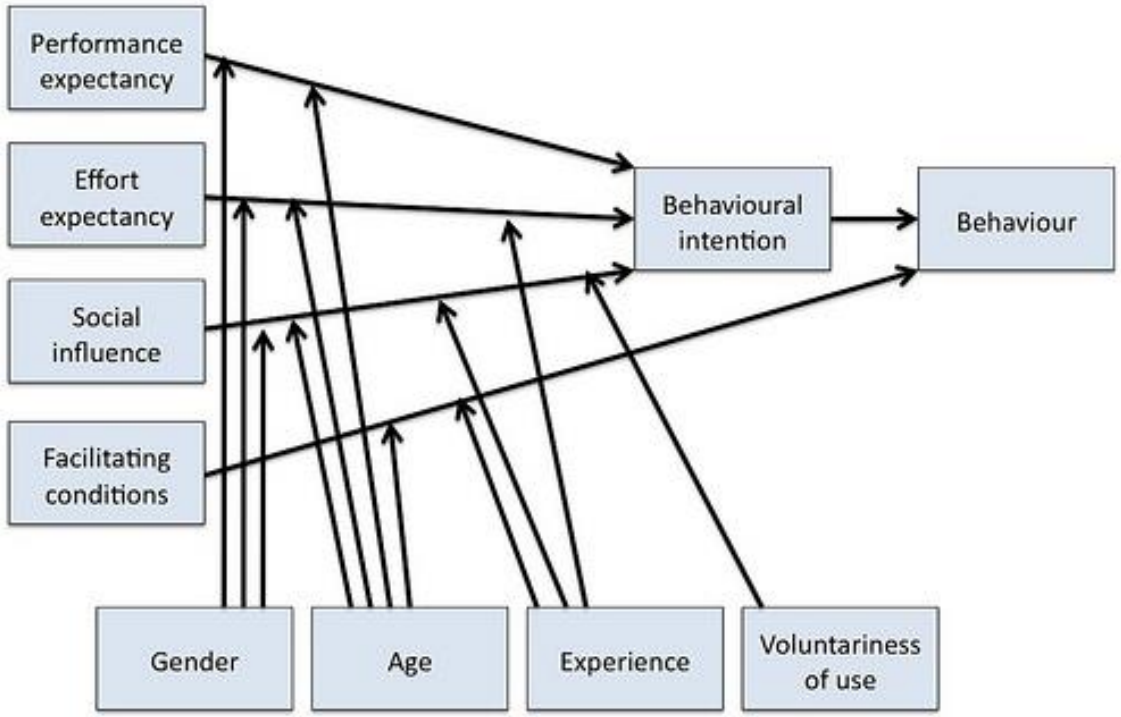

Figure 25: UTAUT (Flickr, 2009)

Since UTAUT deals with technology adoption and this proposed study deals with what platform users' prefer to adopt in terms of acquiring knowledge about online security, this model could be used. In addition constructs from this model can be combined with some of the constructs of Protection Motivation Theory to test user awareness of online security and to possibly find out what the best platform to learn about online security would be.

9.2 User Awareness Strategy Using Games

It is believed that users need to be properly educated about secure systems. In research done by Näckros (2002) a method of educating users is suggested (using a computer game to educate users). This suggests that for users to effectively use information systems, they have to be aware of security goals and threats before interacting with systems (Näckros, 2002). Some research studies show that scenario-based programs can be used to educate users about information security (Furnell, Gennatou & Dowland, 2000). Additional research has been carried out showing the use of computer games to educate individuals about security issues (Cone, Irvine, Thompson, & Nguyen, 2007; Monk 2011; Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007).

A possible strategy to develop a game like this, which could be successful in online security education, is to introduce one scenario and ask security-related questions regarding it. For example, Onguard.com has this type of game on its website. It starts off with a scenario: “Agent Smith has fallen asleep on a mission in Brazil, while details of his mission self-destructed in his briefcase. He is now under scrutiny by headquarters.” Thereafter, if you start the game “Mission laptop security”, the user answers a series of questions and, depending on how these are answered, they either fail to complete the mission or pass it (Onguard, 2012).

9.3 Conclusion

According to Kevin Mitnick (2002) “Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”

Further research regarding the above two strategies could possibly fill the gap in explaining how end-user education and awareness can be improved, thus strengthening the “weakest link” by educating users about online security in the appropriate platforms, with the appropriate tools.

Chapter 10: Conclusion

This chapter explores the research problem and its application of the research objectives. The problem statement as stated in chapter one was: The identification of factors that influences young adults' awareness of online security. To address the problem statement the following research questions were derived:

- What factors influence online security awareness?
- What is the current state of user awareness of online security in South Africa?

10.1 Answering the Research Questions

The main focus of the study was whether the respondents' demographic profiles have an impact on their online security awareness. As identified in the literature (section 2.7) these factors were gender, race, community, language and employment status. As described in chapters five to seven, the results showed that gender, race, community, language and employment status affected online security awareness. This provided answers to the first research question.

As mentioned in Chapter 8 Protection Motivation Theory was used as the theoretical framework to guide this study. Results disclosed that respondents' self-efficacy was the determining factor in showing differences in users' awareness levels. This showed that there is a direct link between user awareness of online security and a user's self-efficacy as shown by figure 26, below.

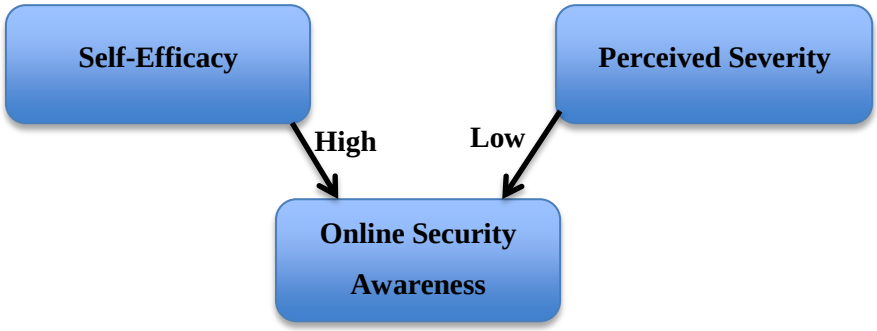

Figure 26: Self-Efficacy and Perceived Severity Influence Online Security Awareness

The results also indicated that constructs of the model behaved differently, depending on which variables were being tested. It was found that there were lower self-efficacy levels amongst certain groups of respondents who had a higher perceived severity. Thus, respondents who had less online security awareness feared online fraud more than respondents who were aware and more knowledgeable about online security.

The second research question was partially answered as results showed that awareness levels of respondents were varied. In terms of this exploratory study user awareness of online security was low. To find out what the user awareness levels on online security would be in the South African context, further research will have to be pursued.

10.2 Conclusion

This study has uncovered factors that affect online security awareness through the application of Protection Motivation Theory (i.e. a health belief model). The results of this study can help organizations and practitioners involved in implementing online security awareness training programmes to take into account the different factors that influence awareness levels and thus possibly improve the design of security awareness programmes.

This study set out to find the factors that influence online user security awareness. As described in chapters 5 to 7, the results show that gender, race, community, language and employment status affect online security awareness. This was largely an exploratory study and could now be extended to incorporate larger areas of the country (the other provinces) with a marginally modified questionnaire to further investigate the issues raised in this study.

Bibliography

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Privacy Enhancing Technologies. 1-22. Proceedings of 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK.

Al Islam, A., & Sabrina, T. (2009). Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble. ICCIT '09 (pp. 603, 608). Bangladesh: Computers and Information Technology.

Allen, M. (2006). Social Engineering: A Means to violate a computer system. Retrieved 2012 21-May from http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529

Alshboul, A. (2010). Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. Communications of the IBIMA, 1-9.

Apau, M. (2011). Best Practices on Social networking Websites (SNS). Retrieved February 10, 2013, from http://www.cybersecurity.my/data/content_files/11/918.pdf

Banks, M. S., Onita, C. G., & Meservy, T. O. (2010). Risky Behaviour in Online Social Media: Protection Motivation and Social Influence. AMCIS 2010 Proceedings.

Barnard, L., & Wesson , J. L. (2003). Usability issues for E-commerce in South Africa: an Empirical Investigation. Proceedings of SAICSIT.

Belanger, F., Carter, L. (2008). Trust and Risk in e-Government Adoption", Journal of Strategic Information Systems. 17(2), 1-15.

Bhutta, C. B. (2012). Not by the Book: Facebook as a Sampling Frame. Sociological Methods & Research, 41(1), 57-88.

Boon Yuen, N.G., Kankanhalli, A., & Xu, Y. (2009). Studying Users' Computer Security Behavior. Decision Support Systems, 46(4), 815-825.

Brush, A. B. (2006). IT@Home: Often Best Left to Professionals. Position Paper for CHI 2006 Workshop: Microsoft Research.

Casalo, L. V., Flavian, C., Guinaliu, M. (2007). The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking. Online Information Review, 31(5), 583-603.

Centre for Innovation in Mathematics teaching. (n.d.). Retrieved April 11, 2013, from http://www.cimt.plymouth.ac.uk/projects/mepres/alevel/fstats_ch5.pdf

Chawki, M. (2009). Nigeria Tackles Advance Fee Fraud. Journal of Information, Law and Technology 1. Retrieved 5 April 2013 from: http://go.warwick.ac.uk/jilt/2009_1/chawki

Chenoweth, T. M. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. 42nd Hawaii International Conference on System Sciences, 1-10.

Christensen, B. (2006). Nigerian Scams - 419 Scam Information. Retrieved 2012 20-May from Hoax Slayer: http://www.hoax-slayer.com/nigerian-scams.html

Cisco Systems. (n.d.). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved 2012 20-June from Cisco: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Cisco Systems White Paper. (2006). Understanding Remote Worker Security: A Survey of User Awareness Vs Behaviour. Retrieved 2012 20-March from: http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf

Club Norton. (2013). Don't Get Trapped in Phishing Scams. Retrieved February 13, 2013, from Norton by Symantec: http://securityresponse.symantec.com/en/uk/norton/clubsymantec/library/article.jsp?aid=cs_phishing_scams

Collins Dictionaries. 2013. Definition of "Semi urban". Retrieved 4th November 2013 from: http://www.collinsdictionary.com/dictionary/english/semiurban

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen,T. D. (2007) . A video game for cyber security training and awareness. Computers & Security 26, 63-72.

CyberSource. (2010). Sixth Annual UK Online Fraud Report. Retrieved 2011 20-June from http://awoof.com.cp-5.webhostbox.net/unibook/uk_online_fraud_report_2010%2520web.pdf

Das, E. (2001). How fear appeals work: motivational biases in the processing of fear-arousing health communications. Retrieved 2011 11-June from http://www.researchgate.net/publication/27685847_How_fear_appeals_work__motivational_biases_in_the_processing_of_fear-arousing_health_communications

Davis, F. (1989). Perceived usefulness, perceived easy of use, and user acceptance of information technology. MIS Quarterly, 319-340.

Dell Sonicwall. (2012). Phishing: When email is the enemy. Retrieved February 13, 2013, from http://i.dell.com/sites/doccontent/business/solutions/whitepapers/en/Documents/phishing-when-email-is-the-enemy.pdf

Demographic Yearbook. (2005). Definition of "Urban". Retrieved 4th November 2013 from: http://unstats.un.org/unsd/demographic/sconcerns/densurb/Defintion_of%20Urban.pdf

Dillard, J. P., & Anderson, J. W. (2004). The role of fear in persuasion. Psychology & Marketing, 21(11), 909–926.

Dillard, J. P., Plotnick, C. A., Godbold, L. C., & Freimuth, F. S. (1996). The multiple affective outcomes of AIDS PSAs. Communication Research, 23(1), 44-72.

Dinev, T., and P. Hart. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research. 1 (17), pp. 61-80

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. AMCIS 2007 Proceedings.

Ernst & Young. (2008). Fighting to close the gap: Global Information Security Survey. Retrieved 2013 29-January from: http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey__Fighting_to_close_the_gap.pdf

Flickr. (2009). Unified theory of acceptance and use of technology. Retrieved 12 April 2013 from: http://www.flickr.com/photos/david_jones/3350330093/

Fogel, J., & Nehmad, E. (2009). "Internet Social Network Communities: Risk taking, Trust, and Privacy Concerns, Computer in Human Behaviour, vol. 25, pp. 152-160.

Furnell S.M., Gennatou M., and Dowland P.S. 2000. Promoting security awareness and training within small organisations. Paper presented at the 1st Australian Information Security Management Workshop, University of Deakin, Australia.

Furnall, S. (2008). End-user security culture: A lesson that will never be learnt? Computer Fraud & Security, 2008(4), 6-9.

Gao, W., &. Kim, J. (2007). Robbing the cradle is like taking candy from a baby. Annual Conference of the Security Policy Institute . Amsterdam.

Gartner. (2009). The War on Phishing Is Far from Over. Retrieved May 28, 2011, from Gartner: http://www.gartner.com/DisplayDocument?id=927921

Gil, P. (2012). What Is an 'Email Spoof'? Is It a Type of Phishing Attack? Retrieved 2012 2-June from About.com: http://netforbeginners.about.com/od/p/f/email-spoof-phishing-attack.htm

Goertzel, K. M. (2011 2-May). Information Assurance Tools Report: Firewalls. Retrieved 2012 13-May from http://iac.dtic.mil/csiac/download/firewalls.pdf

Grindley, E., Zizzi, S., & Nasypany, A. (2008 16-October). Use of Protection Motivation Theory, Affect, and Barriers to Understand and Predict Adherence to Outpatient Rehabilitation. Journal of the American Physical Therapy association and Royal Dutch Society for Physical Therapy, 88(12), 1529-1540.

Grobler, M., Van Vuuren, J., Jansen, J., & Zaaiman, J. (2012). The Influence of Cyber Security Levels of South African Citizens on National Security. From CSIR: http://researchspace.csir.co.za/dspace/bitstream/10204/5832/1/Grobler_2012.pdf

Hall, D. (2012). Cybersecurity Risks,Scams, Frauds, Crimes - 2012. Retrieved February 12, 2013, from http://www.vcsi.org/files/Cybersecurity%20Risks.pdf

Hamburg, L. & Hall, T. (2008). Informal learning and the use of Web 2.0: within SME training strategies. Retrieved 14 January 2011 from: http://www.elearningeuropa.info/en/article/Informal-learning-and-the-use-of-Web-2.0-within-SME-training-strategies

Hampton, K., Goulet, L., Rainie, L., & Purcell, K. (2011). Social Networking Sites and Our Lives: How People's Trust, Personal Relationships, and Civic and Political Involvement Are Connected to Their Use of Social Networking Sites and Other Technologies. Retrieved 2012

11-June from:
http://beta.images.theglobeandmail.com/archive/01287/Pew_Study__Social__1287603a.pdf

Hartley, D., & Abrams, R. (2009, August). Keeping Secrets: Good Password Practice. Retrieved April 29, 2013, from: http://www.eset.com/us/resources/white-papers/EsetWP-KeepingSecrets20090814.pdf

Hart, J. (2009). Top 100 Tools for Learning. Retrieved 21 June 2011 from: http://www.slideshare.net/janehart/top-100-tools-for-learning-2009-2509241

Hashim, A., Ghani, E., & Said, J. (2009, 12 31). Does Consumers' Demographic Profile Influence: An Examination Using Fishbein's Theory. Canadian Social Science, 5(6), 19-31.

Herath T, & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems, [18] 2, 106 -125.

Heyman, K. (2007). New Attack Tricks Antivirus Software. IEEE Computer Society (pp. 18-20). IEEE.

IBM. (2012). Top Cyber Threats in 2011. Retrieved 14 June 2012 from: http://www-03.ibm.com/press/us/en/photo/36882.wss

Internet Crime Complaint Centre. (2011). 2011 Internet Crime Report. Retrieved April 24, 2012, from http://www.ic3.gov/media/annualreport/2011_ic3report.pdf

Internet World and Population stats. (2013). Internet World and population Stats. Retrieved 21 April 2013 from Internet World and population Stats: http://www.Internetworldstats.com/stats.htm

Jagatic, T.,N. Johnson, M. Jakobsson and F. Menczer. (2007). Social Phishing. Communications of the ACM. 50(10), 94-100.

Jahankhani. (2009). The Behaviour and Perceptions of Online Consumers: Risk, Risk Perception and Trust. International Journal of Information Science and Management, 7(1), 79-90.

Jakobsson, M., & Srikwan, S. (2008). Using Cartoons to Teach Internet Security. Cryptologia. 32, pp. 137-154. Taylor & Francis.

Javelin Strategy and Research. (2008). Retrieved November 11, 2010, from Javelin Strategy and Research,: www.javelinstrategy.com/2009/03/17/survey-finds-retailers-missed-out-on-21-billion-in-sales-in-2008-due-to-online-shopping-fears

Jayanti, R. K., & Burns, A. C. (1998). The Antecedents of Preventive Health Care Behavior: An Empirical Study. Academy of Marketing Science Journal, 26(1), 6-15.

Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviours: An Empirical Study. MIS Quarterly.

Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviours: An Empirical Study. MIS Quarterly, 34(3), 549-566.

Kayle, A. (2011). Social networks threaten privacy. Retrieved June 14, 2012, from IT web: http://www.itweb.co.za/index.php?option=com_content&task=view&id=42854&tmpl=component&print=1

Keller, P. A. (1999). Converting the Unconverted: The Effect of Inclination and Opportunity to. Journal of Applied Psychology, 84(3), 403-415.

Kim, D, J., Ferrin, D L., Rao, H, R. (2008). A Trust-based Consumer Decision-making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. Decision Support Systems. 44, 544-564.

Kline, K. N., & Mattson, M. (2000). Breast self-examination pamphlets: A content analysis grounded in fear appeal research. Health Communication, 1-21.

Kumaraguru, P., Y. Rhee, A. Acquisti, L. Cranor, J. Hong and E. Nunge. (2007) Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *Proceedings of the 2007 Computer Human Interaction*, CHI 2007.

Labuschagne, WA and Eloff, M. (2012). Towards an automated security awareness system in a virtualized environment. *Proceedings of the 11th European Conference on Information Warfare and Security*, The Institute Ecole Supérieure en Informatique, Electronique et Automatique, Laval, France, 5-6 July 2012.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting Personal Responsibility for. Communication of the ACM vol. 51, no. 3, 71-76.

Lee, Y., & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. European Journal of Information, 177-187.

Little, J. (2008). The Net Generation: Balancing Freedom and Security in their Digital World. Securing the eCampus 2.0 Conference. Darthmouth College. Retrieved 4 March 2012 from: http://www.ists.dartmouth.edu/docs/ecampus/2008/Presentation_JulieLittle2008.pdf

Lo, J. (2012). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. AMCIS 2010 Proceedings.

Mailfrontier. (2004). Surefire Tips to protect yourself from Phishing. Retrieved March 13, 2012, from http://www.mailfrontier.com/docs/SurefirePhishingTips.pdf

Mcconell International. (n.d.). Retrieved April 2, 2010, from Cyber Security Laws: http://www.mcconnellinternational.com/services/Updatedlaws.htm

Milne, G., Labrecque, L., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. The Journal of Consumer Affairs, 43(3), 380-388.

Mitnick, K. (2002). The weakest link. If only computer security didn't involve people. Retrieved 25 April from: http://www.economist.com/node/1389553

Monk, T. P. (2011). Educating users about information security by means of game play. Retrieved June 12, 2012, from: http://dspace.nmmu.ac.za:8080/jspui/bitstream/10948/1493/1/Thomas%20Philippus%20Monk.pdf

Näckros K. N.D. (2002). Empowering Users to become Effective Information Security and Privacy Managers in the Digital world through Computer Games Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, Sweden. Retrieved 5 January 2011 from: http://smg.media.mit.edu/cscw2002-privacy/submissions/kjell.pdf

National Youth Policy (2009). National Youth Policy 2009- 2014. Retrieved 14 May 2012 from: http://www.thepresidency.gov.za/MediaLib/Downloads/Home/Publications/YouthPublications/NationalYouthPolicyPDF/NYP.pdf

Nielson, J. (2004). User Education is not the answer to Security Problems. Retrieved from http://www.useit.com/alertbox/20041025.html

Ong, C. E. (2003). E-Commerce Trust in Redress Mechanism Cross Border Issues. Petaling Jaya, Malaysia: Monash University.

OnGuard Online. (2012). Retrieved June 1, 2011, from http://onguardonline.gov/index.html

Pahnile S, Siponen, N., & Mahmood, A. (2007). Which factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. PACIS 2007 Proceedings.

Pahnile, S., Siponen, N., & Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. In Innovations in Information Technology (Ed.), Innovations in Information Technology, (pp. 1-5). Dubai.

Pavlou, P.A., 2003. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Int. J. Electron. Commerce, 7: 69-103.

Peltier, T. R. (2002). Information Security Policies; procedures, and standards: guidelines for effective information security. Boca Raton, FL: Auerbach publications.

Pfleeger, C. P., & Pfleeger, S, L. (2003). Security in Computing 3rd Edition (3 ed.). New Jersey: Prentice Hall.

Poston, R. S., & Stafford, T. (2010). Online Security Threats and User Intentions: A Model of Computer Protection Motivation. IEEE Computer, 43(1), 58-64.

Pretorius, P. (2009 29-August). Bank Fraud Over Internet. Retrieved 2012 21-May from Pieters Blog: http://www.pietpetoors.com/blog/bank-fraud-over-the-Internet/

Price, B. (2010, 05 04). Facebook Privacy Concerns Don't Stop Risky Behavior on Social Networks. Retrieved May 22, 2012, from eWeek: http://www.eweek.com/c/a/Security/Facebook-Privacy-Concerns-Dont-Stop-Risky-Behavior-on-Social-Networks-884390/

Pring, C. (2012). The Social Skinny. Retrieved June 19, 2012, from http://thesocialskinny.com/100-social-media-statistics-for-2012/

Raynes-Goldie, K. (2010). Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook. Retrieved 11 February 2011 from: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Rogers. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Social Psychophysiology.

Rogers, E. M. (1995). Diffusion of innovations (4th ed.). New York: Free Press

Rogers, R. W., & Prentice-Dunn, S. (1997). Handbook of health behavior research. Vol. 1: Determinants of health behavior: Personal and social (Gochman G, ed.). New York: Plenum.

Roser, C., & Thompson, M. (1995). Fear Appeals and the Formation of Active Publics. Journal of Communication, 45(1), 103+.

RSA. (2012). The Year in Phising. Retrieved April 30, 2012, from http://www.rsa.com/solutions/consumer_authentication/intelreport/11635_Online_Fraud_report_0112.pdf

Ruiter, R., Abraham, C., & Kok, G. (2001). Scary warnings and rational precautions: A review of the psychology of fear appeals. Psychology and Health, 16(6), 613-630.

Salleh, Hussein, R., Mohamed, N., Abdul Karim, N. S., Ahlan, A. R., & Aditiawarman, U. (2012). Examining Information Disclosure Behavior on Social Networks Using Protection Motivation Theory, Trust and Risk. Journal of Internet Social Networking & Virtual Communities, 2012 (2012), 1-11.

Secure enterprise 2.0. (2009). Top Web 2.0 Security Threats. Retrieved 2012 11-June from http://webcache.googleusercontent.com/search?q=cache:-u4cBhI5-7UJ:webhack.tistory.com/attachment/cfile21.uf%40156D390F49A8FF10A10D3A.pdf+Secure+enterprise+2.0+2009+top+web+2.0+security+threats&cd=5&hl=en&ct=clnk&gl=za

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. CHI 2010. Atlanta: ACM.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge. (2007) . Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. ACM International Conference Proceeding Series, Vol. 229, 88-99.

Siponen, M. (2001). Five dimensions of information security awareness. Computers and Society, 11(5), 24-29.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer, 43(2), 64-71.

Smyth, S. M., & Carleton, R. (2011). Measuring the extent of cyber-fraud: a discussion paper on potential methods and data sources. Retrieved 5 April 2013 from: http://publications.gc.ca/collections/collection_2011/sp-ps/PS14-4-2011-eng.pdf

Solari, C. (2009). Security in a Web 2.0+ World: A Standards-Based Approach. West Sussex, UK: John Wiley and Sons.

Sophos. (2007, August 14). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Retrieved June 15, 2012, from Sophos: http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx

SouthAfrica.info. (2013). SouthAfrica.info. Retrieved February 28, 2013, from http://www.southafrica.info/about/people/language.htm#.UaIGUqKj3j4

Stafford, T. and Poston, R. S. (2010). Online Security Threats and User Intentions: A Model of Computer Protection Motivation. IEEE Computer, 43(1), 58-64.

Stephenson, M., & Witte, K. (1998). Fear, threat, and perceptions of efficacy from frightening skin cancer messages. Public Health Reviews, 147-174.

Springer. (2013). Fischer's exact test. Retrieved 14 April 2013 from: http://www.springerreference.com/docs/html/chapterdbid/305931.html

StaySmartOnline 2010. StaySmartOnline . Retrieved 20 July 2012 from: http://www.staysmartonline.gov.au/

Stephanou, A. T., & Dagada, R. (2008). The impact of information security awareness training on information security behavior: The case for further research. Proceedings of InformationSecurity South Africa (ISSA), Johannesburg, South Africa.

Symantec. (2012 07-June). Symantec Intelligence – May 2012: Malware Moves Outside of the Windows World. Retrieved 2012 20-June from Symantec:

http://www.symantec.com/connect/blogs/symantec-intelligence-may-2012-malware-moves-outside-windows-world

TRU Research. (2010, April 20). Generation Y Online Security Survey. Retrieved July 20, 2011, from http://www.rsa.com/maintainmyprivacy/Gen_Y_Int_Sec_Surv_Res_TRU_RSA.pdf

Turbotodd. (2012). Advancing Security Intelligence to Help Organizations Combat Increasing Threats. Retrieved 2012 20-June from Turbotodd: http://turbotodd.wordpress.com/2012/02/22/

US-CERT. (2005). Spyware. Retrieved 2012 10-June from http://www.us-cert.gov/sites/default/files/publications/spywarehome_0905.pdf

Van Niekerk, J., & Van Greunen, D. (2006). Is user education the answer to online security problems? User Education in Online Security. Information Technology in Tertiary Education, (pp. 18-20). Pretoria.

Van Niekerk, J. F., & Von Solms, R. (2006). Corporate information security education: Is outcomes based education the solution? *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France*.

Van Niekerk, J., & Von Solms, R. (2007). A web-based portal for information security education. Retrieved 2011 5-September from http://www.academia.edu/1951998/A_web-based_portal_for_information_security_education

Von Solms, B. (2011, 6 June). The crime scene of the 21st century. Retrieved June 2, 2012, from Leadership Online: http://www.leadershiponline.co.za/articles/other/1356-cyber-crime

Venkatesh, V., Morris, M.G., Davis, F.D., and Davis, G.B. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27 (3), 425-478.

Wolf Pack. (2013). 2012/2013 The South African Cyber Threat Barometer. Retrieved 14 May 2013 from: http://cyanre.co.za/cyber-threat-barometer.pdf

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security (fourth ed). *Thomson Course Technology.*

Wilson, D. (2004). Partner reduction and the prevention of HIV/AIDS. British Medical Journal, 328, 848-849.

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process. Communication Monographs, 59, 329-349.

Witte, K., Berkowitz, J., Cameron, K., & Lillie, J. (1998). Preventing the spread of genital warts: Using fear appeals to promote self-protective behaviors. Health Education & Behavior, 25(5), 571-585.

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.

Worldnetweb. 2013. Definition of "Rural". Retrieved 4th November 2013 from: http://wordnetweb.princeton.edu/perl/webwn?s=rural area

Young, A.L., Quan-Haase, A. (2009). Information Revelation and Internet Privacy Concernson Social Network Sites: A Case Study of Facebook. Proceedings of the 4th International Conference on Communities and Technologies, pp. 265-274. Retrieved 12 June 2012 from: http://dl.acm.org/citation.cfm?id=1556499

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk Benefit Appraisal Approach. Journal of Broadcasting & Electronic Media, 49, 86-110.

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviour among Young Adolescents. The Journal of Consumer Affairs, 43(3), 389-418.

Appendix A – Letter From Statistician

Gill Hendry B.Sc. (Hons), M.Sc. (Wits)
Mathematical and Statistical Services

Cell: 083 300 9896
email : hendryfam@telkomsa.net

13 May 2013

To whom it may concern

Please be advised that Zahra Bulbulia (student number 202516620) who is presently studying for an MCom (IS&T) has consulted me regarding the statistical analysis of her data.

Yours sincerely

Gill Hendry (Mrs)

Appendix B – Letter from Language Editor

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

LETTER OF CONFIRMATION – EDITING

June, 2013

Zahra Bulbulia

This is to confirm that the Masters dissertation of Zahra Bulbulia has been edited by me. This process is aimed at eliminating grammatical errors and errors of expression only. In no way was the content or structure of the dissertation addressed.

I did not see the dissertation again after final changes were made. However, I am satisfied that the editing was thoroughly done and that the student, in consultation with her supervisor, is able to rectify the errors that were identified.

B Soane (Dr)

Appendix C – Ethical Clearance Letter

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

2 July 2013

Ms Zahra Bulbulia 202516620
School of Management, IT & Governance
Westville Campus

Dear Ms Bulbulia

Protocol reference number: HSS/1235/011M
New project title: Factors that influence young adults' online security awareness

Approval and change of dissertation title

I wish to confirm that ethical clearance has been granted full approval for the above mentioned project:

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/Methods 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 school/department for a period of 5 years

Best wishes for the successful completion of your research protocol.

Yours faithfully

.....

Dr Shenuka Singh (Deputy Chair)
Humanities & Social Science Research Ethics Committee

cc Supervisor: Professor Manoj Maharaj
cc Academic leader: Professor B McArthur
cc School Administrator: Ms A Pearce

Humanities & Social Sc Research Ethics Committee
Professor S Collings (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban, 4000, South Africa
Telephone: +27 (0)31 260 3587/8350/4557 **Facsimile:** +27 (0)31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za

Appendix D – Turnitin Report

preferences

turnitin Originality Report

Processed on: 06-Nov-2013 2:32 PM CAT
ID: 370227809
Word Count: 31132
Submitted: 1

Final
By Zahra Bulbulia

Similarity Index 9%

Similarity by Source
Internet Sources: 5%
Publications: 4%
Student Papers: 4%

Document Viewer

include quoted include bibliography exclude small matches

mode: show highest matches together

Abstract The information age presents many fears of security threats to the integrity, confidentiality

and availability of information systems and their associated data. Despite the 92

advent of countermeasures, such as antivirus software, firewalls, security patches and password change control systems, amongst others, to protect information systems, online attacks have increased significantly. Vast sums are spent by both the government and business sectors on deflecting mechanisms and on cleaning up after online attacks, which are becoming increasingly sophisticated and diverse (Gartner, 2009). The aim of this exploratory study

is to determine the factors that influence online security and the current state of 54

user awareness in South Africa amongst young adults. To guide this approach, Protection Motivation Theory (Rogers, 1983) was used as a conceptual framework. Significant findings of the study are that gender, race, community, language and employment status affect user awareness of online security. In terms of user awareness of online security it was found that most of the respondents were aware of the dangers of online threats and concerned about the state of online security in South Africa. The reasons why gender, race, community, language and employment status affect online security awareness can be explored in further research. i List of Acronyms IS - Information Systems IT - Information Technology PMT - Protection Motivation Theory SNS - Social Networking Websites UTAUT -

Unified Theory of Acceptance and Use of Technology ii Chapter 1: Introduction 81

The September 11 attacks against the United States have prompted many new concerns for physical security and information security. With the advent of the Information age, also known as the computer age, there are increasing fears of security threats to the integrity, confidentiality and availability of information systems. Actions have been taken and measures put in place, however, to prevent these threats from materializing. These include antivirus software, firewalls, password change control systems and security patches, as well as a variety of techniques that are offered to protect information systems (Workman, 2008). It has been found in research done by Cisco Systems (Cisco Systems White Paper, 2006) regarding online security awareness in the workplace, that isolated end-users seem to possess security awareness but their practices are not consistent with this as they still indulge in risky online behaviour. In this research study, participants believed that they were working securely. What is important here is that, although

end-users understand the importance of security, they do not put it 9

into practice. This shows that although users may be aware, they are not properly educated about security threats. So, while users may be aware of security threats, they may not understand the implications of their actions online. Some research states that users are not IT professionals and thus have different priorities (Brush, 2006).

While end-users might be aware of the importance of security, this knowledge is not enough to ensure safer habits 9

by them.

Just because users think or say they are aware does not mean they know how to be safe. An end-user who is poorly informed about security best practices, yet believes he is working safely, can actually intensify security risks for an organisation. It is assumed that the 9

younger generation of users are more net-savvy, although a study about how much personal information people reveal online has shown that the student population is not overly concerned about privacy and security issues (Little, 2008). This is due to the fact that 90% of individuals in the study revealed their real names and pictures online (Little, 2008). It was thus concluded in this study that there is a need to develop awareness of personal and professional risks due to the large number of online threats (Little, 2008). According to a recent survey carried out in South Africa,

1 < 1% match (Internet from 15-May-2012) http://www.thefullwiki.org

2 < 1% match (Internet from 11-Sep-2013) http://www.cmr-journal.org

3 < 1% match (publications) Furnell, S., "End-user security culture: A lesson that will never be learnt?", Computer Fraud & Security, 200804

4 < 1% match (Internet from 23-Sep-2011) http://www.austen-security.co.za

5 < 1% match (publications) Day, Marcus Devieux, Jessy G. Reid, Sand, "Risk behaviours and healthcare needs of homeless drug users in Saint Lucia and Trinidad.", ABNF Journal, Nov-Dec 2004 Issue

6 < 1% match (Internet from 22-Apr-2009) http://www.pacis-net.org

7 < 1% match (publications) Ng, B.Y., "Studying users' computer security behavior: A health belief perspective", Decision Support Systems, 200903

8 < 1% match (Internet from 18-Apr-2012) http://www.aabri.com

9 < 1% match (Internet from 27-Feb-2007) http://www.cisco.biz

10 < 1% match (student papers from 05-Dec-2012) Submitted to University of Iowa

11 < 1% match (student papers from 02-Apr-2013) Submitted to Northcentral

12 < 1% match (student papers from 12-Mar-2012) Submitted to EDMC

Appendix E – Publications

Peer Reviewed Journal

Paper accepted for the Journal of Information Warfare, Volume 12 (1), Pages 83-96, April, 30, 2013. http://www.Jinfowar.com

The abstract of this paper is shown below

Factors that influence young adults' online security awareness in the Durban region of South Africa

Z Bulbulia and M Maharaj
College of Management, IT and Governance
University of KwaZulu Natal,
e-mail:Bulbulia@ukzn.ac.za ; Maharajms@ukzn.ac.za

Abstract

Online fraud is aggressively threatening individuals and some believe that it can turn into a weapon of electronic warfare in the near future. There is strong agreement that society is required to develop its own resilience against this risk (Jakobsson & Srikwan, 2008). Vast sums are spent by both the government and business sectors on deflecting mechanisms and on cleaning up after online attacks which are becoming increasingly sophisticated and diverse (Gartner, 2009). The goal of this exploratory study was to establish what the factors that influenced online security were amongst young South African, Durban based adults. The conceptual framework used to guide this approach was Protection Motivation Theory (Rogers, 1983). Data for this study was collected via an online survey. The questionnaire was e-mailed to prospective participants at the University of KwaZulu Natal, where they could submit it electronically. The survey was also sent to the researchers Facebook friends and Twitter followers who fitted the criteria. Significant findings were that gender, race and employment status affected user awareness of online security.

Peer Reviewed Sapsi Accredited Conference

Abstract accepted for the ISSA 2013 conference that is to be held in Johannesburg on the 14th – 16th August 2013. Below is the abstract of this paper.

Privacy Concerns amongst Young Adults

Z Bulbulia and M Maharaj
College of Management, IT and Governance
University of KwaZulu Natal,
e-mail:Bulbulia@ukzn.ac.za ; Maharajms@ukzn.ac.za

In terms of the Internet, privacy refers to the user's opinion on whether or not the online vendor will try to protect the confidential information collected from them during electronic transactions from unauthorized use or disclosure (Kim *et al.*, 2008). Examples of privacy abuses on the Internet comprise of spamming, usage tracking and data collection, and the sharing of information to third parties (Salleh *et al.*, 2012). When users feel or recognize that their information privacy has been violated, they will avoid disclosing their personal information on the Internet (Dinev & Hart, 2006). It is presumed that the younger generation of users are more net savvy although there has been a study that showed how much personal information people reveal online. Results of this study showed that that the student population is not overly concerned about privacy and security issues (Little, 2008).

The main focus of the study was whether the respondents' demographic profiles had an impact on their online privacy behaviour. The data collected showed that students and young employed adults do reveal a large amount of personal information on social networking websites. What was also found was that race, gender and employment status played a role in revealing certain personal information. This study could be expanded to investigate the differences between online privacy perceptions of young adults in South Africa.

Abstract Acceptance Letter (Annual Teaching and Learning Conference 2013)

This letter is presented on the next page.

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

7TH ANNUAL UNIVERSITY TEACHING & LEARNING HIGHER EDUCATION CONFERENCE

Edgewood Conference Centre, Edgewood Campus, Pinetown, UKZN

25 - 27 September 2013

18 June 2013

RE: Outcome of abstract submission
Abstract Title: **Using Web 2.0 as a strategy to educate users about online security**
Email: Bulbulia@ukzn.ac.za

Dear Zahra Bulbulia,

We are pleased to advise that your abstract submission for the UKZN 7th Annual Teaching and Learning Higher Education Conference to be held at the Edgewood Conference Centre, Edgewood campus from 25 to 27 September 2013 has been accepted by the Abstract Review Committee as a:

Paper: 20 minutes presentations plus 10 minutes for discussion

Please Note:

1. The deadline for payment of registration is 31 July 2013. There will be NO LATE REGISTRATIONS for presenters.
2. If payment is not received on or before the due date, your abstract will not be included in the conference programme.
3. The abstract is subject to layout and language editing.

With best wishes,
Abstract Review Committee
2013 TLHEC

Please forward all correspondence to:
E-mail: utlo@ukzn.ac.za
Tel: +27 (031) 260 3002

University Teaching and Learning Office
Postal Address: 2nd Floor, Francis Stock Building, Howard College Campus, UKZN, Durban, 4041
Telephone: +27 (0) 31 260 3002 **Facsimile:** +27 (0) 31 260 3360 **Email:** utlo@ukzn.ac.za **Website:** utlo.www.ukzn.ac.za

Appendix F – Questionnaire

Factors that influence young adults' online security awareness

I, Zahra Bulbulia am a Masters of Commerce student in the School of Management IT and Governance, at the University of KwaZulu-Natal. You are invited to participate in a research project entitled Factors that influence young adults' online security awareness. The aim of this study is to determine the factors or combination of factors that play a role in increasing user awareness of online security. Through your participation I hope to understand how these factors contribute to user awareness of online security. The results of this survey are intended to contribute to the body of knowledge involving online security from the human perspective. Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this research project. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, IT and Governance, UKZN. If you have any questions or concerns about participating in this study, please contact me or my supervisor at the numbers listed here, Zahra Bulbulia (031 260 8039) Professor Manoj Maharaj (031 260 8023). It should take you about 10 minutes/s to complete the questionnaire. I hope you will take the time to complete this online questionnaire.

* Required

Do you agree to participate in this online survey? *

- ○ Yes
- ○ No

1. Are you currently resident in South Africa? *

○ Yes

○ No

2. How old are you *

○ Under 18

- 18-21
- 21-23
- 23-24
- 24-26
- 26-28
- 28-30
- 30-35
- 35-40
- Over 40

3. Gender *

- Male
- Female

4. My race group is: *

- African
- Coloured
- White
- Indian
- Other

5. Employment Status *

- Employed
- Self-employed
- Unemployed
- Student
- Retired
- Unable to work
- Other

6. In what type of community do you live *

- Urban
- Semi urban
- Rural

7. In what type of community did you grow up *

- Urban
- Semi urban
- Rural

8. At what level do you speak English? *

- First Language
- Second Language
- Third Language
- Fourth or higher Language

9. Your home language: *

- English
- IsiZulu
- IsiXhosa
- Afrikaans
- Other:

10. Where do you mostly access the Internet from? *

- Home
- Work
- University LANS
- Internet cafes
- Other

11. How often do you change the password on your computer? *

- Regularly
- Sometimes
- Seldom
- Not at all

12. Under certain conditions I will give my username and password to a friend? *

	1	2	3	4	5	
Strongly Agree						Strongly Disagree

13. Under certain conditions I will give my username and password to a stranger? *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

14. I know the difference between a virus and a Trojan *

○ Yes

○ No

15. Email attachments may contain viruses or other malware and care must be taken when opening them *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

16. I would be able to tell if my computer is hacked or infected? *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

17. I feel that my computer is very secure *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

18. Is the firewall on your computer enabled? *

○ Yes

○ No

○ I do not know what a firewall is

19. Is your computer configured to be automatically updated? *

○ Yes

○ No

○ I do not know

20. A phishing attack is.... *

○ an e-mail masquerading as a message from a trusted source

○ an attempt to make a computer resource unavailable to its intended users

○ the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.

21. I know what an email scam is and how to identify one *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

22. Is an anti-virus currently installed, updated and enabled on your computer? *

- ○ Yes
- ○ No
- ○ I do not know how to tell
- ○ I do not know what anti-virus software is

23. My computer has no value to hackers, they do not target me. *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

24. I would be comfortable using the Internet to conduct business *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

25. I feel safe about placing my credit card details online *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

26. I have had my credit card details stolen and used in an online transaction *

- ○ Yes
- ○ No

27. Do you know of anyone else who may have had their credit card or card number stolen and used in an online transaction *

- ○ Yes
- ○ No

28. I am concerned about the current state of online security in South Africa *

- ○ Yes
- ○ No
- ○ Somewhat concerned

29. What it is that you fear most with regards to online banking? Select all those that apply to you *

- [ ] An outsider will be able to access my account details and steal my money
- [ ] The Internet might be new to you so it is fear of the unknown
- [ ] Fear of identity theft
- [ ] Fear of being unsure of your rights or protection if something goes wrong
- [ ] If there is a problem there will be no way to trace where your money went
- [ ] I have no fears

30. What is it that you fear with regard to making online purchases? Select all those that apply to you *

- [ ] Money will be "lost" with no record with where it is and how it got there
- [ ] That someone else will gain the benefit of the money you deposited
- [ ] If there is a problem there will be no way to trace where your money went
- [ ] In the event that a problem arises you will experience great difficulty proving that you paid for a product or a service
- [ ] The Internet might be new to you so it is fear of the unknown
- [ ] Fear of identity theft
- [ ] Fear of being unsure of your rights or protection if something goes wrong
- [ ] I have no fears

31. What is it that you fear with regards to social networking? *

- [ ] Fear of identity theft
- [ ] Fear of my account details being accessed by other organisations
- [ ] Fear of my account being compromised
- [ ] I have no fears

32. Installing anti-virus software will keep my computer safe *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

33. Installing anti-spyware software will keep my computer safe *

	1	2	3	4	5	
Strongly Agree	○	○	○	○	○	Strongly Disagree

34. Tick each that apply, I provide the following information on social networking websites *

- [ ] My real name and surname
- [ ] My real pictures
- [ ] My phone number
- [ ] My address
- [ ] My e-mail
- [ ] My work information
- [ ] My interests and hobbies
- [ ] My education information
- [ ] My relationship status
- [ ] I do not have any social networking accounts

35. I get most of my information about online security from *

- [ ] The media
- [ ] Government websites
- [ ] Social networking websites
- [ ] Through friends/family
- [ ] Other

36. What is your perception of online security training? *

- ( ) Not important
- ( ) Important
- ( ) Very important

Appendix G – All Statistical Analysis