

INTERNET PHISHING
HOOK, LINE AND HOPEFULLY NOT SUNK.....

By

Rajan Munien

Student Number 941 350 264

A dissertation submitted in partial fulfilment of the requirements for the
degree of

Masters in Business Administration
in the Graduate School of Business
in the Faculty of Management Studies
at the University of KwaZulu-Natal

Supervisor: Prof. Anesh. M. Singh

November 2010

University of KwaZulu-Natal

Faculty of Management Studies

Graduate School of Business

SUPERVISOR'S PERMISSION TO SUBMIT FOR EXAMINATION

Date :
Student Name : Rajan Munien
Student No. : 941 350 264
Dissertation Title : Internet Phishing – Hook, Line and Hopefully not Sunk....

As the candidate's supervisor,

I AGREE to the submission of this dissertation for examination

I DO NOT AGREE to the submission of this dissertation for examination

The above student has satisfied the requirements of English Language competency.

Name of Supervisor: Prof. Anesh M. Singh

Signature: _____ Date: _____

DECLARATION

I, Rajan Munien, declare that:

- i. The research reported in this dissertation, except where otherwise indicated, is my original work.
- ii. This dissertation has not been submitted for any degree or examination at any other university.
- iii. This dissertation does not contain another person's data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other people.
- iv. This dissertation does not contain another person's written work, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
 - v. Their words have been rewritten but the general information attributed to them has been referenced.
 - vi. Where their exact words have been used, these have been placed inside quotation marks and referenced.
 - vii. Where I have reported a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written solely by myself and have fully referenced such publications.
- viii. This dissertation does not contain text, graphics or tables copied and pasted from the internet, unless specifically acknowledged, and the source is detailed in the dissertation and in the reference sections.

Signed: _____

ACKNOWLEDGEMENTS

I wish to express my sincere appreciation and gratitude to the following individuals, without whose assistance this study would not have been possible:

- Prof. Anesh. M. Singh, who was my supervisor and mentor. You pointed me in the right direction and I am sincerely grateful for that.
- To all the participants of this research, without your invaluable contributions, I would not have acquired the necessary data to successfully conduct this research.
- Mr. H.P. Graber, thank you for your patience, kindness and belief in me. I am extremely honoured to be associated with you.
- Mr. E.J. Myrdal, thank you for your tremendous support during my studies, and most importantly for agreeing to proofread my dissertation. Your kindness cannot be quantified.
- My family who have been by my side throughout this journey, I thank God for each and every one of you, as you have all contributed to my success in your own special way.
- To my friends, thank you for your loyal support and constant words of encouragement throughout this MBA degree.
- To Mr. Frikkie Brooks, thank you for believing in me and my potential to complete this degree and for encouraging me to pursue it. Your professional advice and support will always be treasured;
- To the Department of Co-operative Governance and Traditional Affairs, thank you for affording me a bursary and providing me with flexibility and support during my studies and tenure at the Department. It is an honour and privilege to belong to such an amazing organisation.
- Finally to my MBA Colleagues, this period has been a good one and some of the friendships that were forged will extend beyond our time at the Graduate School of Business. I thank you for that.

ABSTRACT

This study is based on the subject of internet phishing, and the primary goal was to ascertain the level of awareness thereof that exists amongst online users in the Durban area, and to determine if users were able to identify the common characteristics of a phishing attack. Associated research objectives were also to establish whether users were *au fait* with the concept of internet security, and how the correct implementation of this line of defence can prevent possible further or future attacks. Based on the findings of this research, it is further envisaged that a platform be provided to launch a robust awareness programme to attack the insidious invader, thus avoiding and preventing any intentional havoc from being successfully perpetrated. An online questionnaire, being quantitative in nature and comprising 19 questions, was administered to 500 participants. A two-month data collection period was allotted. The questionnaire was completed by 228 respondents, and one of the prerequisites was that they be located in Durban. The data collected was analysed using the Statistical Package for the Social Sciences (SPSS) software. Although the analysis revealed that the level of awareness on the subject matter is average, the incidents of phishing attacks are clearly increasing. The deduction made is that the methods currently deployed to create awareness are obviously not having the desired effect, proving that this strategy has to be revisited urgently. The findings also demonstrate that internet phishing is everyone's responsibility and it is considered prudent for all internet users to make a concerted effort to learn more about the subject. The results concluded that a direct relationship existed between users' level of awareness and the efficacy of internet security installed on a computer. Users who were knowledgeable about the subject, and had installed Internet security software, generally did not experience malicious attacks and were less likely to be targeted. The overall findings presented in this study provide the aforementioned platform upon which an awareness campaign can be formulated to reduce the success rate, and the number, of highly probable future phishing attacks on a previously unsuspecting public.

TABLE OF CONTENTS

DECLARATION	III
ACKNOWLEDGEMENTS	IV
ABSTRACT	V
TABLE OF CONTENTS	VI
LIST OF FIGURES	IX
LIST OF TABLES	XI
LIST OF ACRONYMS	XII
CHAPTER ONE	- 1 -
INTRODUCTION.....	- 1 -
1.1 Introduction.....	- 1 -
1.2 Motivation for the Study	- 1 -
1.3 The Focus of the Study	- 2 -
1.4 Problem Statement	- 3 -
1.5 Research Questions	- 3 -
1.6 Objectives of the Study	- 3 -
1.7 Limitations of the Study.....	- 4 -
1.8 Plan of the Study	- 4 -
1.9 Conclusion.....	- 5 -
CHAPTER TWO	- 6 -
AN OVERVIEW OF INTERNET PHISHING.....	- 6 -
2.1 Introduction.....	- 6 -
2.2 Outline of the Internet	- 6 -
2.3 Internet Phishing	- 8 -
2.4 Types of Phishing Scams	- 10 -
2.4.1 Deceptive Phishing.....	- 10 -
2.4.2 Phishing Resulting from Malware.....	- 11 -
2.4.3 Keyloggers and Screenloggers	- 11 -
2.4.4 Hijacking a Browsing Session:.....	- 11 -
2.4.5 Web Trojans	- 11 -
2.4.6 Poisoning the System Host File.....	- 11 -
2.4.7 Reconfigured System Attacks:	- 12 -
2.4.8 Data Theft:	- 12 -
2.4.9 DNS-Based Phishing (“Pharming”).....	- 12 -
2.4.10 Content-Injection Phishing:.....	- 12 -
2.4.11 Man-in-the-Middle Phishing:.....	- 12 -

2.4.12	Search Engine Phishing	13
2.5	<i>Technology's Impact on Internet Fraud</i>	13
2.6	<i>Technical Trends in Internet Phishing</i>	14
2.6.1	“Bots”	15
2.6.2	Phishing Kits	15
2.6.3	Technical Deceit	16
2.6.4	International Domain Names (IDN) Abuse	18
2.6.5	Session Hijacking	18
2.6.6	Specialised Malware	20
2.6.7	Electronic Surveillance	20
2.6.8	Password Harvesters	20
2.6.9	Account Siphoners	21
2.7	<i>Internet Security - What Protection is Offered to Online Users?</i>	21
2.8	<i>Phishing Protection - Effective Methods to Avoid Internet Phishing Scams</i>	28
2.9	<i>Electronic Mail Security</i>	36
2.9.1	An Example of a Phishing Mail	37
2.9.2	Common Misconceptions / Myths about Email Security	38
2.10	<i>Summary</i>	39
CHAPTER THREE		40
RESEARCH METHODOLOGY		40
3.1	<i>Introduction</i>	40
3.2	<i>Aim and Objectives of the Study</i>	40
3.3	<i>Data Collection Strategies</i>	40
3.4	<i>Research Design and Methods</i>	43
3.4.1	Population	44
3.4.2	Sampling	44
3.4.3	Reliability and Validity / Statistical Technique	45
3.5	<i>Analysis of Data</i>	46
3.6	<i>Summary</i>	47
CHAPTER FOUR		48
PRESENTATION OF RESULTS		48
4.1	<i>Introduction</i>	48
4.2	<i>Demographic Profile of Respondents</i>	48
4.2.1	Cross-tabulation of the Demographic Data	49
4.2.2	Internet Usage	50
4.2.3	Internet Phishing Awareness	50
4.2.4	Internet Phishing Characteristics	52
4.3	<i>Measures of Central Tendency and Dispersion</i>	57
4.4	<i>Calculating Scores to be Used for Detailed Analysis</i>	58
4.5	<i>Score Ratios - Exploring the Distribution of these Scores</i>	59
4.6	<i>Histograms for the Three Scores (Variables)</i>	60
4.7	<i>Analysis of Variances (ANOVA)</i>	62

4.7.1	Group Mean Comparisons	62 -
4.7.2	One-Way Between Groups – ANOVA for Race.....	64 -
4.7.3	One-Way Between Group – ANOVA for Age.....	67 -
4.8	<i>Correlation Analysis</i>	69 -
4.9	<i>Scattergraphs of the Three Scores (Variables)</i>	70 -
4.10	<i>Summary</i>	72 -
CHAPTER FIVE		- 73 -
INTERPRETATION OF RESULTS		- 73 -
5.1	<i>Introduction</i>	- 73 -
5.2	<i>Results of Frequency Distribution Analysis</i>	- 73 -
5.3	<i>Results of the Measure of Dispersion Analysis</i>	- 77 -
5.4	<i>Results of the Correlation Analysis</i>	- 78 -
5.5	<i>Analysis of Variance (ANOVA)</i>	- 79 -
5.6	<i>Summary</i>	- 80 -
CHAPTER SIX		- 81 -
RECOMMENDATIONS AND CONCLUSION		- 81 -
6.1	<i>Introduction</i>	- 81 -
6.2	<i>Findings of This Study</i>	- 81 -
6.3	<i>Implications of This Study</i>	- 83 -
6.4	<i>Limitations of This Study</i>	- 83 -
6.5	<i>Recommendations for Future Research</i>	- 84 -
6.6	<i>Summary</i>	- 86 -
REFERENCES		LXXXVII
APPENDIX 1 – VARIABLES USED TO CALCULATE SCORES.....		XCIV
QUESTIONNAIRE		XCVI
ETHICAL CLEARANCE CERTIFICATE		XCIX

LIST OF FIGURES

No.	Description	Page
Figure 2.1	Graphical Representation of Internet Phishing	8
Figure 2.2	Example of a Security Alert Warning	21
Figure 2.3	Embedded Hyperlink in a Deceptive Email	29
Figure 2.4	Example of a Secured Website	30
Figure 2.5	Example of an Insecure Website (it looks secure, but is not)	31
Figure 2.6	Awareness Creation on the Internet	31
Figure 2.7	Further Awareness Creation Through Print Media	32
Figure 2.8	Concept of a Firewall	33
Figure 2.9	Example of Two Different Pop-Up Windows	34
Figure 2.10	Example of a Phishing Website Requesting Superfluous Information	35
Figure 2.11	Example of a Deceptive Email that Must be Treated with Caution	37
Figure 4.1	Reasons for Internet Usage	51
Figure 4.2	What are the Common Characteristics of Internet Phishing?	53
Figure 4.3	Histogram for the Level of Awareness of the Concept of Internet Phishing	61
Figure 4.4	Histogram for the Level of Awareness of Understanding of Internet Security	62

Figure 4.5	Histogram for the Extent to Which Respondents are at Risk of Being a Victim	62
Figure 4.6	Scattergraph of the Level of Understanding of Internet Security Versus Level of Awareness of Internet Phishing	71
Figure 4.7	Scattergraph of the Level of Awareness of Internet Phishing Versus the Extent to Which Respondents are at Risk of Becoming Victims	72
Figure 4.8	Scattergraph of the Level of Understanding of Internet Security Versus the Extent to Which Respondents are at Risk of Becoming Victims	73

LIST OF TABLES

No.	Description	Page
Table 4.1	Distribution of Respondents in Demographic Groupings	49
Table 4.2	Cross-Tabulation between Race, Age and Gender	50
Table 4.3	Awareness Levels and Victims of Internet Phishing	52
Table 4.4	Information About Internet Phishing Awareness	54
Table 4.5	Understanding the Concept of Internet Security	56
Table 4.6	Mean, Standard Deviation and Variance of Question / Statement	58
Table 4.7	Descriptive Statistics for the Calculated Ratios	60
Table 4.8	Independent Samples <i>t</i> -test for Gender – Group Statistics	63
Table 4.9	Independent Samples <i>t</i> -test for Gender	64
Table 4.10	Descriptives for Race	65
Table 4.11	Test of Homogeneity of Variances (Race)	66
Table 4.12	Analysis of Variance Between Groups for Race	66
Table 4.13	Multiple Comparisons – Scheffè	67
Table 4.14	Descriptives for Age in Terms of the Three Variables	68
Table 4.15	Test of Homogeneity of Variances (Age)	69
Table 4.16	Analysis of Variance Between Groups (Age)	69
Table 4.17	Pearson Correlation	70

LIST OF ACRONYMS

ANOVA	:	Analysis of Variance
APWG	:	Anti-Phishing Working Group
ASCII	:	American Standard Code for Information Interchange
DHTML	:	Dynamic Hypertext Markup Language
DNS	:	Domain Name System
FTP	:	File Transfer Protocol
HTML	:	Hypertext Markup Language
IDNA	:	International Domain Names in Applications
IDS	:	Intrusion Detection Systems
IP	:	Internet Protocol
IRC	:	Internet Relay Chat
ISP	:	Internet Service Provider
IT	:	Information Technology
MBSA	:	Microsoft Baseline Security Analyser
PC	:	Personal Computer
SMB	:	Small and Medium Businesses
SPSS	:	Statistical Package for the Social Sciences
SSL	:	Secure Sockets Layer
UCE	:	Unsolicited Commercial Email
URL	:	Universal Resource Locator

VPN : Virtual Private Networks

WWW : World Wide Web

XSS : Cross-Site Scripting

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The Internet is complicated and it is not getting any simpler (Ratnasingham, 1998). This statement encapsulates the complexity of using this medium for communication purposes. Whilst it has totally revolutionised the way business is conducted by making communication easier and faster, it has also become a haven and a dangerous playground for phishers to easily ply their trade.

The Anti-Phishing Working Group (APWG) officially describes phishing as a process of using spoofed emails designed to lure recipients to websites where phishers attempt to trick users into divulging personal financial information such as passwords and account numbers in order to commit fraud (APWG, 2006). The studies conducted by Vegter (2005) and subsequently by Butler (2006), reveal that users fall prey to phishing scams due to a lack of proper awareness of this particular problem. Therefore, one of the primary objectives of this study is to determine what level of awareness exists, and to try and implement a robust programme to address some of these shortcomings. It also delves further to understand what the common signs of phishing attacks are so that problems can be prevented. This introductory chapter provides an overview of the focus of the survey undertaken and specifies the objectives of the research. It further details the motivation for this study and some of the limitations experienced.

1.2 Motivation for the Study

This study was motivated by the high number of online users who have fallen prey to Internet phishing attacks, some with disastrous consequences, with phishers taking advantage of their naivety. The aim of this study is to contribute to awareness creation, thereby drastically reducing the number of successful phishing attacks that are launched. The preliminary objective was therefore to determine the level of awareness that existed amongst Internet users, and to see if any relationship exists between users' awareness of Internet phishing and the likelihood of them becoming victims thereof. In addition, the study sought to establish if

the amount of Internet security installed on a computer had any bearing on the success of phishing attacks, and to verify whether awareness alone or Internet security, or a combination of these factors, contributed to the success or failure of such attacks.

The second motivation for this study resulted from a series of newspaper articles highlighting fraud associated within the banking sector, particularly of card cloning. Many clients utilised online banking facilities due to the convenience and ease of such practices, but very few were aware of the potential dangers that existed over the Internet.

By ascertaining the current levels of awareness, the study will ensure that a platform can be developed from which an effective programme can be launched to encourage users to be far more vigilant. Being aware of the potential dangers will translate into constantly being on guard against suspicious online behaviours. Highlighting the significance of this problem and its related signs and symptoms will bolster confidence amongst users, as well as enable people to use the Internet as an effective strategic, competitive and communications tool.

This study therefore seeks to provide answers to pertinent questions that online users may have when entering the domain of conducting business over the Internet. The benefits of this study are, however, not limited to employees and employers who have participated in this study, but in fact extend beyond the confines of the organisation, resulting in consumers and investors alike becoming beneficiaries of this research.

The results of this study have hence made a contribution to individuals who utilise the Internet as a medium, whether it is for business or private use, and it has provided answers to some essential questions that needed clarity on the subject of Internet phishing. Users have become more conscious of the subject, but more importantly are now aware of how to prevent becoming victims.

1.3 The Focus of the Study

The focus of this study was the concept of Internet phishing and the level of awareness amongst online users in Durban. It specifically aimed to investigate the frequency and the levels of destruction that these phishing attacks cause. The research also tried to ascertain if any relationship existed, or could be established, between phishing attacks and the levels of Information Technology (IT) security installed on participants' computers, and explored whether exposure to educational literature lessened the probability of them being taken in by such scams.

1.4 Problem Statement

Despite the wealth of knowledge available in the arena of Information Technology and associated Internet security, Internet phishing remains a topic that causes a fair amount of concern (Millettary, 2007). Phishing is used as an underhanded method to steal money from unsuspecting online users. Attacks are escalating and many users fall prey to them because they are not aware of this threat or cannot identify the characteristics thereof. The main purpose of the research is to ascertain online users' knowledge about phishing and to present common tell - tale signs thereof to guide people. This study will also see whether Internet security prevents one from falling victim to online scams. This study will present a foundation for a potential programme that will affect users' online behaviour and prevent them from becoming Internet fraud victims.

1.5 Research Questions

This study addresses the following research questions:

- What is the general level of awareness amongst online users in Durban on Internet phishing?
- What are the common characteristics and tell-tale signs of Internet phishing?
- What should users do if they identify a potential scam?
- Is there a relationship between Internet phishing and the level of security installed on an individual's computer?
- How can one prevent users from falling prey to Internet phishing, and, if one has become a victim, what recourse do they have?

1.6 Objectives of the Study

The objectives of this study were therefore to:

- Determine the level of awareness of Internet phishing amongst online users in Durban;
- Identify characteristics of a potential scam;
- Determine what preventative systems can be adopted by organisations to minimise the threat of this problem; and
- Based on the findings of this research, provide a platform to be used in implementing an awareness programme that thwarts phishers' activities.

1.7 Limitations of the Study

This study was conducted only in the geographical area of Durban, KwaZulu-Natal, and as such, the results may not be representative of other regions in South Africa.

Careful analysis of the responses received revealed that some participants did not answer all of the questions. It is difficult for any researcher to draw descriptive or inferential conclusions from sample data, particularly when some of the questions have not been answered in full.

The method adopted was an online survey, and 86 respondents dropped out of the survey before completing it. Unlike a conventionally administered questionnaire where the researcher can determine and document the reasons for participants not completing the questionnaire, an online survey does not afford the researcher this opportunity, and this can be construed as a limitation.

1.8 Plan of the Study

This chapter provided an overview of the study that was conducted and briefly addressed the stimuli behind undertaking this research as well as the specific objectives thereof. It explained the concept of Internet phishing and showed the importance of being aware of this problem and how one can potentially identify such scams. This is further investigated in the subsequent chapter. Chapter 2 reviews a selection of the vast literature available on the topic, and therefore offers a comprehensive overview on the problem of Internet phishing.

Chapter 3 discusses the research methodology employed in the survey, including the research design, the data collection strategies, and the techniques used to analyse the collected data. A copy of the research instrument, which took the form of an online questionnaire, is included for review purposes as an addendum to this document.

The data received from the 228 respondents was analysed and is graphically presented by means of tables and figures in Chapter 4. An explanation of the findings of this analysis is offered in Chapter 5. The sixth and final chapter provides a conclusion to this study and proposes recommendations based on the findings.

1.9 Conclusion

The main aim of this chapter was to provide an overview of the study with respect to Internet phishing. In an effort to curb Internet fraud, it is essential that people learn about the hallmarks of these phishing attacks. The study's online questionnaire was structured to determine whether any relationship could be established between an individual's awareness level and their having adequate Internet security installed on their computer. Prior to administering the online questionnaire to a sample population in Durban, a comprehensive review of relevant literature was undertaken. The next chapter presents a synopsis of the reviewed literature.

CHAPTER TWO

AN OVERVIEW OF INTERNET PHISHING

2.1 Introduction

Internet phishing, in recent years, has become a serious problem for organisations to deal with, especially financial institutions and individuals. With the advancement of the Internet, the ability to implement underhanded and deviant practices has become prevalent. This chapter provides an overview of the literature that discusses the subject matter, and provides users with the ammunition to prevent them from becoming victims.

2.2 Outline of the Internet

Forcht and Fore III (1995) described a computer network as a group of computers that are connected together through various means, with the primary aim being to transfer information. Telephone lines, fibre optic cables and satellites are commonly used to ensure this connectivity. The Internet is simply a network of networks. This network currently comprises thousands of different networks, with close to three million connected host computers, providing access to approximately 1.9 billion people worldwide to this information super highway (Internet World Statistics...2010).

Statistics currently reveal that the Internet is growing at a rate of 10 % per month (Ratnasingham, 1998). According to Atkinson, Phippen, and Johnson (2005), when personal information is overlapped and influenced by Internet connectivity, the potential for harm emerges. The Internet, as a relatively new medium, offers unlimited opportunities for learning and knowledge sharing, but it can also shape specific inappropriate attitudes and cultivate erroneous and potentially dangerous ideas (Lazarinis, 2009). According to Hawkins, Chou, and Yen (2000), the Internet has become the ideal platform for electronic commerce (e-commerce), but ensuring security remains a key challenge and this is one of the main problems associated with conducting Internet commerce. E-commerce security is defined as a protection system of an information resource against the threat of risks to the integrity, confidentiality, authenticity, non-repudiation, availability and access control of the electronic

transactions transmitted, and more importantly, the reliability of the direct parties involved in electronic commerce (Ratnasingham, 1998).

The threat to computer security is one of the main barriers to Internet commerce. With the current popularity and the potential profits of e-commerce, many executives face a conflict: connecting to the Internet and expanding their business puts them at risk, while not using the Internet could mean they sacrifice customer contact opportunities and sales (Hawkins *et al*, 2000).

The Internet offers a cost-effective medium to build better relationships with customers than was possible with traditional marketing methods such as direct mailing, cataloguing and telemarketing. Internet technologies such as electronic mail (email) and personalised websites offer companies the ability to expand their customer reach, target specific communities and interact with customers in a highly customised manner (Sharma and Sheth, 2004). The growth in the use of email marketing has been accompanied by an enormous increase in unsolicited commercial email (UCE), popularly known as “spam” (Oliva, 2004). In the current context, “spam” is commonly used to describe unsolicited, often bulk, emails (Langford, 2000, p. 23). According to Turban, Lee, King, and Chung (2000), spam (or UCE) is defined as the practice of indiscriminate distribution of messages without permission of the receiver and without consideration for the message’s appropriateness.

As email has emerged as a major means of personal and corporate communication, there has been increased focus on its usage and impact. Researchers have studied, amongst other areas, individual perceptions concerning email (Young, 2004); the impact of email on work practices and employee productivity (Jackson, Dawson, and Wilson, 2003); and the role of email in organisational efforts (McManus, Sankar, Carr, and Ford, 2002). However, there is minimal academic literature on unsolicited emails. While the importance of studying spam is well recognised, little empirical research exists and it is only an emerging field (Sipior, Ward, and Bonner, 2004). As such, this allows would-be hackers and phishers to exploit this domain.

As the Internet represents a global network, providing access to a varying degree of information, it is impossible to make an individual or organisation accountable for it. Therefore, the Internet relies on voluntary co-operation amongst the different network

administrators worldwide to provide people with access to this network of tremendously varied resources (Forcht and Fore III, 1995).

2.3 Internet Phishing

Phishing may be defined as the process of stealing personal information, whereby the Internet is used as the medium in order to commit fraud. This has become a major criminal activity on the Internet (Milletary, 2007). Its main objective is to obtain money fraudulently (Vegter, 2005). Phishing became an official word in August 2005, when it was included in the Oxford Dictionary of English (Independent Online, 2005).

Many users are still unclear as to what comprises a definite phishing attack, and this has been a source of great confusion for computer users or anyone involved in the field of Information Technology. To re-iterate, a phishing attack is characterised by the receipt of an official-looking email from a bank, financial institution or any other service that deals with money such as eBay or PayPal (Vegter, 2005), that attempts to lure users to click onto the link.

In order to demystify the above statement, a schematic as shown in Figure 2.1 will be used to describe the concept of Internet phishing.

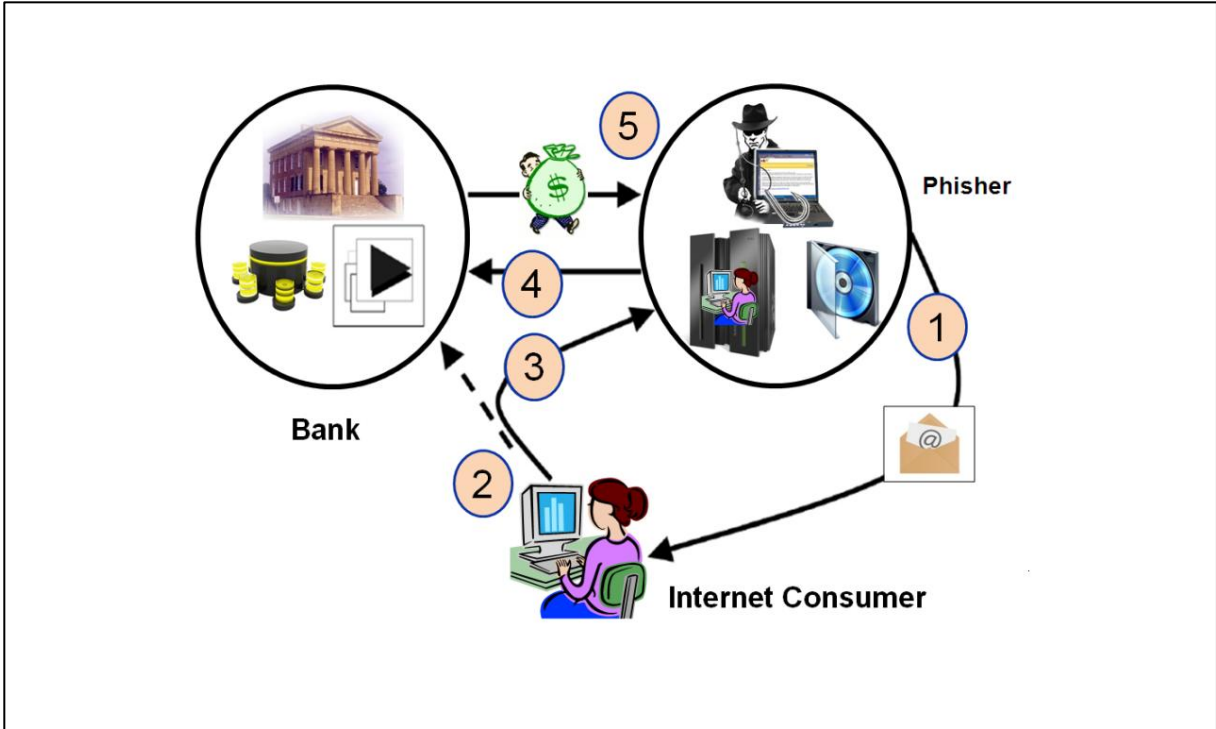


Figure 2.1 – Graphical Representation of Internet Phishing
Adapted from Butler, R. (2006).

Step 1: A user receives an email from the phisher, which states that the recipient should click on to a link to confirm their login and/or password to this particular institution's online facilities.

Step 2: The unsuspecting user clicks on to the link,

Step 3: A webpage opens that looks remarkably similar to the company's genuine website, but is a false page in full control of the phisher, who is implementing an actual phishing scam (Vegter, 2005).

Step 4: Once the unsuspecting users have typed in their login credentials, the hackers immediately capture the data that they require. This data could range from identity numbers, banking account details and / or credit card numbers;

Step 5: The phisher, having all the necessary information at his/her disposal, can now orchestrate identity theft, or steal money from the unsuspecting users' accounts.

The Anti-Phishing Working Group (APWG) officially describes phishing as a process using deceptive emails designed to lure recipients to websites where phishers attempt to trick users into divulging their personal financial information, such as passwords and account numbers in order to commit fraud (APWG, 2006).

With the process of phishing becoming more refined, attributes such as usernames, identity numbers, credit card numbers, birth dates and maternal maiden names are considered important, and therefore become valuable items of information that need to be attained in order that successful phishing attacks can be deployed (Emigh, 2005; Ollmann, 2004). Essentially, phishing is founded upon committing identity theft online.

The incidents of phishing attacks are prevalent because these are comparatively inexpensive to launch, and the potential gain for the phisher can be great (Consumer Reports, 2006). Phishing, as it is known today, burst out across the Internet at the beginning of 2004 (Microsoft, 2006). The term phishing surfaced around 1995 and was used mainly to describe the hijacking of Internet service provider account information (Milletary, 2006). However, today the term has evolved to encompass a variety of attacks with the intent to obtain personal information. Internet phishing, for the purpose of this dissertation, will focus on crimes targeting information of a personal nature that may be used to commit fraudulent activities,

and this can involve identity theft. It has become a successful technique that has been used to steal a person's good name (identity), entailing the use of deceptive email (Emigh, 2005; Ollmann, 2004).

According to Butler (2006), phishers are successful in deploying their attacks as online users are not aware of the associated risks when divulging their personal details over the Internet. Research conducted in the United Kingdom in 2005 showed that nine out of ten survey respondents leave themselves open to identity theft. In a survey comprising 200 respondents, exactly 90% parted with their personal particulars that fraudsters needed to commit identity theft (Clarkson, 2005). With more companies increasing their online presence, the monetary value to be gained by phishers through compromising the account information of their online clients is increasing dramatically (Emigh, 2005).

2.4 Types of Phishing Scams

Deceptive email messages are the most common methods adopted by phishers to gain confidential personal information, although there are many others (Butler, 2006). Other communication avenues do exist, some of which include webpages, Internet Relay Chat (IRC) and instant messaging services, although phishers tend to rely heavily on spoof email to launch their attacks (Butler, 2006). According to Turner, Executive Editor of Symantec's latest report, cyber thieves are currently moving in a totally new direction by focusing on the end user, primarily because the end user is the weakest link in the security chain (Symantec, 2006).

According to Computer Associates International (2005), numerous types of phishing attacks have been identified and the most prevalent ones are:

2.4.1 Deceptive Phishing: The term "phishing" originally referred to account theft using instant messaging, but the most common broadcast method today is a deceptive email message. The content of these messages is varied, and often about the need to verify account information, a system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes or new free services requiring quick action. These emails are sent to diverse groups of people with the hope that unsuspecting users will respond

by clicking on to the link, or alternatively providing login credentials into a fake website, whereby this information can be retrieved at a later stage.

2.4.2 Phishing Resulting from Malware: Malware (from malicious software) refers to software programs designed to damage or execute unwarranted actions on a computer system. This type of phishing therefore refers to scams that involve running malicious software on users' machines. Malware can be introduced as an email attachment, as a downloadable file from a website, or by exploiting known security vulnerabilities – a particular issue for small and medium businesses (SMBs) that do not keep their software applications up to date. In recent times, malware has increasingly been used to target online users who may bank or transact online (Milletary, 2007).

2.4.3 Keyloggers and Screenloggers: The principle behind these loggers are that the keyboard and screen strokes are monitored, and this information is sent in packets via the Internet to the hackers. These applications are lodged within the Internet browser as small utility programs. They are referred to as helper objects that run automatically in the background as soon as the browser is activated.

2.4.4 Hijacking a Browsing Session: This form of attack has been perfected by hackers, whereby the user's activities are continually monitored until they log in the target account or effect the actual transaction, using their legitimate credentials. It is at this point that malware takes over and performs unauthorised actions, such as transferring funds without the user's knowledge, (Computer Associates International, 2005).

2.4.5 Web Trojans are little programs that activate invisible pop-up screens when users attempt to authenticate their accounts. This information is cloned and then transmitted to the phisher via the Internet.

2.4.6 Poisoning the System Host File: All website addresses are first translated into an Internet protocol address before opening up the actual website. All Windows based operating systems contain a "host file" which contains the various "host names" and credentials. Hackers begin by analysing the host file, before Domain Name System (DNS) lookup. By infecting the host file, hackers would have created a false address, thereby taking the user to a fake look-alike website from which their information can be stolen.

2.4.7 Reconfigured System Attacks: This form of attack modifies settings on a user's machine primarily for malicious purposes. An example of this includes hackers accessing a user's favourites folder and modifying existing legitimate sites to point to look-alike websites (Computer Associates International, 2005). A simple example, used to great effect, involved a bank URL that was changed from “**bankofabc.com**” to “**bancofabc.com**”. Changing one letter meant that users did not notice the discrepancy, and they assumed that the URL was legitimate. In this instance, the letter “k” of bank was replaced with a “c”, yet the “feel” of the URL remained the same.

2.4.8 Data Theft: Machines that are not part of a secured environment, generally contain information of a sensitive nature that would normally be stored on secured servers. If these machines are periodically used to access information of those servers, then the integrity of the data is compromised. Data theft is a widely used tactic in business espionage. Thieves often steal confidential information, design documents, legal transcripts, and employee-related records, and profit by selling the data to those who may want to embarrass or cause economic damage to their competitors.

2.4.9 DNS-Based Phishing (“Pharming”): Pharming is the name attributed to a phishing attack that modifies the host file. It is also referred to as Domain Name System (DNS)-based phishing. The basic premise behind any pharming attack involves the hacker tampering with the host files that redirects further requests or communication to a false website. This results in users unknowingly providing confidential information via a website, that is deemed legitimate, but which is in actual fact controlled by hackers. These hackers may not even be in the same country where the crime is being perpetrated, (Computer Associates International, 2005).

2.4.10 Content-Injection Phishing: This type of phishing attack occurs when hackers replace part of a legitimate website with false content designed to force the user into providing their confidential information. For example, hackers may insert malware to log a user's credentials, or an overlay that secretly collects information and delivers it to the hacker's server.

2.4.11 Man-in-the-Middle Phishing: This type of attack is extremely difficult to detect as hackers position themselves between the user and the legitimate website. All of the

information that is exchanged between the user and the legitimate website is being copied, at the same time the requests are being processed, thereby not arousing any suspicion. This copied information can be later sold, depending on the sensitivity, and the phisher can still perform transactions even when the real client is not online.

2.4.12 Search Engine Phishing occurs when hackers craftily design websites offering extremely eye-catching offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services. For example, scammers set up false banking sites offering lower credit costs or better interest rates than other banks, and people who use these sites to save or earn interest are encouraged to transfer existing accounts, in the process giving up their details to the fraudsters.

2.5 Technology's Impact on Internet Fraud

The commercial possibilities of the Internet are vast and marketing products and/or services via Internet email is an inexpensive and easy way to advertise to millions of people (Attaran, 1999). However, the increase in online marketing practices and e-commerce has spawned prolific online fraud (Baker, 1999). Misleading and fraudulent practices in electronic commerce have increased appreciably according to the National Users League (Attaran, 1999). Because consumers have become used to receiving legitimate marketing emails and commercial communications, it is relatively easy for people committing fraud to send credible-looking messages to many potential investors (Baker, 1999).

The World Wide Web has made it easier for people to become entrepreneurs and has led to a rapid growth of companies, many of which run “virtual offices” and sell products via the Internet, which in turn has fuelled Internet fraud (Baker, 1999). Even though growing very rapidly, electronic commerce is still developing, and many entrepreneurs are yet to establish an online presence. Ultimately, if they cannot embrace the technology that the Internet offers, they will lose out to competitors who have modernised their sales and marketing strategies. However, many scams aim to take advantage of an entrepreneur's Internet innocence. It is therefore prudent that Internet-related business opportunities are as carefully considered as any other business opportunity would be, and that entrepreneurs learn about the associated risks and adequately protect their businesses from would-be online criminals (Attaran, 1999).

2.6 Technical Trends in Internet Phishing

Phishing has grown into one of the most prevalent Internet threats (Pruitt, 2005). These scams have surfaced in the past few years as a result of the advancement in technology and positive economic climate (Milletary, 2007). To execute a successful phishing attack requires minimal resources which can be acquired very easily using underground websites. This lowers the barriers of entry for criminals who are not fully *au fait* with the Internet to launch such attacks (Sophos, 2004).

Criminals who prey on the acquisition of innocent or unsuspecting user's personal information are able to prosper in phishing attacks, since many people are now deciding to transact online, resulting in them parting with some of this information (Roberts, 2004). The use of a deceptive email, being portrayed as though it is from a trusted agent (these could include an auctioneer, bank or an online commercial site) is used for phishing attacks today. Clever techniques such as the validation of one's account, failing which, this could result in the account being suspended, is often used by phishers to create a sense of urgency, and this pressures individuals to comply, resulting in them becoming victims (Milletary, 2007).

Recently, several new social engineering approaches have been adopted (Roberts, 2004). For instance, the user may be requested to fill out a survey on an online banking facility and be offered a financial reward if they included their account details, or the message may claim to be from a financial institution and request customers to confirm their credit card information.

Whilst deceptive emails and dubious websites have primarily been used to tempt users to disclose their personal information, phishers are now also starting to use malware to achieve this task (McWilliams, 2003). Once installed on a victim's computer, these applications adopt various techniques to elicit crucial account information.

Phishers have many tools at their disposal that can be used and called upon, depending on the task at hand. Commonly used tasks involve sending deceptive emails, hosting a potential phishing site, or keeping a repository of malicious code that may be easily accessed if required (McWilliams, 2003). The most commonly used tools include:

2.6.1 “Bots” are applications that will be installed unsuspectingly on to a machine. Its primary purpose is to provide remote access using various protocols. Some of these protocols include using Internet relay chat, instant messaging etc (Sophos, 2004). A combination of these bots, which may be controlled centrally, is known as a “botnet”. Through the bot, the phisher has the following capabilities that can be used to create havoc, and these include:

- Devices that will resend spam and deceptive emails;
- Servers that will redirect spam and malicious code;
- Being able to provide software updates for the above code;
- Installation of new or additional malicious code;
- Full proxy access;
- Services that generate revenue when users click on to links;
- To perform scans that show vulnerable areas that can be exploited; and
- Continual surveillance.

New hosts are often infected as a result of the above mentioned capabilities, and many of these are launched through social networks. Some of these include mass mailers, shared programs, and instant messaging networks (McWilliams, 2003).

2.6.2 Phishing Kits: Phishers are extremely organised, and have access to ready-to-use phishing kits containing items such as pre-generated HTML pages and emails for popular banks and online commerce sites, scripts for processing user input, email and proxy server lists, and even hosting services for phishing sites (McWilliams, 2003). These hosting services usually advertise themselves as being impossible to shut down, or as “bullet proof” (Roberts, 2004). Spammers have been using them for years (McWilliams, 2003).

Traditionally, these kits are bought and sold by criminals within the underground community. However, versions of these kits are available for anyone to download at no cost (Sophos, 2004). Phishing kits lower the barrier of entry into the marketplace for criminals, reducing the amount of technical knowledge required to conduct a phishing scam, which promises huge monetary gain if it is perfectly executed.

2.6.3 Technical Deceit: Through awareness initiatives, many people are becoming more *au fait* with phishing, and are better able to detect fake emails and websites, thus criminals have developed alternative techniques (Millettary, 2007). Some of these include confusing the actual website address that renders a phishing site more real, and being able to exploit these vulnerabilities, facilitates the installation of malware from a hostile website. The following are some of the more common forms of deceit:

2.6.3.1 Basic URL Confusion: This approach makes victims believe that a hyperlink or webpage displayed in their web browser or Hypertext Markup Language (HTML)-capable email client is that of a trusted site. This method is technically simple yet highly effective, and is still used to some extent in phishing emails (Sophos, 2004). An anchor element, placed within the legitimate website address, but having its attributes pointing to a malicious website, is still one of the easiest methods used to obscure the actual destination of an actual or real URL. Therefore, by clicking on to a legitimate-looking URL actually sends the user to a phishing site (Sophos, 2004). A user can detect this malpractice by simply hovering the mouse pointer over the hyperlink embedded in the email, as the destination of the hyperlink will be displayed in full. This information is also shown in the actual status bar of the website browser.

Emails delivered in hypertext markup language are becoming more rampant. Phishers are benefiting from this by constructing deceptive emails that contain a single image in JPEG format (Millettary, 2007). When displayed, it is the actual image that is displayed and not the email which appears to be as one coming from a bank or merchant site, particularly as the image often includes the official logos and text, and clicking on to them redirects users to the phishing website.

Many users are becoming suspicious, and some will even try and find out if the website URL is that of a real website. Because phishers are aware of this, they often try and register the domain of the target institution, and this strategy often tricks users into believing that what they are seeing is that of a legitimate website (Sophos, 2004). The above can be easily demonstrated whereby a website displayed as `http://www.bankname-online.biz`, has `<bankname>` substituted with the name of the target bank. An example of this commonly used method uses parts of the real web address to form a new domain name, as shown below,

where the simple replacement of a “dot” with a “hyphen” creates the same “feel” as the legitimate URL.

Legitimate URL `http://login.example.com`

Malicious URL `http://login-example.com`

2.6.3.2 Web Browser Spoofing Vulnerabilities: Phishers have the ability to confuse website addresses, thereby installing malicious code, and they are then able to exploit any vulnerable web browsers (Milletary, 2007). These vulnerabilities are easily installed on machines that have security patches which are out of date. Listed hereunder, are two cases of web browser vulnerabilities that have been used in phishing attacks (Sophos, 2004). Both of these, however, have been fixed, and these updates are available from the vendor websites.

VU#490708 – Associated with Internet Explorer browsers and creates chromeless windows.

According to Milletary (2007), the purpose of the above vulnerability creates a borderless window that can be overlaid over the actual website address. The window is borderless and is therefore difficult to detect. This window also contains a legitimate logo of a real website, but in fact blocks out the phishing website address, thereby tricking users into believing that they are on the real website. This common method is primarily used when financial houses are targeted.

VU#356600 – Also associated with Internet Explorer. The Dynamic Hypertext markup language editing ActiveX Control contains a cross-domain vulnerability.

According to Milletary (2007), hackers use this vulnerable code, which is downloaded from a malicious site to change information in the browser window of a different domain. Unsuspecting users are therefore tricked into clicking on to a malicious web address that activates the DHTML Edit control. This results in a new Internet browser being opened representing that of a trusted website, and then using the above vulnerability change content of the trusted and secure site (Sophos, 2004). The common attributes of the browser window would reflect those of the real website, thereby negating any cause for concern by the user.

2.6.4 International Domain Names (IDN) Abuse

In an existing domain name system infrastructure, the instrument that allows domain names that are represented by unicode characters to be replaced by their ASCII equivalent is known as the international domain names for applications (Milletary, 2007). The encoding language rules are called punycode, which is used to display unicode characters in ASCII format. Browsers that support IDNA would therefore understand this code and accordingly present the unicode characters when appropriate. As a result of this, browsers that support IDNA are easily at risk to phishing via homograph attacks (Gabrilovich and Gontmakher, 2002). Because of this, hackers tend to register domains that have a unicode character that appears to be identical to their ASCII equivalent in a legitimate site. A simple example is that of a website containing the word “bank”, but utilise the Cyrillic character “а” instead of the ASCII “a”, keeping the actual “feel” of the website (Milletary, 2007). The concept of this type of attack has been publicised, even though no cases have as yet been documented.

2.6.5 Session Hijacking

The common modus operandi for phishers is to use deceptive emails that force users into visiting a malicious website (Sophos, 2004). On the other hand, it is possible that a user may be redirected to a phishing site even if they correctly try to access a legitimate site. Examples of session hijacking include:

2.6.5.1 Domain Name Typos

According to Milletary (2007), a recent attack trend has been the registration of domain names that closely resemble the domain name of a legitimate high-traffic site. The domain names are sometimes used to host sites that aim to install spyware or malware on the computer of a victim who mistypes the intended domain name. It is also possible to register domain names that could be common typographical variants of online commerce sites.

2.6.5.2 Man-in-the-Middle Attacks

This class of attacks results in hackers being able to intercept, read and modify communication between two people, without their consent. With reference to Internet phishing, this type of attack usually involves a hacker who serves as the proxy between a user and an online commerce site. As a result of this interception, the hacker has access to all relevant information e.g. passwords and account information, and is thereby able to cause damage to these unsuspecting users.

2.6.5.3 Cross-Site Scripting Attacks (XSS)

This type of attack is generally used on websites that require users to input credentials (Sophos, 2004). They reside on these sites as little applications. If the application fails to clean the keyed information properly, then the vulnerable program may process this data or execute malware that it was not intended for. For instance, a phisher could build a URL that uses a susceptible program on a legitimate commercial website. The web address can contain incorrect or confusing code, such as JavaScript, that could gather account details. These types of attacks have reportedly been used in phishing scams against financial institutions worldwide.

A more common XSS attack involves programs that are redirected as a result of exploiting a vulnerable web address (Milletary, 2007). Websites often use these redirectors to perform custom processing based on attributes such as web browser and authentication status, or simply generate a message when clicking on to a link to an outside website. Numerous incidents were reported whereby commercial sites have used URL redirectors that have allowed a user to input their own external URL. As a result, phishers would send deceptive emails that utilised these vulnerable redirectors on the legitimate sites to trick unsuspecting users into visiting bogus websites.

2.6.5.4 Domain Name Resolving Attacks

Online users' navigation of the Internet relies extensively on the process of mapping "easy-to-remember" domain names to Internet protocol addresses (McCrohan, 2003). Cyber criminals

can subvert this process which results in users being diverted to malicious websites. A commonly used method compromises the information used by the Domain Name System (DNS) through introducing malicious information into authoritative DNS query responses, and this is known as DNS cache poisoning (Sophos, 2004). Pharming has been used to describe this specialised type of attack being used to cause phishing scams. Malware is also another method employed to add fictitious entries into a computer's hosts file which, on some operating systems, will be checked by the local domain name resolver before making a request to a DNS server.

2.6.6 Specialised Malware

As alluded to in section 2.4.2, malware refers to software programs designed to damage or perform unwarranted actions on a computer system. Phishers potential return on their minimal investment is substantially increased by utilising malware, as they are able to target information for as many, or as few sites, as they wish. Moreover, it is easy to reconfigure most malware so that it can change its intended websites or alternatively include new sites, using various mechanisms to steal data. Specialised malware may be seen as a class of spyware.

2.6.7 Electronic Surveillance

Applications that are capable of capturing a user's keyboard input or mouse clicks have been in existence for a while (Milletary, 2007). Applications are now being refined to specifically target information about commercial websites of interest by analysing users' keystrokes typed in browsers. Malware is also capable of capturing network packets or protocol information of interest. Whilst HTTPS (HTTP over SSL) is used for many commercial websites, malware can easily retrieve sensitive data before it is encrypted for transmittal over the secured network. Malware is capable of taking screenshots when it detects that a web browser is visiting a site of interest (Sophos, 2004). This could potentially allow the capture of sensitive information, including bank account numbers and account balances.

2.6.8 Password Harvesters

Several classes of malware are capable of searching a computer for account and password information. On Microsoft Windows platforms, this includes searching the registry and

Protected Store. The Protected Store is a facility provided by the Microsoft CryptoAPI and it is used to store sensitive data, including Internet Explorer AutoComplete fields, passwords, and digital certificates.

2.6.9 Account Siphoners

The basic purpose of malicious phishing code is to steal user account authentication information, and to duplicate this data such that it can be easily retrieved and used at a later stage. One class of malware does exist that actively steals money from a financial institution by automating a transfer from the victim's account, and in the process, siphons the accountholder's details.

2.7 Internet Security - What Protection is Offered to Online Users?

Because no individual, company, government agency, region, country, or association controls the Internet, no one has the authority to dictate policies or actions that would promote secure usage of the Internet (Forcht and Fore III, 1995). This means that using the Internet comes at a premium for the millions of users who have been taken advantage of by cyber criminals.

So, what makes the Internet susceptible to electronic attacks? The Internet, being a decentralised system, provides access to millions of computers around the world. These computers have their own encryption, in the form of passwords and security protocol, or possible lack thereof (Forcht and Fore III, 1995). In most scenarios, however, the Internet is only as strong as its weakest link, and the intruders who hack into one part of the system inevitably gain access to much of the rest. Hence, having appropriate security is important, as it will create alerts when suspicious activity is recognised, as demonstrated by Figure 2.2.

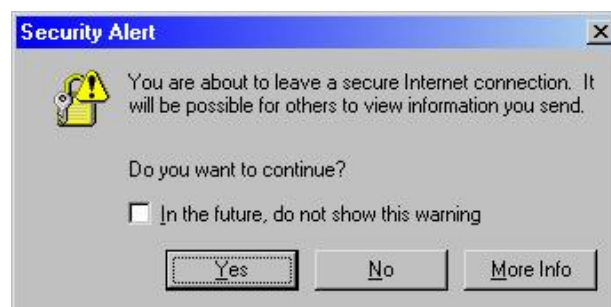


Figure 2.2 – Example of a Security Alert Warning

Adapted from Configuring the CSS for Device Management. 2006.

According to Forcht and Fore III (1995), Internet protocol spoofing is a commonly used method that allows hackers to penetrate an organisation's network. This involves passing security measures e.g a firewall, pretending to be a computer that resides on the companies internal network. Each machine on the network is identified by its Internet protocol address, which attaches to a digital envelope that can contain sensitive and important data. Generally, when machines on a network display their full Internet protocol address, then full access is normally granted to these machines. In order to penetrate the system, the hacker impersonates the Internet protocol address of one of those specified internal computers. Any firewall that has not been configured properly will immediately grant the hacker access into the system, as a result of picking up the incorrect Internet protocol address. A second method causes the hacker to communicate with the target computer, which sometimes sends back a number, but this is repeatedly changed. A trusted computer would have to be able to repeat that number in order to gain access. These types of intrusions, however, are proving to be more common.

Another way that hackers gain entry on UNIX machines is by intercepting their telnet ports, normally querying the sendmail application, and this enables the hackers to find out certain types of information about a system (Forcht and Fore III, 1995). Generally, the version number and the type of operating system is the information that is most sought after, as this informs the hackers next step, having received valuable clues and the level of security that he has to deal with. Many known bugs and holes in older versions of sendmail still exist and hackers exploit this area. In addition, a hacker can pretend to be an internal user thereby being able to send requests through certain commands, thus obtaining information. The "expn" or "vrfy" command can be used to collect information about users, giving the hacker valid user credentials to try and break into the system, thereby compromising the security of the user.

The primary goal of the hacker is to gain access into the system. Once the system's security has been breached, the hacker can install a virus on to the server. There are many different types of computer viruses. Whilst some are downright annoying, there are others that can be extremely vicious (Forcht and Fore III, 1995). Certain viruses are capable of being parasites on files that are being transferred via File Transfer Protocol (FTP). This scenario can be catastrophic since the information on the host server can be compromised.

Cyber crimes are becoming more prevalent. Forcht and Fore III (1995) showed that employees of a large financial institution who were cash strapped, but well equipped with computer skills, accessed the company's mainframe computer and "kidnapped" invaluable

company secrets by locking them into a sophisticated encryption program. This intervention can facilitate the transfer of funds into bogus bank accounts (Forcht and Fore III, 1995).

The above is an example of an Internet-based computer crime. Spoofing programs are regularly used to intercept important messages and the successful execution thereof enables passwords to be stolen and computer networks to be entered illegally, allowing hackers to virtually create havoc on an organisation's infrastructure. Computers have been used in crimes associated with tax evasion, insurance and credit card scams, software infringements and it also has been used for violent crimes ranging from corporate espionage all the way to homicide.

The Internet security threat report released in September 2006 by Symantec revealed that during the first half of the year 2006, 157 477 phishing messages were sent with the intention of gaining personal information, as picked up by the Symantec probing network. The report revealed that all of the messages were different in terms of content, and each represented a unique approach in deceiving the end users into divulging their personal credentials. Notably, a single message may be used many times in different phishing attempts to target diverse group of consumers (Symantec, 2006).

According to Butler (2006), phishers are successful in deploying their attacks as online users are not aware of the associated risks of divulging their personal details over the Internet. Users need to be more vigilant of the possible risk of identity theft through phishing, and should be familiar with the tell-tale signs of a typical phishing attack (Butler, 2006).

The Internet has no built-in security as messages and information sent via computer may be routed through many different systems before reaching their destination (Aldridge, White and Forcht, 1997). Users need to know that properly applied security measures can protect them from falling victim to cyber attacks, and how to react appropriately and timeously on discovering that they have fallen prey to a phishing attack (Butler, 2006).

The Internet is a strategic tool and can provide a competitive edge to all organisations worldwide who want to embrace it, because it gives them access to valuable information and ensures that their suppliers and customers can be reached with ease (Aldridge *et al.*, 1997). However, the risks associated with such transactions are high. In order to capitalise on the

vast resources that are available on the Internet, organisations must strike a balance between accessing and providing access to information and mitigating the potentially adverse consequences of doing so (Aldridge *et al.*, 1997). There is only one sure way of avoiding any potential risks, and that is to refrain from using the Internet (Butler, 2006).

One of the commonly asked questions is how can the Internet be used without causing anyone harm? Consideration for fundamental security issues should be the starting point (Liddy, 1996). Confidentiality has to be adhered to, and sensitive information should be restricted only to those who should have access to it. Data integrity is fundamental, as this assures companies that data has not been modified. Finally, it is extremely important that the Internet is always available i.e. lines are not down, since complex enterprises to small companies need to be continually running if they are utilising the Internet to conduct their business (Liddy, 1996).

In order to create a safe organisational domain, the method often used in recent years was to install a firewall between the Internet and the internal network that required protection (Franklin, 2008). The problem with this concept is that it has been designed to let nothing in from the Internet, while still permitting users to send messages out to the rest of the world. This level of security translates into an incredible loss of functionality (Franklin *et al.*, 2008).

A subsequent development combined the firewall with a router and this allowed selected Internet traffic to pass through (Grimes, Head, Hines and Franklin, 2008). This approach has been considered mediocre, mainly because the actual headers for the information packets were capable of being filtered by the router. Hackers who are more sophisticated are fully capable of modifying the source location and routing information contained in these headers, and can therefore reconfigure aliases and user IDs, thereby bypassing most firewalls and routers. Subsequent developments involved the Internet community utilising certain security measures that were once hidden and previously have been the privilege of the intelligence community only (Grimes *et al.*, 2008).

Cryptography is currently being utilised to guarantee Internet security and it is fast becoming the standard. It is based on a combination of encryption, authentication, and digital signatures. Encryption may be defined as the transformation of data into a form unreadable by anyone

without a secret decryption key (Forcht and Fore III, 1995). Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended.

In a multi-user setting like the Internet, encryption allows secure communications over an unsecured channel. Forcht and Fore III (1995) describe an example of the encryption process if one wants to prevent an intruder from reading the message, whereby a user 1 who wishes to send a secured message to a user 2, needs to adopt this procedure. User 1, by using an encryption key, encrypts the message that is intended for user 2. This initial message before encryption is called plaintext. User 2 now receives this encrypted message which is now referred to as cyphertext. With the aid of a decryption key, user 2 is capable of reading this message. A third user, normally the hacker, will try and intercept this secret key or even attempt to get the plaintext message. In a secured cryptosystem, the conversion process from the plaintext to cyphertext will not be possible without the use of the decryption key. A single key can only serve both purposes i.e. encryption and decryption in a fully symmetric cryptosystem.

Authentication in a digital setting is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message. Authentication protocols can be based either on conventional secret-key cryptosystems or on public-key systems (Forcht and Fore III, 1995). Forcht and Fore III (1995) show that traditional cryptography is based on using a common secret key, that only the sender and the intended recipient has access to. The sent message is encrypted utilising this key, whilst the recipient decrypts the message using the same key. This method is commonly referred to as secret-key cryptography. The associated problem, however, is ensuring that both the sender and receiver agree on the secret key, without its code being discovered. If the sender and receiver are geographically separated, then the services of a courier company or some other communication means can be utilised, not to disclose the secret key. If the key is intercepted, then the entire process is jeopardised.

Digital signatures are currently used for authentication purposes in public-key systems (Aldridge *et al.*, 1997). Digital signatures for digital documents play a similar role to that of handwritten signatures for printed documents. The signature is an unforgeable piece of data asserting that a named person wrote or otherwise approved the document to which the signature is attached. The recipient, as well as a third party, can verify that the document did

indeed originate from the person whose signature is attached, and that the document has not been altered since it was signed. A secure digital signature system consists of two parts: a method of signing a document in such a way that forgery is impossible, and a method of verifying that a signature was actually generated by whomever it represents (Aldridge *et al.*, 1997). Secure digital signatures cannot be repudiated, and the signatory of a document cannot later dispute it by claiming it to be a forgery.

The generation, transmission, and storage of keys is called key management (Forcht and Fore III, 1995). All key management issues must be addressed through cryptographic systems. In a public-key cryptography system, each person is assigned a public and private key. As the name suggests, the public key is published. However, the secrecy of the private key is the responsibility of the individual with whom it is entrusted. Public keys are used to facilitate all open communication, and the private key is not shared or transmitted (Forcht and Fore III, 1995). It would be naïve to think that the communication channel is absolutely secured and the threat from outside intervention is not possible. It is important to note that a confidential message may be sent using a public key, but it has to be decrypted with a private key belonging to the recipient for whom the message is intended.

Having secured communication channels is a bonus, but it does not eradicate all the anxiety of the end user. The above only ensures safety of the actual Internet routers that is used for communication purposes. Choosing to do business online does not mean that the people you engage with are reputable, and therefore having all the appropriate security measures is not going to identify this trait. Based on the above, as an example, users should only transact online if they feel they can trust a server administrator with their credit card number before entering into any online transaction (Liddy, 2006). The above situation is comparable to using telephone banking that involves you parting with your account details over the telephone and you have to trust the person on the other end of the call. This brings about the concept of privacy, whereby one hopes that no third party has intercepted the conversation, and the second concept being authentication, whereby one trusts the operator on the other end of the call, and believes that this operator actually works for the company that you are attempting to do business with. The users must therefore be in a position to trust the telephone operator and the actual company (Liddy, 2006).

In order to thwart security violations, it is crucial for end users and network administrators to take additional precautions. In an effort to safeguard data, users need to be vigilant in having physical security on their machines and servers. This can also be achieved by ensuring that all systems access control is through the use of appropriate passwords. There are several simple methods that one may adopt. Firstly, to have a good starting point to control the physical access that one has on one's computer. Secondly, passwords should be changed regularly. Thirdly, ensure that one has the latest updates associated with the anti-virus software in current use to prevent viruses from attacking one's computer. Normally, a virus can only become active if the user starts a computer from a disk infected with a boot virus, or if one runs an infected program. Finally, virus definitions should be continually updated and regular system scans performed, especially when new software is being installed.

Automatic scanning should be activated so that this process is conducted at specified times. Backups of all essential data must be made regularly. One should also try and purchase and install legal copies of software, and make write-protected backup copies of all software.

While it is a good idea to make workstations, servers and other systems as individually secure as possible, this is not sufficient to defend one's website from attack (Liddy, 2006). Without the ability to protect an entire network at its connection point, this defence is only as strong as its weakest link. Securing every system is a complex and cumbersome job with no guarantee of success due to the variety of different operating systems, releases, vendor patches and administrative domains in play. However, by analysing and defending against threats at a site's point of connection to the Internet, one can take advantage of most Internet services while simultaneously limiting the risk of intrusions.

According to Hawkins *et al.* (2000), organisations in both the public and private sectors are aware of the need for Internet security to protect their Internet data and corporate systems. Internet security describes the methods used by an organisation to protect its corporate network from intrusion. The best way to prevent an intruder from entering the network is to provide a security wall between the intruder and the corporate network, as such invaders are quite capable of entering the network. To achieve their aim, they can either download a virus, install a trojan horse or even a worm, all of which are forms of software programs.

2.8 Phishing Protection - Effective Methods to Avoid Internet Phishing Scams

The risks of working and doing business in cyberspace are outweighed by the tremendous potential for reward (Aldridge *et al.*, 1997). As long as one keeps one's eyes open, assesses the risks realistically, and takes intelligent precautions, one can navigate cyberspace, knowing that one's networks are safe from unwanted intrusion (Russell, 1995).

Educating the consumer about phishing threats are essential, but more importantly, the proper application of the appropriate Internet security measures which may minimise the danger of identity theft will therefore play a fundamental part in ensuring that a sustainable resolution to the problem can be achieved (Emigh, 2005).

According to Warren (2005), the following precautions and examples will assist in reducing the chances of users falling victim to phishing.

1. **Ensure That Your Anti-Virus is Always Up-to-Date** – It cannot be emphasised how important it is to keep one's anti-virus software up to date, as this is the first line of defence. Do not compromise the system by using a cracked version of the software that is not capable of receiving automatic updates. Most anti-virus vendors have built-in signatures that protect against common technology exploitations. One such threat is a Trojan, which is capable of camouflaging the URL or even impersonating a https secured link. By not having the anti-virus software up-to-date, one is merely subjecting oneself to threats, such as having the browser session hijacked (Warren, 2005).
2. **Do Not Click on to Hyperlinks Embedded in Emails** – It is never advisable to click on to any hyperlink in an email, especially from an unknown source. One never knows where the link is going to really take you or whether it will trigger malicious code. Some hyperlinks can take one to a fake HTML page that may try to scam one into typing sensitive information. If one really wants to check out the link, manually retype it into a web browser (Warren, 2005).

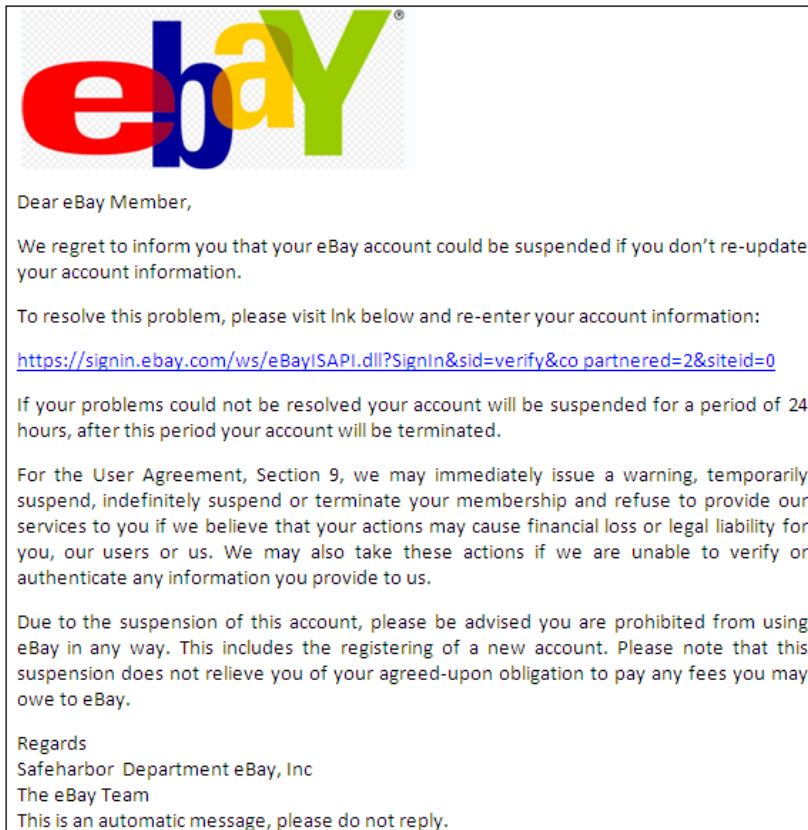


Figure 2.3 – Embedded Hyperlink in a Deceptive Email

Adapted from eBay Scams (2009) – Sample phishing email.

3. **Take Advantage of Anti-Spam Software** – Anti-spam software can help keep phishing attacks to a minimum. Spam is used as a vehicle to launch these attacks. Using anti-spam software can reduce the types of phishing attacks, since the messages are prevented from being delivered to their falsely intended recipients (Graham, 2002a).
4. **Check for HTTPS (SSL) Link** – If one is dealing with sensitive information (account names and numbers, credit card numbers etc), it is crucial to verify that the link is secured. This can be achieved by looking at the address bar to make sure that it shows “https://” rather than just “http://” and to ensure that the “lock icon” (which depicts a secured page) is at the bottom right hand corner of your browser.

Figure 2.4 shows an example of a secured website. Careful attention needs to be paid to the https:// in the actual URL and the “lock icon” at the bottom right of the webpage.

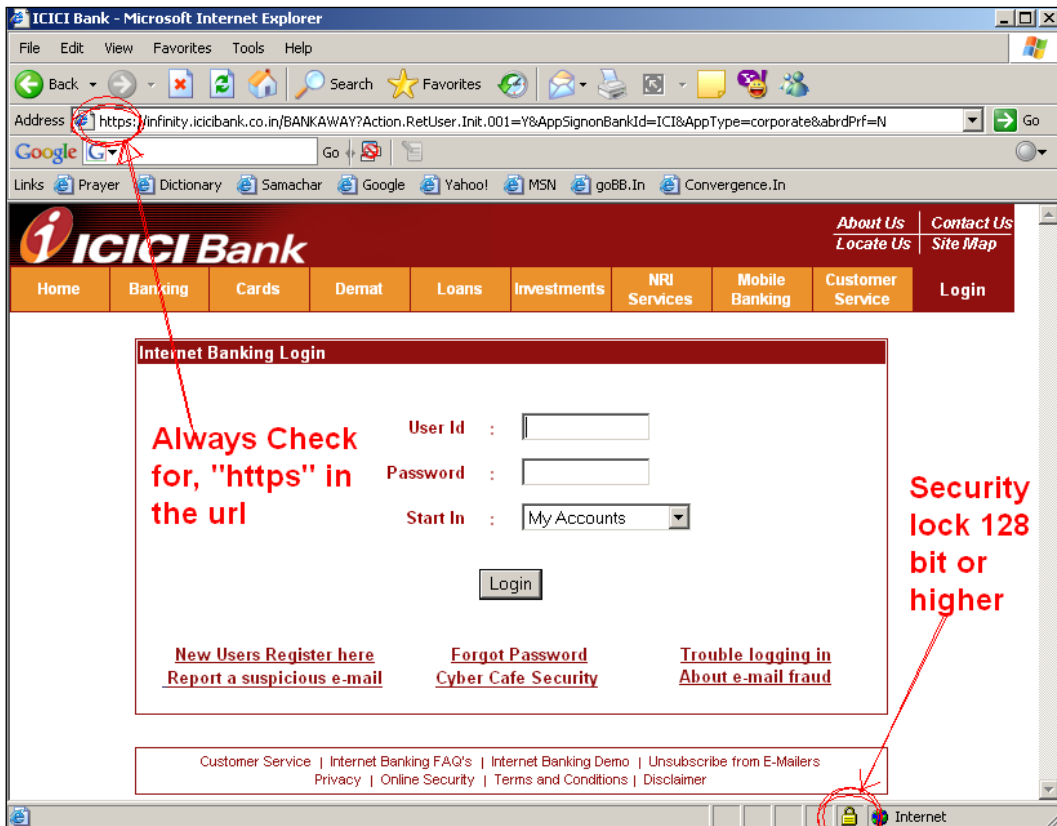


Figure 2.4 – Example of a Secured Website

Adapted from Fake ICICI Bank Website (2010) – Beware of phishing email.

By double clicking on to the lock icon, one is able to view the actual guarantee certification of the third-party SSL that provides the https service. Many types of attacks are not encrypted, but mimic an encrypted page. Thus, one should always check that the web page is truly encrypted (Warren, 2005). Be mindful that some of these sites may appear to be legitimate, but are false, as depicted below.

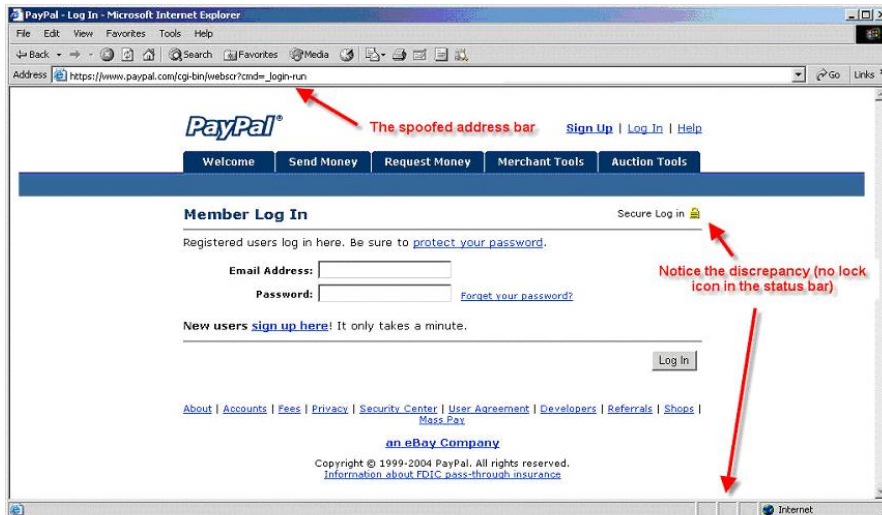


Figure 2.5 – Example of an Insecure Website (It looks secure, but is not.)

Adapted from Berghel, (2006).

5. **Education** – Education is key for the prevention of future incidents. The Internet boasts a lot of valuable information that individuals can use for education, and in so doing, can prevent the pain and economic hardship of becoming a victim of identity theft.

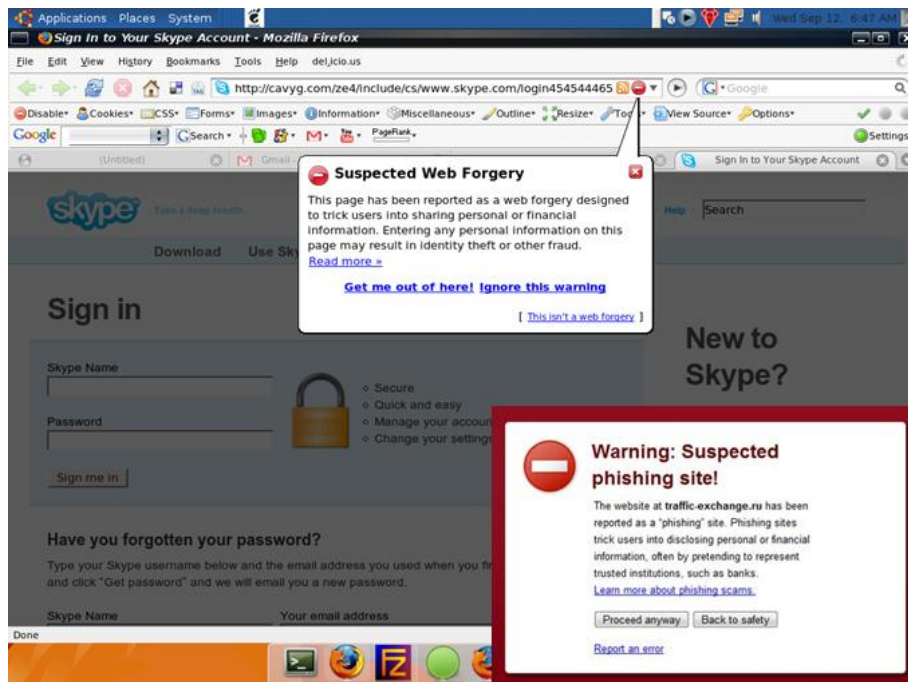


Figure 2.6 – Awareness Creation on the Internet

Adapted from Atwood, J (2007). Phishing : The Forever Hack.

The above figure shows some of the information that one can use to identify these bogus websites. If receiving spam that requests information, forward it to the Anti-Phishing Working Group (Emigh, 2005).

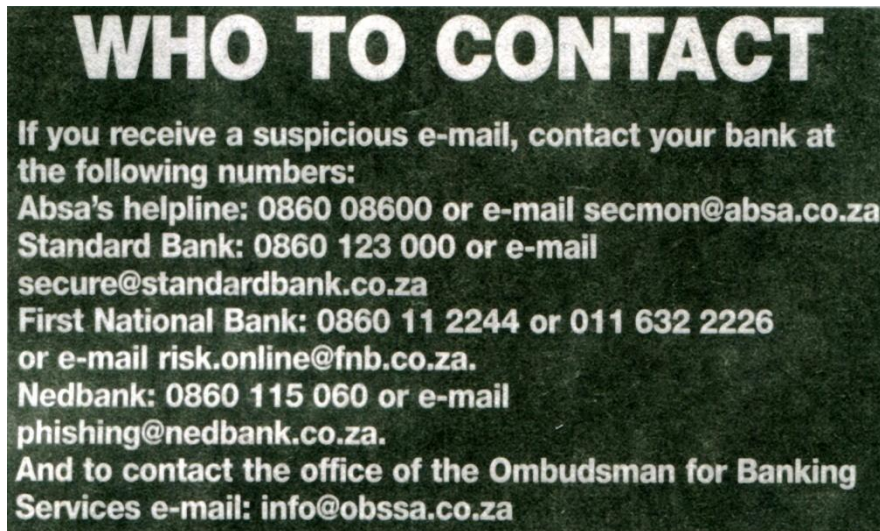


Figure 2.7 – Further Awareness Creation Through Print Media

Adapted from Cole, (2010).

6. **Using the Security Analysing Feature in Microsoft** – This can be used so that all patches are updated. This free tool can be downloaded from Microsoft's website. By keeping the computer patched, it will protect one's system against known exploits that could be incorporated into Internet Explorer, Outlook, and Outlook Express (Warren, 2005).

7. **Use a Firewall** – The use of a firewall can prevent damage through malicious code that can be entered into one's computer. Some operating systems have built-in firewalls that can be adopted. Whilst a firewall is no guarantee that it will prevent scam emails entering a mailbox, it may offer some protection to attachments that may have viruses. When a firewall detects any suspicious activity, this could imply that one has unknowingly already installed a virus. A desktop (software) and network (hardware) firewall is recommended (Warren, 2005).

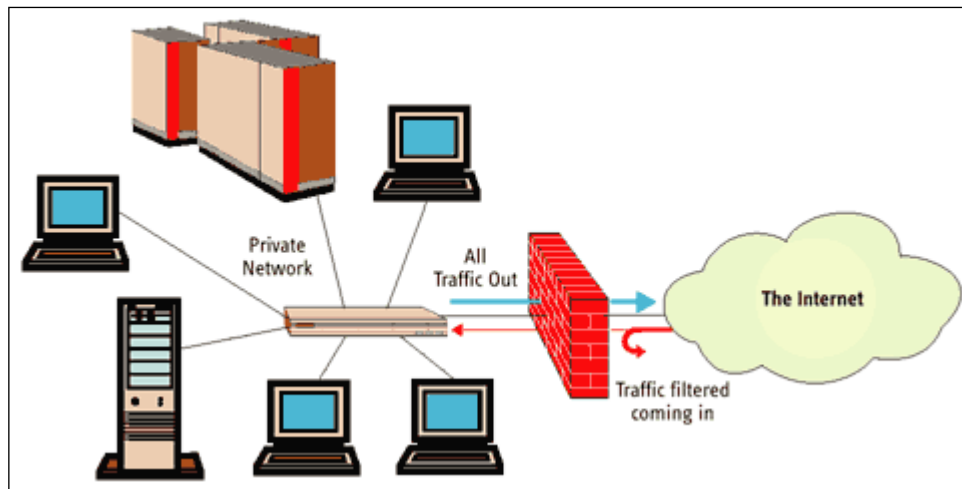


Figure 2.8 – Concept of a Firewall

Adapted from Bajaj, (2006).

8. **Always Create a Backup of Your System** – It is essential to create regular backup of one’s information and to take screenshots of system structure. This will enable one to restore the information to its original form if subjected to a phishing attack, either through spyware or malware. There are various applications that can achieve this backup, but tools such as Symantec Ghost and Acronis True Image are perfect for this (Warren, 2005).

9. **Do Not Enter Sensitive or Financial Information Into Pop-up Windows** – Bogus pop-up windows are a commonly used method adopted by phishers to lure users to fake websites. These windows are activated when users click on to the embedded link in deceptive emails. Phishers are extremely clever in that they are also capable of positioning these windows in front of a legitimate website, thereby convincing users that this pop-window is valid. Avoid entering sensitive information into any pop-up window, no matter how secure it may look. Note that there is no way to look at the security certificate of a pop-up window. Users should immediately click the X of the pop-up window (top right hand corner) and not click “cancel”, because doing the latter may still send users to a false webpage where malware can be downloaded onto one’s machine (Warren, 2005).

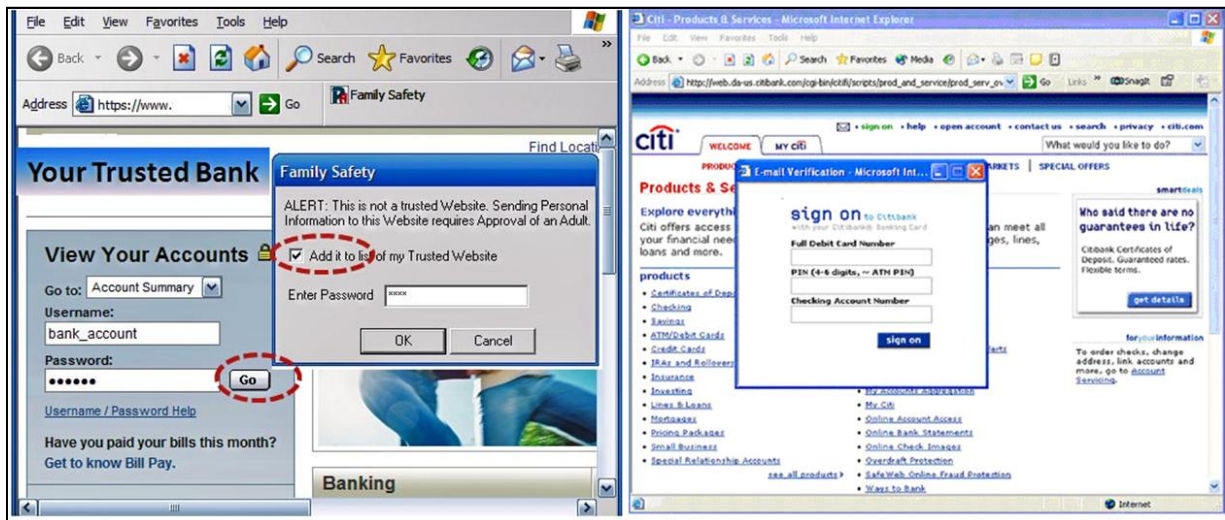


Figure 2.9 – Example of Two Different Pop-Up Windows

Adapted from Fraudwatch International - Education on Phishing website methods (2010).

10. **Host File Security** – A phisher is capable of compromising the host file on a workstation resulting in the user being redirected to a fraudulent website. It is crucial to configure the host file status to “read-only”. By doing this, phishers are not able to manipulate its status. Solid protection, however, involves a properly configured firewall that would prevent phishers from interfering with one’s machine, thereby ensuring the safety thereof.

11. **Protection Against Pharming Attacks** – This type of phishing attack does not annoy individuals with spam, but silently attempts to poison the Domain Name System server. This attack causes all web requests to be redirected to a different website that mimic the one to be visited. For example, the user may type in eBay’s web address, but the poisoned DNS server will redirect the user to a fraudulent site. This is considered to be new-age phishing, and needs to be controlled by an administrator experienced in the use of modern security techniques to lock down the company’s DNS servers (Warren, 2005).

12. **Email Client Configuration:** According to Warren (2005), careful configuration of your email client is essential so that one is less susceptible to deceptive phishing emails. There are many ways to achieve this. A simple example would be to configure one’s email

software in such a way that views are based on “text only”, as this will protect an individual from potential scams that utilise HTML.

13. **Understand the Organisations Email / Information Technology Policy:** Organisations transacting online generally have clear policy guidelines that dictate how their business will be conducted. The most common characteristic is that no organisation will send you an email, as a client, to update account details on the website and provide a link in the email for the user to click on to. Being familiar with such policies will help you detect and avoid such phishing and / or other scams. Encryption is safe, and one should always ensure that sending sensitive information is done via an encrypted email (Sorkin, 2006).

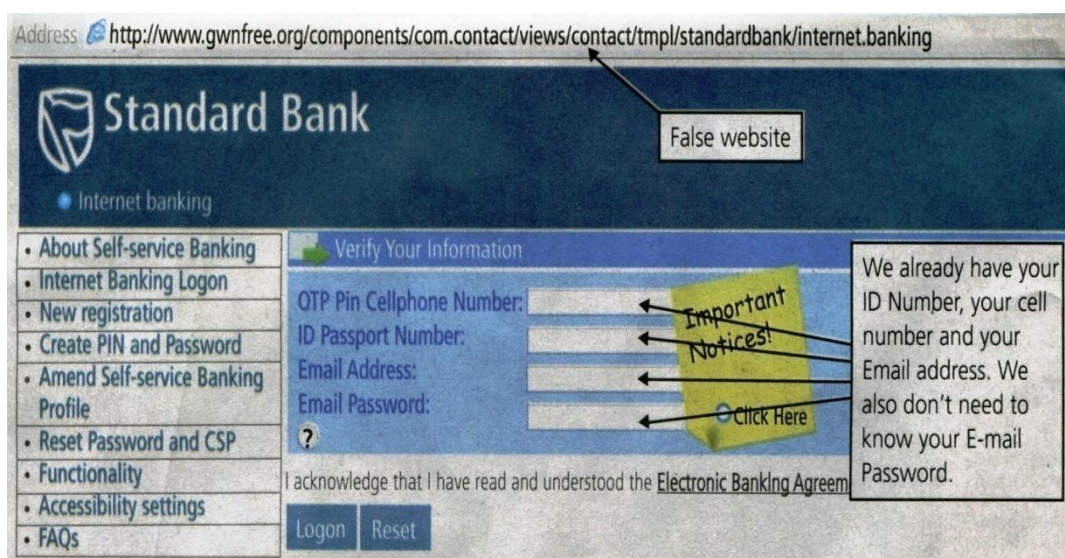


Figure 2.10 – Example of a Phishing Website Requesting Superfluous Information

Adapted from Cole, (2010).

14. **All Email Attachments Must be Treated With Caution:** Hackers tend to use email attachment as a vehicle to deliver a virus on to a machine. As alluded to earlier, the virus can cause serious damage, ranging from stealing personal information, to compromising the integrity of the system. It could open the system to abuse, whereby the machine may be used as a “bot” for “denial-of-service” and other online crimes. Familiar website addresses are not a guarantee of safety, due to chromeless windows. Similarly, a valid email address is also not a guarantee of safety either. Some viruses actually interrogate the recipient’s address book and duplicate valid addresses, thereby creating doubt in the end user, as an email may come from a valid friend’s email address (Warren, 2005).

15. Unsolicited email must be treated with suspicion: Basic rule of thumb – if one does not know the sender, or the address looks suspicious, delete it immediately without opening the email. The most important lesson is never click on to an embedded link found in an email. Fake links are very carefully designed by hackers, which redirect individuals to bogus websites where private information is divulged or malware, or even viruses, are downloaded on to one's machine unknowingly. Simple applications are designed by spammers that monitor the commonly used links on their servers, and using this information, the hackers are able to target victims who fall for repeated spam attempts.

2.9 Electronic Mail Security

Phishing emails are crafted to look as if they've been sent from a legitimate organisation. These emails attempt to fool one into visiting a bogus website, which looks like the real thing, to either download and install malicious code (viruses and other software intended to compromise one's computer) or disclose information of a personal nature.

A common case involves users receiving deceptive emails, with the subject being a problem with your account, requesting unsuspecting users to attend to the query. The email looks genuine, and appears as though it has been sent from a major financial institution. The message will claim that there is a "Problem with one's bank account", and in order to validate the account, one must complete an online form that will appear once the user clicks on to the link (Recognising and avoiding...1998). Doubt is obviously created when users who are clients of a bank, receive such an email, and unsuspectingly click on to the false link which then redirects them to the fake website. The email is obviously sent as spam to many recipients, even if you do not bank with that institution, and this should immediately warn individuals.

2.9.1 An Example of a Phishing Mail

If HTML is used as your default email view setting, then the visible link may be that of the actual institution, thus creating confidence, but in fact, the actual coded link within HTML redirects the user to the fraudulent site. An example of the above:

Visible link: <http://www.standardbank.com/accounts/>

Actual link to bogus site: <http://itcare.co.kr/data/standardbank/index.html>

The fake site looks extremely similar to the real one, and will present an online form asking for information such as your account number, your address, your online banking username and password – all the information a hacker needs to steal your identity and raid your bank account. Figure 2.11 shows an example of an email that should be treated with caution, as it displays multiple characteristics of a typical phishing attack.

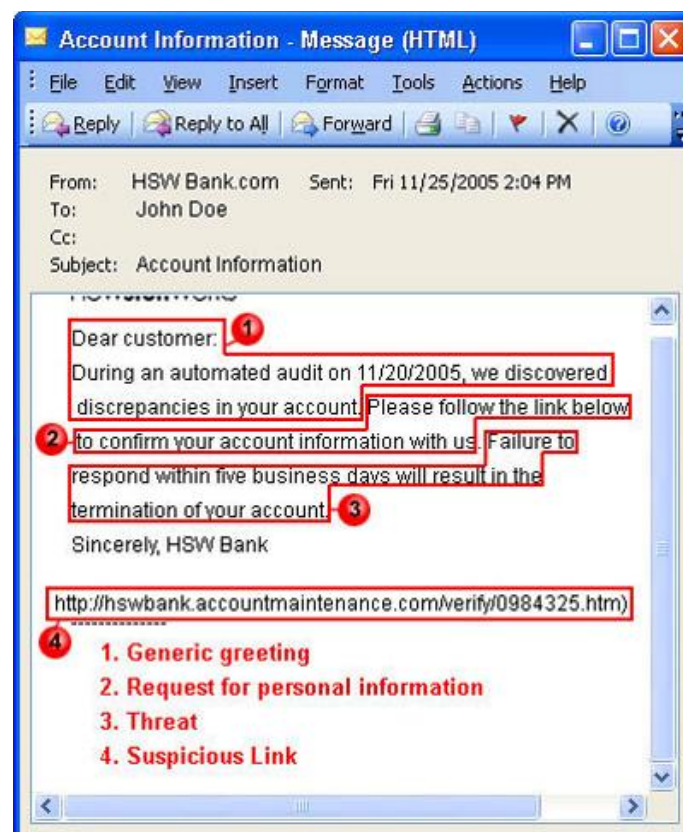


Figure 2.11 – Example of a Deceptive Email that Must be Treated with Caution

Adapted from Wilson, (2005).

2.9.2 Common Misconceptions / Myths about Email Security

According to Dong-Her, Hsiu-Sen, Chun-Yuan, and Lin (2004), it is surprising that many managers fear email virus threats, but lack a comprehensive understanding of the risks and controls related to various security technologies. The following are the most commonly associated misconceptions when it comes to email and the Internet.

1. **Myth 1 – I’m not opening the email attachment, so my email is safe.** Individuals may not understand that when receiving email, their computer could be infected with a virus even if they do not open the attachment. “MELISSA” and “LOVELETTER” are examples of email viruses that infect one’s computer as soon as the emails are opened.
2. **Myth 2 – I use a wireless connection, so my email is safe.** It is true that when using a wireless connection, individuals are assigned a different Internet protocol address each time they connect, making it harder to find your computer and browse your contents. Some Trojan email viruses (e.g. FEVER and TROODON) are independent of Internet protocol addresses, and therefore, there are no security guarantees through wiring and network environments. Individuals who stay connected for long periods are especially at risk of being “Trojaned”.
3. **Myth 3 – I use an anti-virus application, so my email is safe.** Anti-virus software can protect a computer from email viruses, but may not protect it from newer, just-released viruses. In addition, anti-virus software will offer no protection against hackers.
4. **Myth 4 – I use a firewall, so my email is safe.** Firewalls do provide added security, but they do not provide protection against email viruses or protection for an unsecured computer.

Dong-Her *et al.* (2004) advocate that although understanding these myths can help in correcting mistakes, managers and individuals must also be familiar with general email protections. It is crucial that managers understand some of the protection aspects that may be required in the typical office environment.

2.10 Summary

The authors of the extensive literature reviewed for the purposes of this study all concurred that Internet phishing is a serious issue, and as such, has to be addressed. The literature included here described phishing trends and the ammunition they use, as well as some of the protection available to online users.

The next section of this study outlines the research methodology used to examine how aware participants of this survey were regarding the problem of Internet phishing.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on how the study was investigated. It outlines the sampling methods used, data-gathering instruments and the statistical techniques utilised to satisfy the objectives of this study. The sample for this study was drawn from various sectors of the employment spectrum, but all participants were based and employed in Durban, KwaZulu-Natal. The measurement instrument used was an online questionnaire comprising 19 questions. Even though a fair amount of research has already been conducted into the field of Internet security and on Internet phishing, the problem is still very topical. Whilst a level of awareness has been created, it is clearly insufficient, given the alarming rate at which the public fall prey to scams.

3.2 Aim and Objectives of the Study

Internet phishing attacks are currently on the increase, yet there has been no significant decline in users falling prey to this problem. Many users are unaware of this threat, and cannot identify the symptoms thereof. Even though a fair amount of literature has been published on the topic, as evidenced in Chapter 2, awareness levels are still very low.

To reiterate the objectives of this study, the researcher aimed to:

- Determine the level of awareness of phishing amongst online users in Durban;
- Determine what preventative systems can be adopted by organisations to minimise the threat of this problem;
- Determine the characteristics of a potential scam; and
- Based on the findings of this research, provide a platform to be used in implementing an awareness programme that thwarts phishers' underhanded and criminal activities.

3.3 Data Collection Strategies

For purposes of this study, an online self-completed questionnaire was considered an appropriate data-gathering instrument. The questionnaire comprised 19 questions that varied in terms of question type.

A self-completed questionnaire has many benefits associated with its use. For instance, it is relatively quick to administer; is free from the interviewer effect; and is convenient for the participants.

Bramble and Mason (1989) state that questionnaires are very similar to interviews. However, with interviews, items are administered and someone else records the responses, whereas with a questionnaire, the items are merely administered and the respondent records his/her opinions. The questionnaire format offers certain advantages over the interview. Specifically, a larger sample can be reached more economically, and greater anonymity can be provided to the respondents. The first advantage, namely a bigger sample, ensures that data can be generalised, whilst the second results in people being more willing to respond openly and honestly to the questions.

Questionnaires do, however, have disadvantages. The main problem relates to the issue of non-response to certain items in the questionnaire. In addition, participants could fail to return questionnaires (with the conventional administration method), which makes it difficult to generalise from a sample to a population. White (2000) stated that if questionnaires are not returned, then a follow-up reminder letter to respondents is a good idea; the letter should re-emphasise the importance of the study, and enclose another stamped addressed envelope with a copy of the questionnaire. This method was applied to the survey, albeit in the form of follow-up emails.

The participants were approached in their personal capacity and were informed of the purpose and objectives of this study; assured of their anonymity and the confidentiality of the information they provided; and advised of their right to withdraw from participating in this research.

Each participant was emailed a link that opened the online questionnaire; a covering letter stating the purpose of the research and the ethical considerations of confidentiality and anonymity of participants formed part of the introduction of the online questionnaire. In order to ascertain the actual awareness level of each participant, he or she was requested to reply honestly, and without the assistance of any other person. This restriction was to minimise any potential distortion of the results due to the influence of a third party.

The researcher used “closed-ended” questions in the questionnaire. Bryman and Bell (2007) stated that open-ended questions present both advantages and disadvantages to the researcher, but, due to problems related to the processing of answers, using closed-ended questions is more common.

According to Bryman and Bell (2007), the advantages of using closed-ended questions are:

- They are relatively easy to analyse. Every answer can be assigned a number or value so that a statistical interpretation can be formulated.
- They are also well suited for computer analysis. If open-ended questions are analysed quantitatively, the qualitative information is reduced to coding, and answers tend to lose some of their initial meaning. Because of the simplicity of closed-ended questions, this does not pose a problem.
- They are specific, thus communicate meaning consistently. Because open-ended questions allow respondents to use their own words, it can be difficult to compare the meanings of the responses.
- In large-scale surveys, they are not overly time-intensive for the interviewer, the participant and the researcher, and using closed-ended questions presents an inexpensive survey method.
- Using them in surveys results in a higher response rate than using open-ended questions.

A pilot study was conducted amongst 10 colleagues to ascertain the usability and clarity of the questions in the questionnaire, and to ensure that there were no misleading or ambiguous questions. White (2000:51) stated, “With all questionnaires it is essential that a pilot is carried out with a small number of volunteers”. Whilst nine of the respondents were happy with the questionnaire and its associated terms and conditions, one respondent was totally against the fact that one needed to check the “I agree” box before proceeding to the questionnaire, and, on principle, opted not to be part of the actual survey. The participants in the pilot study were similar to the people in the sample.

The data was collected over a two-month period. The questionnaire would have taken respondents approximately seven minutes to complete and the participants were requested to complete the questionnaire at their convenience. Reminder emails were sent approximately two weeks after the original “invitation to participate” followed by a second reminder

approximately two weeks thereafter. At the end of the two-month data collection period, all of the “raw data” was exported from QuestionPro.com to be analysed.

3.4 Research Design and Methods

Cooper and Schindler (2003) defined research design as providing the basic direction for carrying out a research project to obtain answers to research questions.

The research method adopted for this study was the online survey questionnaire method and the study was based on a quantitative research design. Quantitative research “is a research strategy that emphasises quantification in the collection and analysis of data” (Bryman and Bell, 2007:28). Bryman and Bell (2007:154) stated that “Quantitative research is a distinctive research strategy, described as entailing the collection of numerical data and as exhibiting a view of the relationship between theory and research as deductive, a preference for a natural science approach, and as having an objectivist conception of social reality.” According to Hair *et al.* (2001), the goal of quantitative research is to provide specific facts decision-makers can use to:

- Make accurate predictions about relationships between market factors and behaviours;
- Gain meaningful insights into those relationships; and
- Verify or validate the existing relationships (Hair *et al.*, 2001).

In this study, quantitative research provided the means to arrive at a comprehensive understanding of a user’s awareness of the problem of Internet phishing.

According to Smailes and McGrane (2000), by using this technique, the acquired data is “measured, counted or quantified” providing numerical measurements. In contrast, qualitative data “consists of attributes, labels or non-numerical entries” (Larson and Farber, 2006). Qualitative research usually “emphasises words rather than quantification in the collection and analysis of data” (Bryman and Bell, 2007:28).

According to Bramble and Mason (1989:258): “Researchers in education and the behavioural sciences measure constructs such as achievement, personality, aptitude and ability, behavioural tendency, interests and values. Researchers generally prefer utilising existing measurement instruments. However, if no existing ones are appropriate, researchers will

construct instruments to meet their needs, using a plan such as a table of specifications. In addition, they will necessarily determine the reliability and validity of their tests.”

3.4.1 Population

According to Polit and Hungler (1991), the population of a study area encompasses the total collection of elements about which the researcher can make some inferences. The target population for this study consisted of online users in Durban, KwaZulu-Natal. Based on the target population’s responses, the researcher attempted to draw conclusions and generalisations therefrom.

A sample population (500 online users) was selected to participate in this research. This group comprised users in various hierarchical levels in numerous organisations, ranging from junior to senior members of staff, with a prerequisite being that they all had access to the Internet. All participants were selected on a referral basis, and all consented to participating in this study. A total of 314 participants attempted the survey, and 228 completed the survey within the data collection period. The latter figure represents a response rate of 73 %.

3.4.2 Sampling

Bramble and Mason (1989) defined sampling as an act of drawing a sample from a population. According to Cooper and Schindler (1998), a sample is carefully selected from the target population in order to represent that population or elements thereof, thus allowing the researcher to make conclusions about the entire target population. The sample is usually considerably smaller than the population under study, though in the case of a relatively small population, the sample size may be similar to that of the target population. Bramble and Mason (1989) stated that a sample must be large enough to provide fairly accurate estimates of the parameters of interest, and should also be representative of the population being studied and not of some atypical, or biased, part of it.

3.4.2.1 Sampling Design

White (2000) stated that there are two methods of choosing samples: random (probability) sampling and non-random (non-probability) sampling. Random sampling works best with a very accurate and up-to-date sampling frame, and is the preferred method to carry out any form of statistical analysis. There are three main ways to use non-random sampling: cluster sampling, quota sampling and purposive sampling.

The sampling design that was considered appropriate for the present study was probability sampling, as the researcher only selected those participants with access to the Internet and email. The respondents were first asked if they had access to the Internet and only if they agreed to participate in the survey, then their details were captured.

3.4.2.2 Considerations regarding Sampling

Even though a random sample will most likely provide a true cross-section of the population, this might not be the sole objective of the research. Cooper and Schindler (2003:74) stated: “If there is no need to generalise to a population parameter, then the non-probability sampling method can be employed.”

3.4.2.3 Sample Size

The most important factor in determining the size of the sample for estimating the population parameter is the size of the population variance. The greater the dispersion of the variance in the population, the larger the sample must be to provide the estimate precision (Cooper and Schindler, 2003). Krejcie and Morgan (1970) stated that if the population is 100 000, then 384 surveys are required to be administered. According to Bryman and Bell (2007), the decision about the sample size is not straightforward, as it depends on a number of considerations, and there is no one definite answer. Moreover, most decisions on sample size are affected by considerations of time and cost. Invariably decisions about sample size represent a compromise between the constraints of time and cost, the need for precision, and a variety of further considerations, that will now be addressed.

Although the ideal sample size was intended for 400 users, 500 questionnaires were actually administered. Of the 314 participants who attempted the survey, 228 completed responses were received by the end of the data collection period. As mentioned earlier, this represents a 73 % response rate of those who attempted the survey.

3.4.3 Reliability and Validity / Statistical Technique

Reliability refers to the consistency of a measure for a concept (Bryman and Bell, 2007). The three most prominent factors involved in the consideration of the reliability of a measure are stability, internal reliability and inter-observer consistency. “One of the most popular reliability statistics in use today is Cronbach's alpha. Cronbach's alpha determines the internal

consistency or average correlation of items in a survey instrument to gauge its reliability” (Santos, 1999). This test indicates whether the results of the research are consistent and therefore repeatable. When results are computed, the test provides a coefficient that varies between 0 and 1. A score of 1 denotes perfect internal reliability and 0 denotes that there is no internal reliability. According to Bryman and Bell (2007), a figure of 0.80 is typically used to denote an acceptable level of internal reliability.

Validity refers to whether or not an indicator, or set of indicators, devised to gauge a concept, really measures that concept. It should be noted that although reliability and validity are analytically distinguishable, they are related because validity presumes reliability (Bryman and Bell, 2007).

3.5 Analysis of Data

The data resulting from the questionnaire was exported from QuestionPro.com for further analysis with SPSS software. The following statistical techniques/measures were utilised during this analysis phase, and a brief overview is included hereunder:

- Percentages;
- Frequency Distribution;
- Measures of Central Tendency;
- t – test
- Measures of Dispersion;
- Correlation; and
- Regression Analysis.

Percentages provide information on the ratio of respondents within each of the biographical variables, an example being the proportion of males compared to females participating in the study. Histograms and bar charts are commonly used to display these intervals.(Cooper and Schindler, 2003:93).

A Frequency Distribution can be described as a tabular arrangement of data, in which the data is grouped into different intervals. The number of observations associated with each interval

is determined and summarised in what is known as a frequency table (Bryman and Bell, 2007).

“Measures of central tendency encapsulate in one figure a value that is typical for a distribution of values. In quantitative data analysis, three different forms of averages are recognised” (Bryman and Bell, 2007, p. 359). These are the arithmetic mean, the median and the mode. “This is the most familiar measure of an ‘average’. Up to now, it was probably the first measure that one would have considered on being asked to find the average of a set of data. The mean is found by adding up all the values of the variable and dividing by the number of values, which is used as the measure of central tendency.” (Bedward, 1999:119)

Standard deviation is used as a measure of dispersion to analyse the amount of variation in each data set (Bryman and Bell, 2007). It is a measure of variation based on all the observations in a set of data rather than on just two values, which is the case for both the range and the inter-quartile range. The standard deviation measures the spread around the mean (Bedward, 1999:131).

Regression analysis is a “search for variables that influence a dependent variable” (Nieuwenhuis, 2009). This tool allows the researcher to “predict values of the dependent variable from one or more independent variables” (Field, 2005). Bramble and Mason (1989:172) stated, “In behavioural research situations it is often useful to conduct prediction or estimation studies. In prediction, current characteristics are used to identify scores at a future time. Estimation involves identification of a present attribute from other traits or scores.”

3.6 Summary

The primary objective of this chapter was to describe the methodology employed in conducting this study. In essence, it outlined the research and sampling design, data gathering procedure and the statistical techniques that were employed to answer the research questions.

Chapter 4 presents the statistical variables, some of which include the frequency distribution, measures of central tendency, measure of dispersion, correlation and analysis of variance.

CHAPTER FOUR

PRESENTATION OF RESULTS

4.1 Introduction

As discussed in Chapter 3, the main aim of the study was to identify the awareness levels of online users in Durban about Internet phishing. The raw data from the online questionnaire was extracted from QuestionPro.com and was imported into SPSS 15 so that further analysis could be undertaken. The results of this analysis are presented by means of tables and graphs in this chapter, and the interpretation of the results is discussed in Chapter 5.

4.2 Demographic Profile of Respondents

The questionnaire was distributed to both male and female participants, and the demographic composition of the sample is reflected in Table 4.1.

Table 4.1 – Distribution of Respondents in Demographic Groupings

DESCRIPTION		PERCENTAGE %
Gender	Male	62 %
	Female	38 %
Race	Indian	44 %
	White	33 %
	Black	19 %
	Coloured	4 %
Age	Under 25	6 %
	25 - 34	32 %
	35 - 44	36 %
	45 - 54	16 %
	Over 55	10 %

From Table 4.1, it is clear that almost two thirds (62 %) of the respondents were male. The race group most represented was the Indian group (44 %), followed by the White group (33 %) and then the Black group (19 %). The Coloured group was the smallest (4 %). In terms of the age breakdown, it can be seen that more than two thirds (68 %) of the respondents were between 25 and 44 years old and only 6% were younger than 25 years of age.

4.2.1 Cross-tabulation of the Demographic Data

A cross-tabulation was then undertaken between race and age against gender to understand if any significant conclusions can be made. The reason for using cross-tabulations is that it gives the reader a better understanding of the analysis. The result of this analysis is reflected in Table 4.2.

Table 4.2 – Cross-Tabulation between Race, Age and Gender

DESCRIPTION		GENDER	
		Male	Female
Race	Black	49 %	51 %
	Coloured	33 %	67 %
	Indian	65 %	35 %
	White	69 %	31 %
Age	Under 25	46 %	55 %
	25 - 34	56 %	44 %
	35 - 44	67 %	33 %
	45 - 54	57 %	43 %
	Over 55	78 %	22 %

Further analyses were subsequently conducted based on the cross-tabulations of the above variables. The diverse element of the race and age grouping is highlighted in this sample. Table 4.2 illustrates that the male group predominantly contained Indian and White respondents, while the female group comprised mostly Black and Coloured respondents.

Table 4.2 also depicts that the over 55 group was predominantly male. The under 25 group was the only one in which the proportion of female respondents was larger than that of male respondents. Following the analysis of the demographic information depicted above, a frequency analysis was conducted on the remaining 16 questions, which dealt directly with the subject matter. Each question and the results of the analysis are presented in the subsequent pages of this chapter.

4.2.2 Internet Usage

Analysis was subsequently conducted to investigate the number of respondents who utilised the Internet, and the reasons for them using the Internet. From the data collected, 99 % of the responses used the Internet, and the reasons for their usage are illustrated in Figure 4.1.

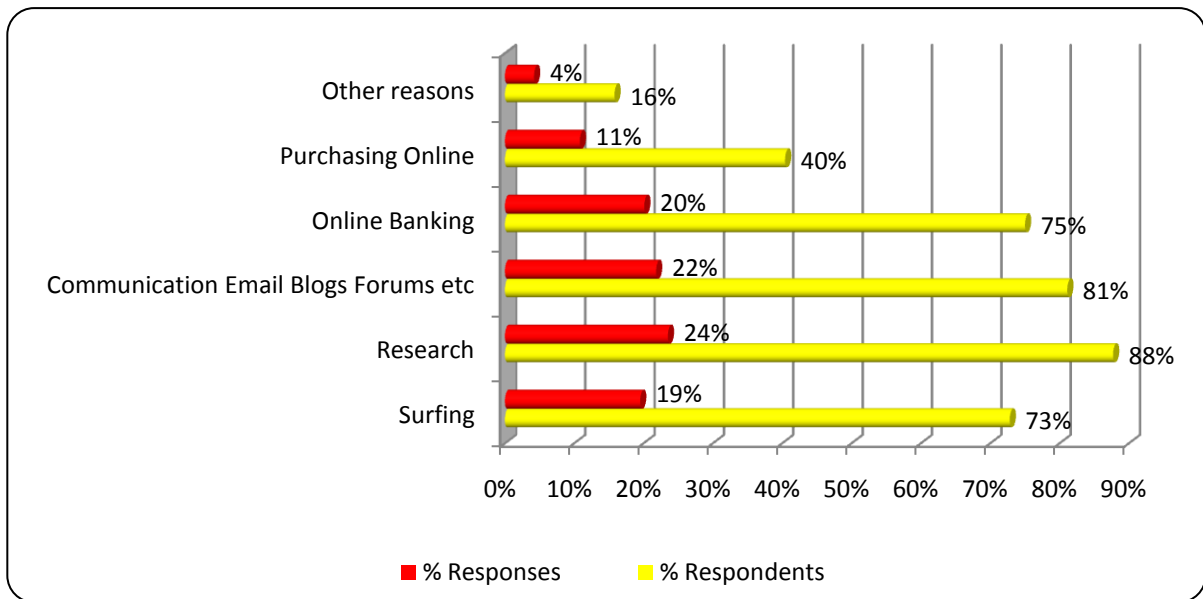


Figure 4.1 - Reasons for Internet Usage

The analysis revealed that 228 respondents selected 850 possible responses, indicating that, on average, respondents participated in between 3 and 4 ($m = 3.7$) different types of Internet activities.

Figure 4.1 shows that the Internet usage with the highest frequency of responses was research (24 %). This usage was also *cited* by the largest proportion of respondents (88 %). The least popular was purchasing online with 40 % of the respondents having selected it. This activity makes up 11 % of the total number of responses.

4.2.3 Internet Phishing Awareness

A cross-tabulation was conducted on the concept of Internet phishing in terms of the strategies used to counteract the problem, including the consequences of being a victim. The results are shown in Table 4.3.

Table 4.3 – Awareness Levels and Victims of Internet Phishing

DESCRIPTION		PERCENTAGE
Have you heard of the concept of Internet phishing?	Yes	85 %
	No	15 %
	Total	100 %
My understanding of the term Internet phishing	It is a method of acquiring personal information from me over the Internet	77 %
	It is a method of acquiring information data from my computer	18 %
	I am always at risk as long as my Internet protocol address is available	5 %
	Total	100 %
My strategy to counteract the problem	I am aware of the problem and very cautious when using the Internet	37 %
	I have technology that protects me	27 %
	I do not disclose any personal information over the Internet	26 %
	I use the Internet and just hope that I am not a victim of Internet phishing	8 %
	I am not at threat because I do not do any transactions over the Internet	2 %
	Total	100 %
Have you been a victim of Internet phishing?	Yes	12 %
	No	88 %
	Total	100 %
As a victim of Internet phishing, I was affected in this way	My computer downloaded a virus and crashed my system	69 %
	Purchases were made on my credit card	25 %
	My bank account was cleaned out before I suspected anything	6 %
	Total	100 %

Table 4.3 shows that 85% of the respondents knew about Internet phishing. It also shows that 77 % of the respondents who knew about Internet phishing, and offered a response to this question, believed it is a method of acquiring personal information. Table 4.3 illustrates that 37 % of the respondents who knew about Internet phishing and responded to this question felt that they were aware of the problem, and were therefore very cautious when using the

Internet. The data showed that of the respondents who knew about Internet phishing, 88% offered a response to this question and had not been a victim.

Only 14 of the 22 respondents who reported that they had been victims of Internet phishing indicated what had happened to them. These 14 respondents recorded 16 of the possible responses, indicating that, on average, respondents had experienced between 1 and 2 ($m = 1.14$) types of malicious symptoms of Internet phishing.

The largest proportion of respondents who had fallen prey to Internet phishing, reported that a virus had crashed their computer system. This consequence was also the most frequently reported (69 %) as seen in Table 4.3. None of the respondents had had their identities stolen or used to open retail accounts.

4.2.4 Internet Phishing Characteristics

Analysis was then conducted to understand what respondents perceived to be the common characteristics of an Internet phishing. The results are shown in Figure 4.2.

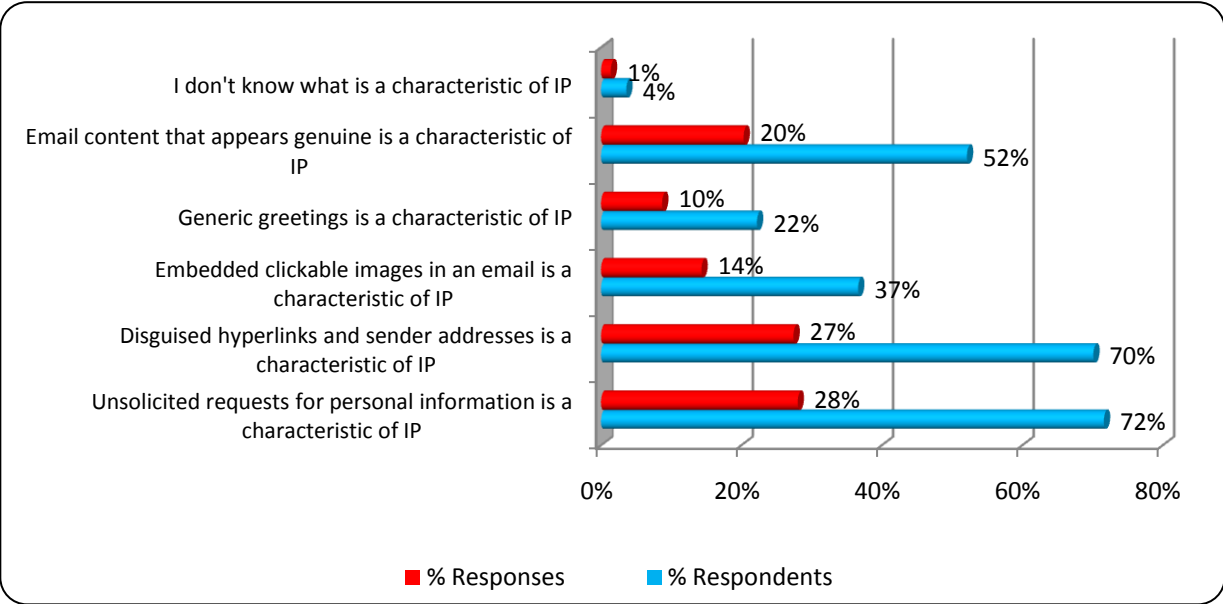


Figure 4.2 – What are the Common Characteristics of Internet Phishing?

Analysis based on Figure 4.2 illustrated that 194 of the respondents gave their opinion on which of the listed characteristics are that of Internet phishing, and a total of 497 responses were generated. Thus, on average, each of these respondents selected between 2 and 3 ($m=2.55$) different characteristics of Internet phishing. Figure 4.2 depicts that the characteristics selected by the largest proportion of respondents are unsolicited requests for

personal information (72 %) and disguised hyperlinks and sender addresses (70 %). These characteristics were also the most frequently selected responses, 28 % and 27 % respectively. To determine the awareness levels of Internet phishing, a tabulation was done using the role of Internet service providers, preferred methods of communication, and literature to which one was exposed. The results of this analysis are shown in Table 4.4.

Table 4.4 – Information About Internet Phishing Awareness

DESCRITPION		PERCENTAGE
Have you read any literature newspaper emails journals or books on Internet phishing	Yes	68 %
	No	32 %
	Total	100 %
Which of the following statements best describes your awareness of the problem?	I knew about Internet phishing and the article just made me more wary	70 %
	It was the first time that I was exposed to the problem	11 %
	I circulated the article so that others could be made aware of it.	11 %
	I knew about Internet phishing and did not bother to read the article	8 %
	Total	100 %
Internet Service Providers must advise prospective subscribers about Internet phishing before they subscribe	Strongly Agree	58 %
	Agree	33 %
	Strongly Disagree	6 %
	Disagree	3 %
	Total	100 %
What would be your preferred method of communication about Internet phishing?	I would prefer to be informed via Popup Ads on my Internet Browser	27 %
	I would prefer to be informed via Newspaper Articles	25 %
	I would prefer to be informed via Television coverage	25 %
	I would prefer to be informed via Pamphlets at Banking or retail outlets	23 %
	Total	100 %

Table 4.4 illustrates that more than two thirds (70 %) of the 141 respondents who have encountered literature about Internet phishing knew about the problem and the literature made

them more wary about it. A high 32% had not read any literature on Internet phishing and this could imply the awareness levels are relatively low.

Table 4.4 also shows that 91% of the respondents were in agreement, and believed that Internet service providers have a responsibility to advise prospective customers of the dangers of Internet phishing before they subscribe. It was also determined that 200 of the respondents indicated which communication method they would prefer, and 405 responses were generated. Thus, on average, each of these respondents selected 2 ($m = 2.03$) different communication methods.

In terms of the preferred communication methods, all were reasonably popular, with pamphlets at banking or retail outlets being the least popular, and popup adverts on their Internet browser being the most favoured. Popup adverts made up 27 % of all the responses and was selected by 55 % of the respondents, while pamphlets accounted for 23% of the responses, and was selected by 47 % of the respondents.

In order to ascertain the level of understanding of Internet security, a series of questions were posed to the respondents. The analysis started off by trying to see if respondents had heard of the concept of Internet security, and immediately delved further to establish exactly what users' understanding of Internet security was. Because Internet security is crucial, questions were further posed in terms of secured versus unsecured websites, seeing that this becomes the foundation for financial institutions that encourage users to perform online banking.

The results of the analysis are tabulated in Table 4.5.

Table 4.5 – Understanding the Concept of Internet Security

DESCRIPTION		PERCENTAGE
Do you have Internet security installed on your computer?	Yes	93 %
	No	3 %
	I don't know	4 %
	Total	100 %
Internet security installed on my computer	I have Anti-Virus Software installed on my computer	30 %
	I have a Firewall installed on my computer	20 %
	I have all of the above installed on my computer	15 %
	I have Anti-Spyware installed on my computer	14 %
	I have Active Security Updates installed on my computer	13 %
	I have Anti-Phishing Software installed on my computer	7 %
	I don't know which security products are installed on my computer	1 %
	Total	100 %
The products listed in question 17 are sufficient to combat the threat of Internet phishing	Agree	56 %
	Disagree	34 %
	Strongly Agree	6 %
	Strongly Disagree	4 %
	Total	100 %
All secured websites denoted by https are safe from phishing scams	Disagree	53 %
	Agree	31 %
	Strongly Disagree	13 %
	Strongly Agree	3 %
	Total	100 %

Table 4.5 shows that 93% of the respondents had some form of Internet security installed on their system. Further, 190 of the 191 respondents who had some form of Internet security on their system indicated which listed security facilities were installed on their systems, and they generated 412 responses. Thus, on average, each of these respondents had 2 ($m = 2.17$) different security facilities installed.

The analysis also depicts that almost two thirds of the respondents had Anti-Virus Software installed on their systems, and these made up 27 % of the total number of responses. The second most popular security option was a Firewall, with 44 % of the respondents indicating that they had one installed, and these responses made up 20 % of the total. Only a few respondents (16 %) had Anti-Phishing Software installed on their computers.

The results further showed that almost 40 % of the respondents did not think that the listed security options were sufficient to combat the threat of Internet phishing. It was also noted that two thirds (66 %) of the respondents did not believe that all secured websites, denoted by <https://>, are safe from phishing scams.

4.3 Measures of Central Tendency and Dispersion

The measures of central tendency and dispersion (arithmetic mean and standard deviation) for the responses received to each of the statements are reflected in table 4.6.

Table 4.6 – Mean, Standard Deviation and Variance of Question / Statement

	Question or Statement that was asked	Mean	Standard Deviation	Variance
1	Gender	-	-	-
2	Race.	-	-	-
3	Age	-	-	-
4	Do you use the Internet?	1.00	0.07	0.00
5	If you have answered “Yes” to question 4, what do you use the Internet for?	2.92	1.42	2.03
6	Have you heard of the concept of Internet phishing?	1.17	0.38	0.14
7	If you answered “Yes” to question 6 above, which of the following statements best describes your understanding of the term?	1.34	0.74	0.55
8	If you answered “Yes” to question 6 above, which of the following strategies do you use to alleviate the problem?	3.22	1.26	1.59
9	Which of the following, in your opinion, are common characteristics of Internet phishing?	2.76	1.58	2.50
10	If you answered “Yes” to question 6 above, have you been a victim of Internet phishing?	1.88	0.32	0.10
11	If you answered “Yes” to question 10 above, how were you affected?	3.56	0.81	0.66
12	Have you read any literature (newspaper, emails, journals or books) on Internet phishing?	1.35	0.48	0.23
13	If you answered “Yes” to question 12 above, which of the following statements best describes your awareness of the problem?	2.14	0.79	0.62
14	Internet Service Providers must advise “prospective subscribers” about Internet phishing before they subscribe.	3.43	0.82	0.68
15	In terms of creating Internet phishing awareness, what would be your preferred method of communication?	2.54	1.14	1.29
16	Do you have Internet Security installed on your computer?	1.13	0.46	0.21
17	If you answered “Yes” to question 16, which of the following is installed on your computer?	3.27	1.91	3.64
18	The products listed in question 17 are sufficient to combat the threat of Internet phishing	2.63	0.66	0.44
19	All secured websites, denoted by https://, are safe from phishing scams.	2.24	0.71	0.51

The questions in the above table do not have a measurement level that is appropriate for measures of central tendency, even though these statistics were capable of being calculated as part of QuestionPro. Use of the above statistics is useful when forced likert scale statements are used, as opposed to closed ended questions, as adopted in the survey. Frequency tables were therefore used earlier as they gave a better description of the sample in terms of the proportionate distributions among the different categories.

4.4 Calculating Scores to be Used for Detailed Analysis

In an effort to determine the level of awareness of the concept of Internet phishing; the level of understanding of Internet security; and to ascertain to what extent respondents are at risk due to lack of knowledge and understanding of the threats when using the Internet, three different groups of variables were combined to calculate an Internet phishing awareness score, an Internet security understanding score and an at-risk score for each of the respondents.

Respondents who indicated that they did not use the Internet were excluded from the analysis. The respondents who used the Internet, but who also indicated that they had never heard of the concept of Internet phishing, were given a score of zero for Internet phishing awareness.

The groups of variables used to calculate the three scores are listed in Annexure 1. The responses of these variables were evaluated and classified as very high, high, low and very low in terms of their contribution to demonstrating awareness of Internet phishing, understanding of Internet security and at-risk potential respectively, when selected by a respondent. Corresponding weights, as per Annexure 1, were then allocated to each of the responses and the sum of all the weights for all the relevant variables constituted the Internet phishing awareness, Internet security understanding and at-risk score for that respondent.

If a response was classified as very high, then a weight of 3 was allocated; for high a weight of 2; for low a weight of 1; and for very low a weight of 0 was allocated. If a respondent selected the “Other” option for any of the questions, then the weight for that variable was recorded as missing (**M**). When the sums of all the relevant weights were calculated for the scores and missing values were encountered for the Internet phishing awareness and Internet

security understanding (see red marking in Annexure 1), the score was recorded as missing and that respondent was therefore excluded from the analysis.

4.5 Score Ratios - Exploring the Distribution of these Scores

To compare the relative magnitude of the Internet phishing awareness, Internet security understanding and at-risk scores, each respondent's scores were normalised by dividing the relevant score by the maximum possible score for each of the three variables, namely 41, 43 and 38, respectively. This ratio was then multiplied by 10 to produce a score that is measured on a scale of 0 to 10.

Higher values for Internet phishing awareness and for Internet security understanding are associated with a higher level of awareness and understanding, respectively. Higher values for the at-risk are associated with being more at risk of becoming a victim of Internet fraud.

Table 4.7 examines the distribution of the scores for the three variables using descriptive statistics.

Table 4.7: Descriptive Statistics for the Calculated Ratios

	Minimum	Maximum	Mean	Std. Deviation
Level of awareness of the concept of Internet phishing	0.00	6.59	4.4552	1.20678
Level of understanding of Internet security	0.47	7.44	4.3968	1.33968
The extent to which a respondent is at risk of being a victim	0.53	5.53	3.2548	0.97759

Table 4.7 shows that the scores for both Internet phishing awareness and Internet security understanding are below that of the middle of the possible range, namely 5. This means that, on average, the level of Internet phishing awareness and Internet security understanding can, on a scale of 0 to 10, tend to be low.

The third variable, being the at-risk score, is even less, indicating that the respondents tend to have Internet security installed on their systems and were therefore not at risk of falling prey to fraud on the Internet. Possible explanations for this are that most of them do not expose themselves to high-risk transactions on the Internet.

4.6 Histograms for the Three Scores (Variables)

Normality is one of the assumptions of Analysis of Variance (ANOVA). Before this procedure can be used, the distribution of the variable must be investigated to decide whether the use of ANOVA is warranted. Histograms were therefore used to understand this distribution, since they make it easy to see where the majority of values fall in a measurement scale, and how much variation exists.

Having examined the results in Table 4.7, it was clear that the distributions of the three scores did not deviate extremely from normality (95% confidence interval with a 5 % margin for error), hence the ANOVA can be used for the three variables. Histograms were generated for the three variables against the number of respondents in each case, and they are depicted in Figures 4.3, Figure 4.4 and Figure 4.5 respectively.

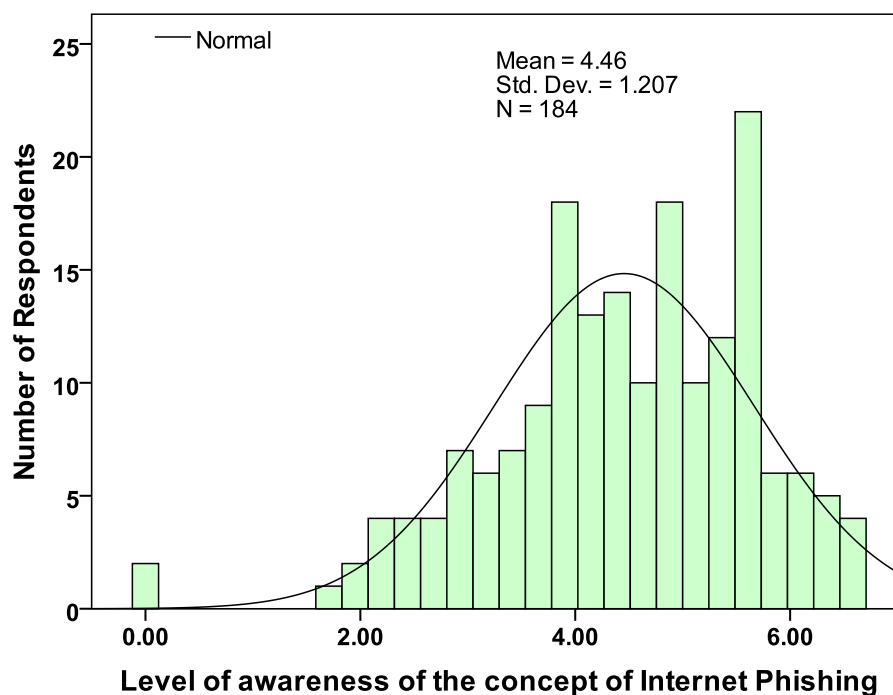


Figure 4.3 – Histogram for the Level of Awareness of the Concept of Internet Phishing

The second histogram examined the relationship between the level of understanding of Internet security amongst the various respondents. The results are illustrated in Figure 4.4

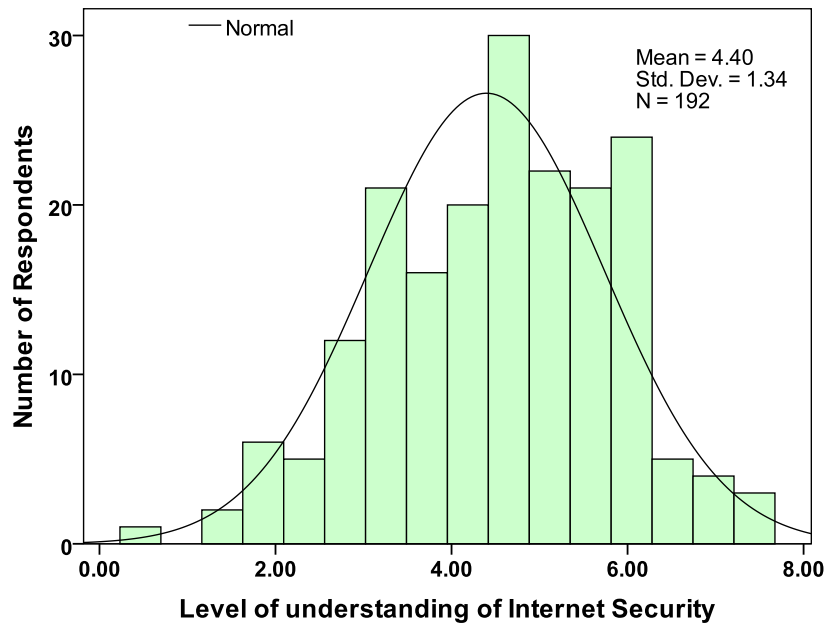


Figure 4.4 – Histogram for the Level of Understanding of Internet Security

The third histogram examined the relationship of the extent to which respondents are at risk of being a victim amongst the various respondents. The results are illustrated in Figure 4.5

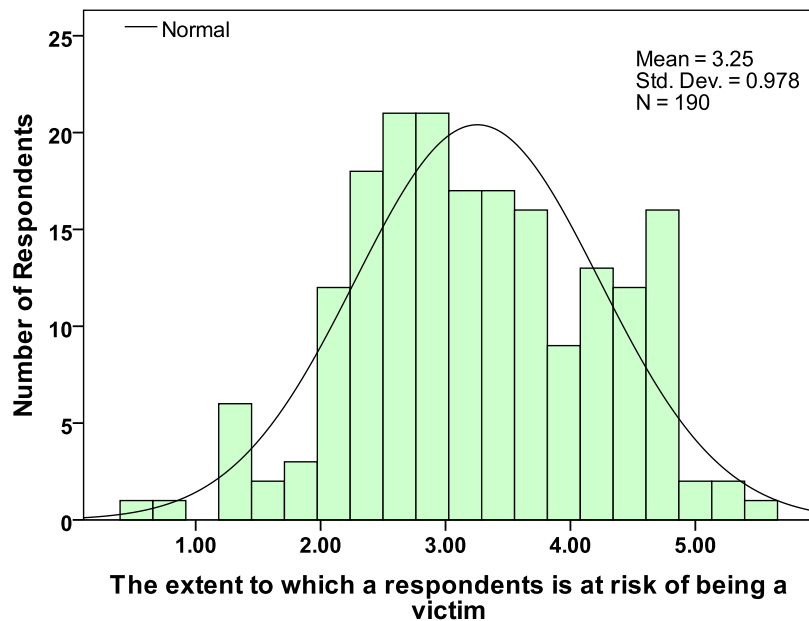


Figure 4.5 – Histogram for the Extent to Which Respondents are at Risk of Being a Victim

Examining the histograms for all three variables, the following conclusions can be drawn. The means are 4.46, 4.40 and 3.25 respectively, showing that all three variables are centred around

4.0. Most of the data are within target, with very little variation from the mean. Even though most the data were within bounds, some of them were dispersed away from the target. The standard deviations are 1.2, 1.3 and 0.9 respectively, thereby concluding that all three variables assume full normality with respect to each other.

4.7 Analysis of Variances (ANOVA)

Several ANOVA analyses were performed to investigate the relationship between a range of dependent and independent variables, as identified in Annexure 1. They were also conducted to identify any influence that these variables may have had on the dependent variable. Group mean comparisons were undertaken for the three variables that were identified.

4.7.1 Group Mean Comparisons

The independent samples *t*-test was used to test for differences between the two gender groups on the three continuous scores (Pallant, 2005), and also for the race and age groups, one-way, between-groups, analysis of variance (ANOVA) was employed to compare the variability in scores (variance) between the different groups (believed to be due to the independent variable) with the variability within each of the groups (believed to be due to chance). An independent samples *t*-test was conducted to compare the mean level of Internet phishing awareness, the mean level of understanding of Internet security and to what extent, on average, males and females were at risk of becoming a victim of Internet fraud. The results are shown in Table 4.8.

Table 4.8 – Independent Samples *t*-test for Gender – Group Statistics

DESCRITPION		Male	Female
Level of awareness of the concept of Internet phishing	N	119	65
	Mean	4.64	4.12
	Std. Deviation	1.128	1.281
	Std. Error Mean	0.103	0.159
Level of understanding of Internet security	N	127	65
	Mean	4.42	4.35
	Std. Deviation	1.374	1.280
	Std. Error Mean	0.122	0.159
The extent to which a respondent is at risk of being a victim	N	123	67
	Mean	3.33	3.11
	Std. Deviation	0.978	0.959
	Std. Error Mean	0.089	0.117

As seen in Table 4.8, gender had a significant effect [$t(182) = 2.837, p = 0.005$] on the level of awareness of the concept of Internet phishing. More specifically, the mean level of Internet

phishing awareness for males [M = 4.64, SD = 1.128] is significantly higher than for females [M = 4.12, SD = 1.281].

There was no significant difference in the scores for males [M=4.42, SD=1.374] and females [M = 4.35, SD = 1.280] regarding their level of understanding of Internet security [t(190) = 0.341, $p > 0.05$]. There was no significant difference in the scores for males [M = 3.33, SD = 0.983] and females [M = 3.11, SD = 0.959] regarding the extent to which they were at risk of becoming victims of Internet fraud [t(188) = 1.504, $p > 0.05$].

An independent sample *t*-test for gender was subsequently compiled because of the significance levels shown above. The results for the Levene test are shown in Table 4.9.

Table 4.9 – Independent Samples *t*-test for Gender

DESCRIPTION		Levene Test for Equality of Variances		<i>t</i> -test for Equality of Means		
		F	Sig.	<i>t</i>	df	Sig. (2-tailed)
Level of awareness of the concept of Internet phishing	Equal variances assumed	0.100	0.753	2.837	182	0.005
	Equal variances not assumed			2.733	118.17	0.007
Level of understanding of Internet security	Equal variances assumed	0.293	0.589	0.341	190	0.734
	Equal variances not assumed			0.349	137.48	0.728
The extent to which a respondent is at risk of being a victim	Equal variances assumed	0.435	0.510	1.504	188	0.134
	Equal variances not assumed			1.516	138.61	0.132

With respect to all three of the dependent variables, the Levene test for equality of variance was not significant and the null hypothesis, which assumes that the variance in the groups are equal, could therefore not be rejected. Thus, the *t*-test with equal variance assumed, will be used to determine the significance of the mean difference between the gender groups.

4.7.2 One-Way Between Groups – ANOVA for Race

A one-way between-groups analysis of variance was conducted to explore the impact of race on the three different calculated scores for Internet phishing awareness, Internet security understanding and at-risk. The respondents were divided into four groups according to their race (Group 1: Black, Group 2: Coloured, Group 3: Indian, Group 4: White).

Descriptive statistics for the different groups are listed in Table 4.10.

Table 4.10 – Descriptives for Race

DESCRIPTION		Black	Coloured	Indian	White	Total
Level of awareness of the concept of Internet phishing	N	29	8	79	67	183
	Mean	3.616	4.786	4.547	4.656	4.450
	Std. Deviation	1.443	0.701	1.165	1.054	1.208
	Std. Error	0.268	0.247	0.131	0.128	0.089
	Minimum	0.00	3.90	1.95	2.20	0.00
	Maximum	5.85	5.85	6.59	6.59	6.59
Level of understanding of Internet security	N	28	8	84	71	191
	Mean	3.571	4.9709	4.529	4.497	4.395
	Std. Deviation	1.295	0.735	1.303	1.355	1.343
	Std. Error	0.245	0.259	0.142	0.160	0.097
	Minimum	0.47	4.19	1.16	1.63	0.47
	Maximum	6.05	6.28	7.44	7.44	7.44
The extent to which a respondent is at risk of being a victim	N	29	8	82	70	189
	Mean	3.258	3.026	3.100	3.454	3.252
	Std. Deviation	0.812	0.912	1.035	0.965	0.979
	Std. Error	0.151	0.322	0.114	0.115	0.071
	Minimum	1.84	1.84	0.53	0.79	0.53
	Maximum	4.74	4.74	5.53	5.26	5.53

Table 4.10 provides statistics about the distribution of respondents within each group. The descriptive information in this table will be used to interpret if there are any significant results

amongst the three variables. A test of homogeneity of variance revealed that none of the scores violated the assumption of homogeneity of variance, namely $p > 0.05$ (see Table 4.11). Thus, reporting the F ratio for these are in order (see Table 4.12).

Table 4.11 – Test of Homogeneity of Variances (Race)

DESCRIPTION	Levene Statistic	df1	df2	Sig.
Level of awareness of the concept of Internet phishing	1.503	3	179	0.216
Level of understanding of Internet security	0.921	3	187	0.432
The extent to which a respondent is at risk of	0.736	3	185	0.532

One of the assumptions of ANOVA is homogeneity of variance (same pattern of variance in all the groups) and the Levene test, actually tests the null hypothesis that there is homogeneity of variance. With the p -value being higher than 0.05 (95 % confidence interval), the null hypothesis cannot be rejected and therefore homogeneity of variance can be assumed.

If this assumption was violated, then the use of the F -test would not be warranted. Because this rule is intact, the F -test was conducted amongst the three variables using ANOVA and these results are illustrated in Table 4.12.

Table 4.12 – Analysis of Variance Between Groups for Race

DESCRIPTION		Sum of Squares	df	Mean Square	F	Sig.
Level of awareness of the concept of Internet phishing	Between Groups	24.651	3	8.217	6.103	0.001
	Within Groups	241.020	179	1.346		
	Total	265.671	182			
Level of understanding of Internet security	Between Groups	23.903	3	7.968	4.673	0.004
	Within Groups	318.829	187	1.705		
	Total	342.732	190			
The extent to which a respondent is at risk of being a victim	Between Groups	5.181	3	1.727	1.823	0.144
	Within Groups	175.258	185	0.987		
	Total	180.439	188			

The results revealed a statistically significant effect of race on the mean level of Internet phishing awareness [$F(3, 179) = 6.103, p < 0.01$] and Internet security understanding [$F(3, 187) = 4.673, p < 0.01$]. The full summary of results is shown in Table 4.12. The results indicated that race had no significant effect on the mean at-risk score [$F(3, 185)=1.823, p > 0.05$] among the different race groups.

In order to assess pair wise differences among the four race groups for the average level of Internet phishing awareness and Internet security understanding, a post-hoc comparison using the Scheffè test was performed. The results are illustrated in Table 4.13.

Table 4.13 – Multiple Comparisons – Scheffè

Dependent Variable	(I) 2 Race	(J) 2 Race	Mean Difference (I-J)	Std. Error	Sig.
Level of awareness of the concept of Internet phishing	Black	Coloured	-4.79741	1.89995	0.099
		Indian	-3.81798*	1.03296	0.004
		White	-4.26197*	1.05751	0.001
	Coloured	Black	4.79741	1.89995	0.099
		Indian	0.97943	1.76516	0.958
		White	0.53545	1.77964	0.993
	Indian	Black	3.81798*	1.03296	0.004
		Coloured	-0.97943	1.76516	0.958
		White	-0.44398	0.79015	0.957
	White	Black	4.26197*	1.05751	0.001
		Coloured	-0.53545	1.77964	0.993
		Indian	0.44398	0.79015	0.957
Level of understanding of Internet security	Black	Coloured	-6.01786	2.25089	0.071
		Indian	-4.11905*	1.22523	0.012
		White	-3.98089*	1.25296	0.020
	Coloured	Black	6.01786	2.25089	0.071
		Indian	1.89881	2.07747	0.841
		White	2.03697	2.09395	0.814
	Indian	Black	4.11905*	1.22523	0.012
		Coloured	-1.89881	2.07747	0.841
		White	0.13816	0.90516	0.999
	White	Black	3.98089*	1.25296	0.020
		Coloured	-2.03697	2.09395	0.814
		Indian	-0.13816	0.90516	0.999

These results show that, at the 1% level of significance, the mean score for Internet phishing awareness for Black respondents (M = 3.62, SD = 1.443) differed significantly from the mean score for both Indian respondents (M = 4.55, SD = 1.165) and White respondents (M=4.66, SD = 1.054). Coloured respondents (M = 4.79, SD = 0.701) did not differ significantly from any of the other three race groups with regard to their mean level of Internet phishing awareness. At the 95% confidence level, with margin of error = 5%, the mean score for Internet security understanding for Black respondents (M = 3.57, SD = 1.296) differed significantly from the mean score for both Indian respondents (M = 4.53, SD = 1.304) and White respondents (M = 4.50, SD = 1.355). Coloured respondents (M = 4.97, SD = 0.735) did not differ significantly from any of the other three race groups with regard to their mean level of Internet security understanding.

4.7.3 One-Way Between Group – ANOVA for Age

A one-way between-groups analysis of variance was conducted to explore the impact of age on the three different calculated scores, Internet phishing awareness, Internet security understanding and at-risk. The respondents were divided into five groups according to their age. Descriptive statistics for the different groups are listed in Table 4.14

Table 4.14 – Descriptives for Age in Terms of the Three Variables

DESCRIPTION		Group 1 Under 25	Group 2 25 - 34	Group 3 35 - 44	Group 4 45 - 54	Group 5 Over 55	Total
Level of awareness of the concept of Internet phishing	N	6	58	64	33	22	183
	Mean	3.7805	4.3944	4.7218	4.2350	4.3016	4.4489
	Std. Deviation	1.00859	1.41371	1.08239	1.15342	0.98009	1.2070
	Std. Error	0.41175	0.18563	0.13530	0.20078	0.20896	0.0892
	Minimum	1.95	0.00	2.20	1.71	2.20	0.00
	Maximum	4.88	6.59	6.59	6.10	5.61	6.59
Level of understanding of Internet security	N	7	58	67	35	23	190
	Mean	4.0532	4.3705	4.6060	4.2525	4.1557	4.3941
	Std. Deviation	1.66002	1.44660	1.27393	1.42866	1.04546	1.3456
	Std. Error	0.62743	0.18995	0.15563	0.24149	0.21799	0.0976
	Minimum	1.16	0.47	1.63	1.40	2.09	0.47
	Maximum	6.05	7.44	7.44	6.74	6.98	7.44
The extent to which a respondent is at risk of being a victim	N	6	60	65	34	23	188
	Mean	2.8947	3.4956	3.2429	2.9180	3.1808	3.2461
	Std. Deviation	0.97048	0.93209	0.97038	1.07506	0.86887	0.9789
	Std. Error	0.39620	0.12033	0.12036	0.18437	0.18117	0.0714
	Minimum	1.32	1.32	1.32	0.53	1.58	0.53
	Maximum	3.68	5.00	5.53	4.74	5.00	5.53

According to the descriptive statistics generated in Table 4.14, the test revealed that none of the scores violated the assumption of homogeneity of variance, namely $p > 0.05$. Based on the above conclusion, a test for homogeneity of variances and the ANOVA for age can therefore be calculated. These variances are shown in Table 4.15.

Table 4.15 – Test of Homogeneity of Variances (Age)

DESCRIPTION	Levene Statistic	df1	df2	Sig.
Level of awareness of the concept of Internet	1.118	4	178	0.350
Level of understanding of Internet security	1.249	4	185	0.292
The extent to which a respondent is at risk of being a victim	0.130	4	183	0.971

Notice that all “p” values (last column in Table 4.15) are greater than 0.05 and this confirms that the F ratio for these descriptives are in order, hence these F values can be calculated. The results of this are shown in Table 4.16.

Table 4.16 – Analysis of Variance Between Groups (Age)

DESCRIPTION		Sum of Squares	df	Mean Square	F	Sig.
Level of awareness of the concept of Internet phishing	Between Groups	9.606	4	2.401	1.673	0.158
	Within Groups	255.559	178	1.436		
	Total	265.165	182			
Level of understanding of Internet security	Between Groups	5.864	4	1.466	0.806	0.523
	Within Groups	336.369	185	1.818		
	Total	342.233	189			
The extent to which a respondent is at risk of being a victim	Between Groups	8.236	4	2.059	2.204	0.070
	Within Groups	170.981	183	0.934		
	Total	179.217	187			

An ANOVA test was used to determine whether age has an effect on the level of awareness of the concept of Internet phishing, Internet security understanding, and to what extent a respondent is at risk of becoming a victim of Internet fraud. The results indicated that there is no significant effect of age on the mean score of either Internet phishing awareness [$F(4, 178)=1.673, p > 0.05$], Internet security understanding [$F(4, 185) = 0.806, p > 0.05$] or at-risk of becoming a victim [$F(4, 183) = 2.204, p > 0.05$] among the different race groups.

4.8 Correlation Analysis

In order to determine the type of relationship that existed between the three calculated scores, Internet phishing awareness, Internet security understanding and at-risk, Pearson correlation coefficients were calculated (Table 4.17).

While the coefficient of co-variance has no upper and lower limits, the coefficient of correlation can vary from positive one (+1) (indicating a perfect positive relationship), through zero (0) (indicating the absence of a relationship), to negative one (-1), thereby indicating a perfect negative relationship. As a rule of thumb, absolute correlation coefficients between 0.00 and 0.30 are considered low; those between 0.30 and 0.70 are moderate; and coefficients between 0.70 and 1.00 are considered high. However, this rule should always be qualified by the circumstances.

Table 4.17 – Pearson Correlation

DESCRIPTION		Level of awareness of the concept of Internet phishing	Level of understanding of Internet security	The extent to which a respondent is at risk of being a victim
Level of awareness of the concept of Internet phishing	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	184		
Level of understanding of Internet security	Pearson Correlation	0.636**	1	
	Sig. (2-tailed)	0.000		
	N	182	192	
The extent to which a respondent is at risk of being a victim	Pearson Correlation	0.320 **	-0.254**	1
	Sig. (2-tailed)	0.000	0.000	
	N	184	188	190

** . Correlation is significant at the 0.01 level (2-tailed).

Understandably, there was a medium to strong positive relationship between the level of Internet phishing awareness and the level of Internet security understanding ($r = 0.636$, $p < 0.001$).

There was a small but significant ($r = 0.320, p < 0.001$) positive relationship between the level of Internet phishing awareness and the extent to which a respondent is at risk of becoming a victim of Internet fraud. A possible explanation for this is that high awareness of Internet phishing means that the respondent is probably exposing himself/herself to higher-risk types of activities such as buying online.

There was a very small negative ($r = 0.254, p < 0.001$) but significant relationship between the level of Internet security understanding and the extent to which a respondent is at risk of becoming a victim of Internet fraud. This is understandable though, as one would expect that with higher levels of understanding Internet security, a respondent would be less at risk when using the Internet.

4.9 Scattergraphs of the Three Scores (Variables)

Scattergraphs are useful for plotting multivariate data and to determine potential relationships that exist amongst scale variables. It is also used to indicate the direction and strength of the relationship (Bryman and Bell, 2007:362).

Figure 4.6 examines the relationship between the level of understanding of Internet security against the level of awareness of Internet phishing.

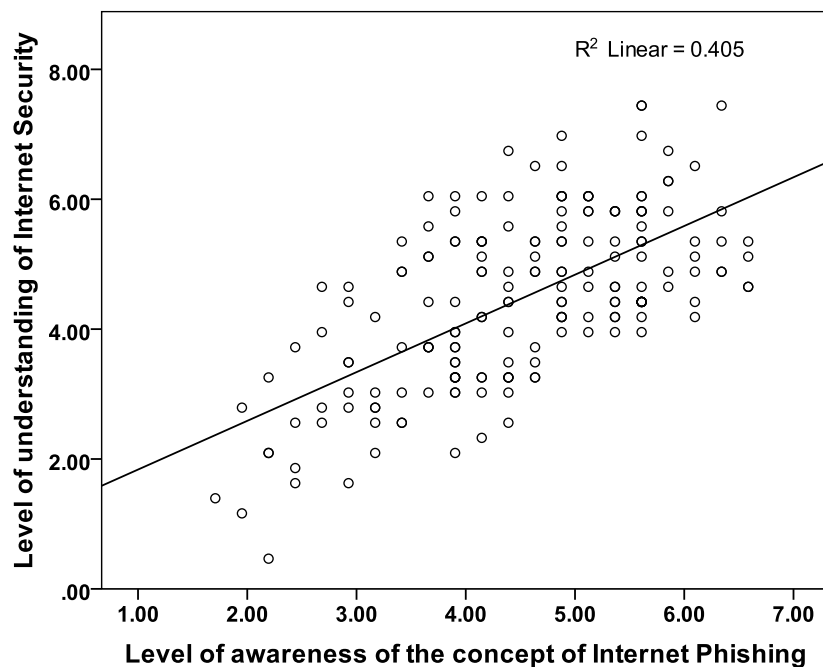


Figure 4.6 – Scattergraph of The Level of Understanding of Internet Security Versus Level of Awareness of Internet Phishing

The graph reveals that a relatively strong, positive relationship exists between these variables, and that a high level of awareness for Internet phishing implies that users inadvertently understand the concept of Internet security more clearly i.e. the variation in the two variables is very closely connected.

The second analysis was conducted to examine the relationship between the level of awareness of Internet phishing against the extent to which respondents are at risk of becoming victims. The results of this are shown in the scattergraph below as per Figure 4.7

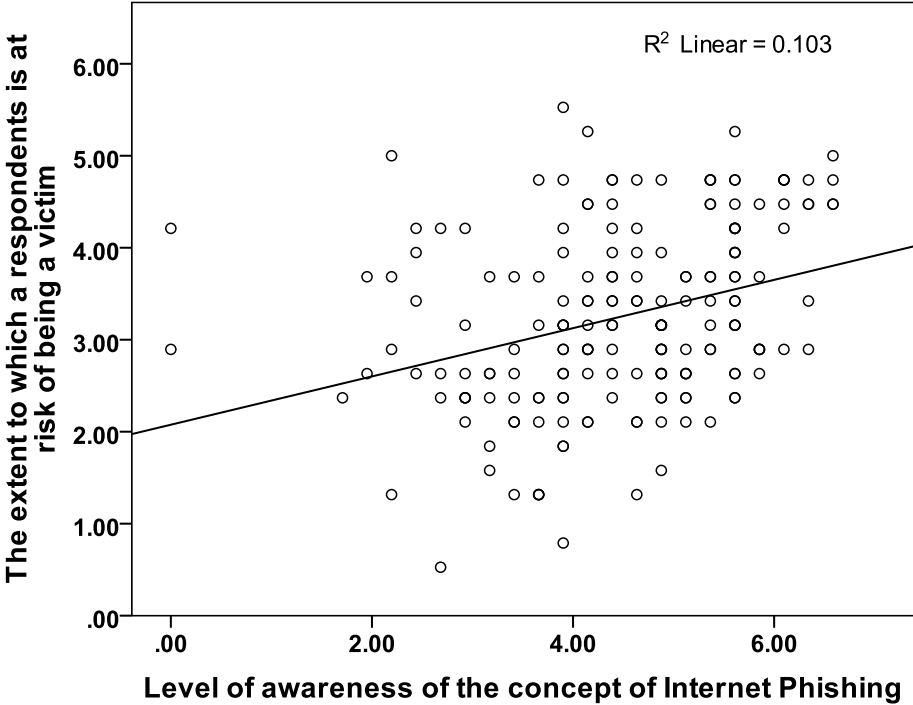


Figure 4.7 – Scattergraph of the Level of Awareness of Internet Phishing Versus the Extent to Which Respondents are at Risk of Becoming Victims

From the scattergraph, it is evident that a positive connection exists between these variables, although the strength of the relationship is not necessarily strong. The final scattergraph examines the relationship between the level of Internet security against the extent to which respondents are at risk of becoming victims.

The results are shown graphically in Figure 4.8

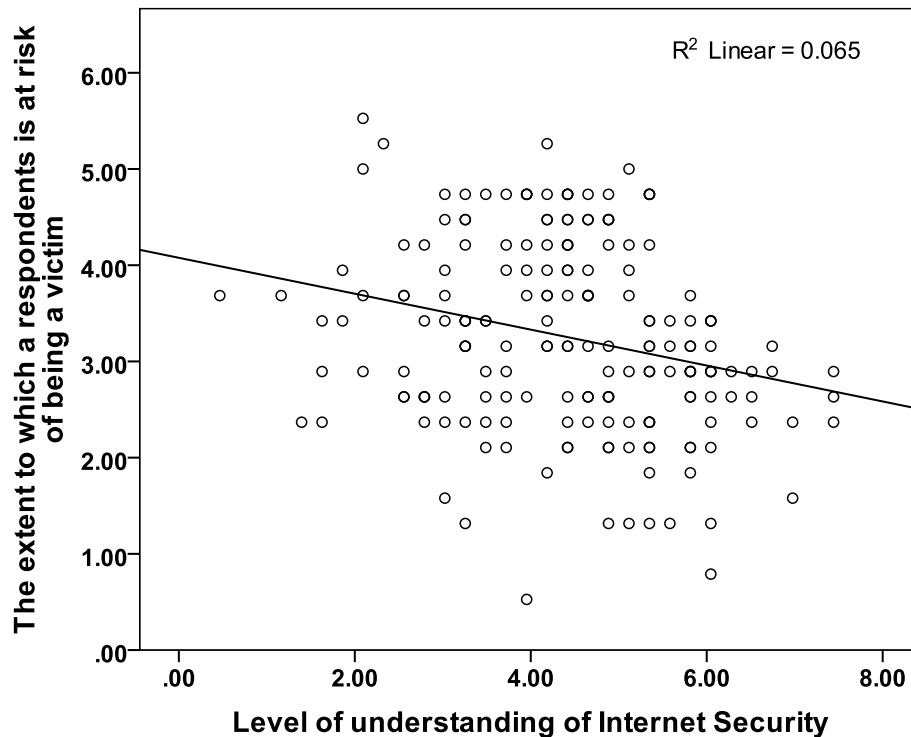


Figure 4.8 – Scattergraph of the Level of Understanding of Internet Security Versus the Extent to Which Respondents are at Risk of Becoming Victims

The results conclude that there is a weak, negative relationship that exists between these variables. The graph shows that lower levels of understanding of Internet security correspond to higher incidents of respondents becoming victims to Internet phishing. Even though the graph has a negative gradient, it does not imply that the relationship is not significant.

4.10 Summary

Chapter 4 presented the results of the study using statistics generated by SPSS. It depicted descriptive statistics in the form of frequency distribution tables, measures of central tendency and measures of dispersion. It also presented inferential statistics in the form of correlation and regression analyses.

Chapter 5 entails a detailed interpretation and discussion of these results.

CHAPTER FIVE

INTERPRETATION OF RESULTS

5.1 Introduction

The results of the survey, limited to graphs and tables, were presented in Chapter 4. The purpose of this chapter, is to interpret these analytical results in order to draw meaningful and useful conclusions. This chapter discusses and explains these findings, and attempts to make inferences from the various readings reviewed in Chapter 2.

5.2 Results of Frequency Distribution Analysis

The frequency distribution analyses (Chapter 4) conducted on the data set providing the demographic information revealed that 62 % of the participants were male and 38 % were female (Table 4.1). The demographics were then further categorised in terms of race, 44 % were Indian, 33 % were White, 19% were Black, and the remaining 4 % were Coloured.

The sample population was subdivided into six age groups. The analysis revealed that 36 % of the respondents, representing the highest frequency, were in the 35 – 44 age group range whilst the lowest (6%), were under 25 years of age.

The next frequency analysis examined the sample population in terms of Internet usage. From Figure 4.1, it is evident that the Internet is a commonly used tool and 24 % of the respondents used the Internet primarily for research, 22% used the Internet as a means of communicating with others, 11 % used it to transact online, 20% used it for online banking, 19 % used it for surfing and the remaining 4% used it for other undisclosed reasons.

The results of the frequency analysis conducted in questions 4 and 5 clearly show that the Internet is an essential tool with a variety of uses and applications and is therefore vital for users in Durban.

The second research question in this study sought to ascertain the participants' current awareness of Internet phishing (Table 4.3). The frequency analysis revealed that 85 % of the respondents had heard of the concept of Internet phishing as opposed to 15 % who were not familiar with the term.

Pertaining to Question 7 (Table 4.3), it is interesting to observe that 77 % of the participants understood Internet phishing to be a method of acquiring personal information from unsuspecting users over the Internet, whilst 18 % understood it to be a method of acquiring information / data from users' computers. It seemed a contradiction that only 5 % of the respondents felt that users are always at risk as long as their Internet protocol address is available, yet no-one concluded that Internet phishing may be a means of downloading viruses onto their computer.

In terms of the strategies that users adopted to alleviate the threat of Internet phishing, the following can be noted (Table 4.3).

- Of the respondents, 37 % showed awareness of the problem and were very cautious when using the Internet, whilst 27% relied heavily on technology, in the form of Internet security, to prevent them becoming victims.
- Of the respondents, 26% tried to prevent becoming victims of Internet phishing by ensuring that they provided absolutely no personal information over the Internet.
- Of the participants, 8% acknowledged their need to use the Internet, but merely lived in hope of never actually falling victim.
- Of the participants, 2% were absolutely certain that they would not become victims because they did not initiate any transactions over the Internet.

In order to identify a potential phishing scam, it is imperative that users have some idea of what they should be on the look-out for. Analysing question 9 revealed respondents' perceptions about characteristics of phishing attacks (Figure 4.2):

- They believed that identifiable characteristic of phishing is unsolicited requests for personal information (28%), followed closely by users (27%) feeling that disguised hyperlinks and sender addresses are more common.
- Of the users, 20 % became suspicious when email content appeared to be genuine, with 14 % feeling that embedded clickable images were sure tell-tale signs of a phishing attack.
- Of the respondents, only 10 % saw generic greeting as a characteristic of phishing.
- An issue of concern reveals that 1 % of the respondents did not even know what common characteristics of such an attack are, and it is this group that phishers will concentrate on to successfully launch their attacks.

The above statistics reveal that there are no definitive responses in terms of being able to identify the characteristics of a phishing attack. This statement is supported further by studies conducted by the Honeynet Project and Research Alliance (2005), which centred around Internet phishing awareness creation, stating that online users need to be vigilant by knowing the enemy within, and this study looked at the “behind the scenes of phishing attacks” to isolate the tell-tale signs of a typical phishing attack.

Even though participants’ perspectives of the characteristics of Internet phishing were not decisive, it was evident that the majority of the respondents (88 %) had not fallen victim to an Internet phishing attack, whereas 12 % had become victims of phishing (Table 4.3). This is aligned with earlier statistics of users who could not identify what the characteristics of a phishing attack were. According to Tsai (2005), studies undertaken showed that 43% of adults had been phished, which is a high percentage. Of those who had become victims of cyber crime, 69 % reported that a virus had been downloaded on to their computer, thereby compromising their hard drives, whilst 25% reported that purchases had been made on their credit cards. Quite a high percentage (6 %) reported that their bank accounts had been “cleaned out” before they suspected anything untoward. It is interesting to note that none of the respondents’ identities had been stolen in order to open retail accounts.

Only 68 % of respondents reported to have read some literature on Internet phishing, implying that an astounding 32 % have not read anything on the subject (Table 4.4). As developed by Ollman (2004), “The phishing guide – understanding and preventing phishing attacks”, concurred with the above trend that many online users are not reading adequate literature on Internet phishing, thereby putting themselves at risk of becoming victims. This is an extremely high percentage if one considers that most awareness initiatives are spread through the written word. Of those who were exposed to the subject matter, 11 % had read some literature for the first time. In terms of the way in which respondents wanted to be exposed to educational materials on phishing, only 25 % preferred television coverage, 27 % preferred pop-up ads on their Internet browsers, and the remaining 48 % preferred printed matter in the form of newspaper articles and pamphlets.

Question 14 attempted to understand the role that Internet service providers should play in the awareness creation programmes. Of the respondents, 91% thought that prospective subscribers should be educated on Internet phishing before they actually subscribed to

services, thereby showing the scepticism that people have regarding security on the Internet, while 9 % did not believe that education was the responsibility of the ISPs (Table 4.4).

In an attempt to establish whether people understood the concept of Internet security, the researcher asked if they had any form of security installed on their machine. Whilst 93 % of the sample had some sort of security installed, 3 % had none at all. Another issue of concern, however, is the fact that 4 %, (10 respondents) did not know whether or not they had Internet security, which implies that they were unaware of the benefits of Internet security software (Table 4.5). Studies conducted by Clarkson (2005), concluded that humans are still the weakest link in the security chain. Bresz (2004), also arrived at the same conclusion, but maintained that people are still the best place to start to improve the situation, and this can only be achieved through continuous education.

Of the respondents, 30% mentioned that they had installed some sort of an Anti-Virus; 14 % had Anti-Spyware; 7 % had Anti-Phishing; 20 % had a Firewall; 13 % had Active Security Updates, and 15 % claimed to have had all of the above installed as part of their defence systems. It was noted that 1% did not know which security software they had installed on their computer.

Delving further into the subject of security, it was interesting to note that 38 % did not think that the products listed above were sufficient to combat the threat of Internet phishing, whilst 62 % were in agreement. Studies conducted by Gartner (2005), showed that frequent data security lapses and increased cyber attacks have damaged consumer trust in online commerce. Because the issue of Internet security is subjective, a question was posed regarding secured websites, generally ones associated with financial institutions denoted by <https://>, followed by the actual URL. A high level of scepticism was revealed in response to this question as 66 % disagreed with the statement that “All secured websites are safe from phishing scams” and only 34 % acknowledged that they were happy to perform online transactions, as long as the website was secured (Table 4.5).

It is clear from these statistics that online users are not fully aware of Internet security issues, and that a fair amount of scepticism or mistrust exists in the domain of transacting online, which therefore creates a playing field for phishers to apply their skilful trade. To summarise, based on the findings of the frequency distribution analysis, it is evident that online users in Durban perceive Internet phishing to be a huge challenge and it therefore needs to be

addressed. Creating better awareness is vital, but the method to be adopted needs to be more appropriate.

Written literature works to an extent, but is clearly not adequate to curb the threat of this problem. Other forms of communication (television and radio) should therefore be explored to see if they will have the desired effect.

5.3 Results of the Measure of Dispersion Analysis

To determine the amount of variation in the sample, the standard deviation of each data set was calculated. The results of this analysis indicated that there was more variability in the responses received to the following statements, as highlighted in Table 4.7:

Q5	: What do you use the Internet for?	1.42
Q8	: Which strategies do you use to alleviate the problem of Internet phishing?	1.26
Q9	: What are the common characteristics of Internet phishing?	1.58
Q15	: In terms of Internet phishing awareness, what is your preferred method of communication?	1.14
Q17	: What type of Internet security do you have installed on your computer?	1.91

Each of these data sets produced a standard deviation that ranged between 1.26 and 1.91, thus indicating that there are differences in opinion with regard to these questions. The standard deviation for each of the other data sets was less than 1, thus indicating that there was minimal variation from the mean in these instances.

It is very disconcerting that the standard deviation for question 9 is high, which shows that respondents did not understand the common characteristics of Internet phishing. As such, many users may fall prey to Internet phishing because they cannot identify tell-tale signs of phishing scams. The standard deviation for Question 17 is also high, which shows that respondents do not really have a clear understanding of Internet security issues. As such, many users may become victims of Internet phishing because their first line of defence is not in place.

The complete breakdown of the standard deviation for each data set is presented in Table 4.6.

Studies undertaken by Vegter (2005), and subsequently by Butler (2006), concurred with the aforementioned results and revealed that users will constantly fall prey to phishing attacks, mainly because of a lack of awareness. This is further supported by the analyses done for Question 9, where it is unclear what some respondents actually perceive Internet phishing to be all about.

5.4 Results of the Correlation Analysis

Using the Pearson's technique, a correlation analysis was undertaken on the data with respect to the three variables, namely:

- Level of awareness of the concept of Internet phishing;
- Level of understanding of Internet security; and
- The extent to which a respondent is at risk of being a victim.

This analysis was conducted to establish the strength of the relationship between the variables. As previously discussed, the closer the Pearson coefficient is to 1, the stronger the relationship. As highlighted in Chapter 4, a strong positive correlation exists between level of awareness and the level of Internet security, as the coefficient was 0.636. This relationship supports the work undertaken by Liddy (2006), who examined the ways in which people can use the Internet safely. The author considered some of the fundamental issues regarding security and the manner in which users understand them and maintain confidentiality about sensitive information.

A second analysis was performed in order to understand the correlation that existed between Internet awareness and the risk of becoming a victim. Even though the Pearson coefficient is 0.320, the relationship that exists between these variables is low but positive, and is therefore still important. A possible explanation for this relationship could be due to the fact that Internet users who demonstrate a level of awareness on phishing will expose themselves to activities such as online banking, albeit with caution, and these activities have a degree of risk associated with them. Studies by Milletary (2007) showed some support for the above statement in that, with the advancement of technology and the associated conveniences thereof, users will inadvertently and unknowingly expose themselves to risk.

The third analysis examined the correlation that existed between Internet security and the risk of becoming a victim. Even though the Pearson coefficient (-0.254) may appear small, a relationship exists between these two variables, thus there is a risk of users becoming victims of Internet fraud. This is understandable given that higher levels of understanding Internet security would potentially put a respondent at less risk when using the Internet. This suggests that although this relationship is an important one, the two variables are in fact not particularly closely linked.

5.5 Analysis of Variance (ANOVA)

Analysis of Variance (ANOVA) is a statistical test used to determine whether or not the mean scores, of some measurement, for several groups of respondents are all equal. The one-way ANOVA is used to test differences between two or more independent groups, and involves one independent variable that can be used to divide the sample of respondents into two or more groups, and a continuous dependent variable. One-way ANOVA is usually employed to test for differences amongst at least three groups since the *t*-test can be used for differentiating between two groups (Pallant, 2005). ANOVA compares the variance believed to be due to the independent variable (between groups) to the variance believed to be due to chance (within groups) and calculates an F ratio by dividing the variance between groups by the variance within groups. If this F ratio is large, then it is an indication that the variability between the groups is greater than the variability within each group (Pallant, 2005).

The null hypothesis for this test is that the population means are equal, and if the F-test is considerable, by rejecting the null hypothesis, one can conclude that the independent variable has an effect on the dependent variable. However, this test cannot show which of the groups differ from one another, and thus one needs to conduct post-hoc tests to find out where these differences are (Pallant, 2005).

In summary, race has an effect on the level of awareness of the concept of Internet phishing. More specifically, on average, Black respondents demonstrated a lower level of awareness of Internet phishing than both Indian and White respondents. The level of awareness of Internet phishing for Coloured respondents does not differ much from any of the other race groups.

Race has an effect on the level of understanding of Internet security. More specifically, on average, Black respondents demonstrated a lower level of understanding of Internet security than both Indian and White respondents. The level of understanding of Internet security for Coloured respondents does not differ much from any of the other race groups.

5.6 Summary

Chapter 5 provided an interpretation of the results from the analysis conducted on the set of data obtained from the participants. The discussion revealed that Internet phishing is a serious problem, and it is prudent for all Internet users to exercise extreme caution when doing any activity online. The data not only showed various protective measures that can be adopted to circumvent phishing attacks, but also showed that a lack of awareness of the problem causes users to become victims of phishing. In addition, the results showed that whilst awareness is being created through various methods, the volume and impact of literature on the problem is inadequate, and coupled with the relatively low level of understanding, is therefore not having the desired effect of curbing this problem. The sixth and final chapter draws conclusions on this study and provides recommendations to users on how to avoid Internet phishing attacks.

CHAPTER SIX

RECOMMENDATIONS AND CONCLUSION

6.1 Introduction

The literature discussed in Chapter 2 reveals that Internet phishing is an extremely important subject and deserves to be recognised as such. The Internet shopping industry plays a vital role in the economy of a country and it has gained a substantial share of a market previously dominated by well-established chain stores and fashion houses, suggesting that the potential impact of this “online shopping” is enormous. Based on companies’ expansion to doing business online, phishers have realised that e-commerce is still developing and thus is an ideal target for exploitation and a very lucrative road to riches.

Various researchers have identified Internet phishing as a very simple and inexpensive scam to execute, with considerable profits for the scammer. Their deviant behaviour, though not new, has proliferated with the growth of the Internet, mainly from an online banking perspective, and this success has accorded phishers great scope to apply their trade in other areas.

This study aimed to establish what the levels of awareness were amongst users in Durban, and to gauge their understanding of the subject matter. The study also attempted to establish if a correlation existed between users who had installed Internet security and those who had become victims of Internet phishing.

6.2 Findings of This Study

The results of the analysis revealed that the research had been successful in achieving its objectives. Previous studies have identified the security/privacy dimension as being an important factor when using the Internet. Privacy (the protection of personal information) and security (the protection of users from the risk of fraud and financial loss) have been empirically shown to have a strong impact on attitudes towards the use of online financial services (Montoya-Weiss, Voss and Grewal, 2003).

The research findings showed that 100% of the sample population were of the opinion that Internet phishing is an important subject, and as such, should be given the due respect it deserves, as the implications of these phishing attacks have far reaching consequences. The

study also concluded that Internet service providers had a crucial role to play in ensuring that users are adequately primed before they become subscribers to the Internet. From the results, 92 % of the respondents agreed that prospective subscribers should be educated on Internet phishing before subscribing. Conversely, only 8 % did not believe that education was the responsibility of the Internet service providers.

The methods being used to create awareness deserve a mention at this stage. A noticeably high 32 % of the respondents had not read any literature on the subject, even though 85 % had heard of the concept of Internet phishing. While awareness creation initiatives have been launched through printed matter, it is evident that they are not having the desired effect. This alone justifies research on how to achieve effective phishing awareness campaigns.

Another important element that materialised was the lack of understanding of the concept of Internet security, and the actual purpose of having this protective line of defence. A great amount of scepticism exists, as demonstrated by the fact that 38 % of respondents noted that security products are not sufficient enough to protect online users, thereby implying that hackers and phishers are considered to be way ahead of the security systems currently in place.

The findings suggest that the Internet is an excellent business and strategic tool, and its usage is essential and universal. The rate at which it is evolving pressures individuals to take advantage of this new-age technology, because of the ease with which it is associated with daily tasks such as online banking. This convenience, however, introduces one to threats such as phishing, and the study has highlighted some of the concerns that users have in this regard. It is therefore crucial that users are educated about the online environment and how they can avoid becoming victims of this weapon of mass deception.

The findings of this study are aligned with the findings of the various authors whose work was discussed in detail in Chapter 2.

6.3 Implications of This Study

The specific focus of this study was to ascertain the level of awareness that exists amongst users in Durban.

The most important conclusion is the fact that even though users knew about the concept of Internet phishing, they still became victims. The issue of how to identify a phishing attack thus becomes an area of immediate concern, closely followed by the best means to educate the public on the matter.

It is therefore recommended that a study with a similar scope be conducted using “open-ended questions” to review a person’s ability to identify these attacks. Using “closed-ended questions” forced users to choose specific answers, even if the subject matter was not understood, and this could have resulted in the analysis and findings being skewed.

6.4 Limitations of This Study

This study was conducted in the geographical area of Durban, KwaZulu-Natal, to the exclusion of all other regions within South Africa.

One of the limitations of this study was that the respondents may have discarded or forgotten about the questionnaire emailed to them, despite the email reminders that were periodically sent during the two-month data collection period. Some of the respondents were evidently reluctant to answer the online survey used, as 86 respondents dropped out before completing it. Due to the method adopted, the researcher could not determine the reasons why this happened. Using the conventional questionnaire administration method would ensure that such reasons could be determined and documented.

Of the responses received, some participants did not answer all of the questions in full, and in light of this limitation, it may be difficult for other researchers embarking on similar studies to draw descriptive or inferential conclusions from the sample data of a much larger population.

6.5 Recommendations for Future Research

Section 2.8 provided some of the protection measures that are currently available to users on the subject of Internet phishing. The results in Chapters 4 and 5 clearly addressed the objectives of this study.

The following, however, are areas and measures that need to be addressed in order to decrease the number of successful phishing attacks:

- The study revealed that the lack of awareness of Internet phishing amongst the respondents was high. Users are not educated on the problem and education is everyone's responsibility. It is therefore imperative that all stakeholders play a more active role in awareness creation. The study also showed that the medium, which is primarily of a written nature (journal articles, pamphlets at banks etc.) is not having the desired effect in terms of awareness creation. Further studies can investigate which medium is considered most appropriate. In the interim, more television coverage (educational programmes, documentaries, public broadcasts, talkshows, news et cetera) is required on the subject.
- The study revealed that users have a limited understanding of the concept of Internet security and the direct bearing that it has on Internet phishing. Because users cannot adequately identify the characteristics of a phishing attack, it implied that they are not in a position to prevent themselves from becoming victims. It is therefore crucial that users are educated in the concept of security measures in general. Again, stemming from the previous bullet, the method used to encourage this education is crucial. Even though studies on Internet security do exist, it is recommended that research be conducted to understand how each form of Internet security affects the success rate of Internet phishing.
- The public only takes cognisance of a problem when they have become personally affected or involved, resulting in negative consequences. The role that financial institutions can play in awareness creation cannot be quantified. Whilst efforts are in place, they are clearly inadequate to counteract this problem. These institutions need to be more proactive in light of recent events that have taken place in our South African banking environment. Banks are therefore responsible to ensure that their staff members are fully *au fait* with the problem of Internet phishing, and this can be achieved through

focused training programmes. The acquired skills can subsequently be transferred to their clients.

- The role that Internet service providers and computer vendors play in curtailing this problem is essential. Whilst one-on-one training is not recommended, due to logistics, it is imperative that a training programme is designed and presented to prospective clients. Social networks also have a vital role to play in educational process. They should ensure that users are aware of the potential dangers that do exist over the Internet before they can subscribe, and legislation should be enforced to protect their clients.
- Clients who perform banking online generally activate sms alerts, so that they are made aware of transactions when they are concluded. Whilst this concept is brilliant for legitimate transactions, are phishers able to prevent these alerts when phishing scams are committed that involve fraudulent transactions? It is accordingly recommended that research be conducted to ascertain whether active alerts such as sms's are able to be bypassed by phishers when they conclude a fraudulent transaction on a user's account without the user being made aware of the transaction;
- This survey tried to utilise participants from the various race and age groupings. Even though certain conclusions have been drawn, the overall research in this area is minimal, and shows no noticeable correlation between age and gender. It would be valuable to determine if these criteria have any impact on Internet usage and evaluation of online purchasing patterns, thereby lending themselves to possible phishing attacks;
- The current study looked at a homogeneous population and sample, with similar backgrounds and levels of education. A truly representative sample would look at a heterogeneous sample comprising a number of different users. A larger sample should be drawn so that results can be generalised to the population, and it is also extremely important to research people who use the Internet from home; and
- Based on the findings of this research, a platform has been set so that a robust awareness programme can be developed. Whilst all of the above can be put in place, ultimately people must be held accountable for their own actions.

6.6 Summary

This study was in no way intended to solve or provide an answer as to how to curtail the criminal activities of the phishing fraternity. That is beyond the scope of this exercise and it is the duty of the criminal justice system to bring these criminals to book.

The primary objective of this dissertation was to determine the levels of awareness, or lack thereof, of Internet phishing that existed amongst users in Durban, and to alert Internet users to the dangers lurking within the world of modern day communication practices and ever evolving technological advances. To this end, the results obtained with the aid of the SPSS statistical software revealed that the subject matter is important to Durban users. The results of the survey show that this study is applicable to organisations and individuals who use the Internet and that the lessons from this study should be circulated to all Internet users.

The study further demonstrated that knowing about Internet phishing is not sufficient to combat the threat of this problem. A careful understanding of Internet security is essential. The analysis also revealed that users could not identify the characteristics of phishing attacks. When awareness programs are designed, it is imperative that the model chosen to convey the message is carefully scrutinised so that it fulfils its intended purpose.

REFERENCES

- Aldridge, A., White, M., and Forcht, K. (1997). *Security considerations of doing business via the Internet: cautions to be considered*. MCB University Press. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- Anti-Phishing Working Group (APWG). (2006). *Phishing Activity Trends Report*. Available from www.antiPhishing.org (Accessed on 9th April 2010)
- Attaran, M. (1999). *Internet-based business opportunities: buyers beware of scams*. School of Business and Public Administration, California State University: Bakersfield, California, USA. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- Atkinson, S., Phippen, A., and Johnson, C. (2005). *Improving protection mechanisms by understanding online risk*. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- Atwood, J. (2007). *Phishing: The Forever Hack*. [Online]. Available at <http://www.codinghorror.com> (Accessed 12th October 2010).
- Baker, C.R. (1999). *An analysis of fraud on the Internet*. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- Bajaj, S. (2006). *Concept of a Firewall*. [Online]. Available at <http://www.sunny-bajaj.com> (Accessed 12th October 2010).
- Bedward, D. (1999), *Quantitative Methods*, Butterworth-Heinemann, Great Britain.
- Berghel, H. (2006). *Phish Phactors: Offensive and Defensive Strategies*. [Online]. Available at <http://www.berghel.net> (Accessed 12th October 2010).
- Bramble, W., and Mason, E. (1989). *Understanding and Conducting Research*. New York: McGraw-Hill Book Company.

- Bryman, A. and Bell, E. (2007). *Business research methods*. 2nd edition. New York: Oxford University Press.
- Butler, R. (2006). *A framework of anti-Phishing measures aimed at protecting the online consumer's identity*. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- Clarkson, D. (2005). *Humans still the weak security link*. Available from <http://www.itweb.co.za> (Accessed on 9th April 2010)
- Cole, B. (2010). *Internet Scammers pull in R7million*. *Daily News*, 21st October, pp 10. Independent Newspapers, Durban.
- Configuring the CSS for Device Management*. 2006. [Online]. Available at <http://www.cisco.com> (Accessed 12th October 2010).
- Consumer Reports. (2006). *Don't bite at phishers' email bait*. Available from <http://www.consumerreports.org> (Accessed on 9th April 2010)
- Cooper, D.R., and Schindler, P.S. (2001). *Business Research Methods*. 7th edition. New York: McGraw-Hill.
- Dong-Her, S., Hsiu-Sen, C., Chun-Yuan, C., and Lin, B. (2004). *Internet Security: malicious emails detection and protection*. Available from <http://www.emerald-library.com> (Accessed on 9th April 2010)
- eBay Scams – *Sample phishing email*. 2009. [Online]. Available at <http://www.mopo.ca> (Accessed 12th October 2010).
- Emigh, A. (2005). *Online identity theft: Phishing technology, chokepoints and countermeasures*. 3 October. Available from <http://www.antiPhishing.org/phishing-dhs> (Accessed on 9th April 2010)

- Fake ICICI Bank Website – *Beware of phishing email*. 2010. [Online]. Available at <http://www.indiaconsumerforum.org> (Accessed 12th October 2010).
- Field, A. (2005). *Discovering statistics using SPSS*. 2nd edition. London: Sage Publications.
- Forcht, K.A., and Fore III, R.E. (1995). *Security issues and concerns with the Internet*. Internet Research: Electronic Networking Applications and Policy, Volume 5, Number 3, 1995, pp. 23–31. MCB University Press.
- Franklin, C. Grimes, R.A., Head, B., and Hines, M. (2008), “*Internet security: just wishful thinking?*”, Information Age, February/March, pp. 14-25.
- Gabrilovich, E., and Gontmakher, A. (2002). *The Homograph Attack*. Communications of the ACM: 45(2):128, February 2002. Available from <http://www.cs.technion.ac.il/gabr/papers> (Accessed on 9th April 2010)
- Gartner (2005), “*Gartner Survey show frequent data security lapses and increased cyber attacks damage consumer trust in online commerce*”, [Online]. Available from <http://www.gartner.com> (Accessed 30 October 2010).
- Graham, P. (2002a), *A Plan for Spam*, [Online]. Available from <http://www.paulgraham.com/spam> (Accessed 28 October 2010)
- Graham, P. (2002b), *Hackers and Painters - Big Ideas from the Computer Age*, O’Reilly and Associates, Sebastopol, CA.
- Grimes, R.A., Head, B., Hines, M., and Franklin, C. (2008). *Internet security: just wishful thinking?* Information Age, February/March, pp. 14-25.
- Hair, J.F., Black, W.C., Babin, B.J., and Anderson, R.E. (2001). *Multivariate Data Analysis*, 7th Edition, Prentice Hall

- Hawkins, S., Chou, D.C., and Yen, D.C. (2000). *Awareness and challenges of Internet Security*. Available from <http://www.emerald-library.com>. (Accessed 8 July 2010)
- Honeynet Project and Research Alliance (2005), *Know Your Enemy: Phishing – Behind the Scenes of Phishing Attacks*, [Online], Available from <http://www.honeynet.org/papers/phishing>, Accessed on the 17th November 2010
- Independent Online. (11 August 2005). Oxford rocks up with a Ruby Murray. *The Star*. Available from www.iol.co.za.
- Internet World Statistics. (31st June 2010). [Online]. Available from <http://www.internetworldstats.com> (Accessed 17th November 2010).
- Jackson, T.W., Dawson, R., and Wilson, D. (2003). *Understanding email interaction increases organisation productivity*. Communications of the ACM: Vol. 46, No. 8, pp. 80-4.
- Krejcie, R.V. and Morgan, D. W. (1970). *Determining sample size for research activities educational and psychological measurement*. Vol. 30. Pp 607 - 610.
- Langford, D. (2000). *Internet Ethics*. Basingstoke: Macmillan.
- Larson, R., and Farber, B. (2006). *Elementary statistics*. 3rd edition. New Jersey: Pearson Prentice Hall.
- Lazarinis, F. (2009). *Online risks obstructing safe Internet access for students*. Technological Educational Institute of Mesolonghi: Mesolonghi, Greece. Available from <http://www.emerald-library.com>. (Accessed 10 July 2010)
- Liddy, C., (1996). *Internet-Based EDI Trust and Security*. Daruma Management Services: Toronto, Canada.
- McCrohan, K.F. (2003). *Facing the threats to E-commerce*. George Mason University, School of Management: Fairfax, Virginia, USA.

- McManus, D.J., Sankar, C.S., Carr, H.H., and Ford, F.N. (2002). Intraorganisational versus interorganisational uses and benefits of electronic mail. *Information Resources Management Journal*, Vol. 15, No. 3, pp. 1-13.
- McWilliams, B. (2003). *Cloaking Device Made for Spammers*. Available from <http://www.wired.com/news/business>. (Accessed 9 June 2010).
- Microsoft. (2005). *Help prevent identity theft from Phishing scams*. Available from www.microsoft.com. (Accessed 10 February 2010).
- Microsoft. (2006). *Protecting a business from online threat*. Available from www.microsoft.com. (Accessed 21 April 2010).
- Millettary, J. (2006). *Technical trends in Phishing attacks*. Available from <http://www.cert.org>. (Accessed 21 April 2010).
- Montoya-Weiss, M.M., Voss, G.B., and Grewal, D. (2003). *Bricks to clicks: What drives customer use of the Internet in a multi-channel environment?* Working Paper. Caroline State University, (USA)
- Nieuwenhuis, G. (2009). *Statistical methods for business and economics*. United Kingdom: McGraw - Hill Education.
- Oliva, R.A. (2004). Spam! *Marketing Management*, Vol. 13, No. 1, pp. 50-3.
- Ollmann, G. (2004). *The Phishing guide: understanding and preventing Phishing attacks*, September, available at: <http://ngsconsulting.com>.
- Pallant, J. (2005). *SPSS Survival manual*. 2nd edition. New York: Open University Press.
- Polit, D.F., and Hungler, B.P., (1991). *Nursing Research. Principles and Methods*, 4th Edition. J.B. Lippincott Company, Philadelphia, New York, Hagestown.

- Pruitt, S. (2005). Firefox users snap up anti-Phishing toolbar. *Network World*, Vol. 22, No. 21, 30 May 2010, p. 20. Available from <http://www.networkworld.com>. (Accessed 21 August 2010)
- Ratnasingham, P. (1998). *Internet-Based EDI Trust and Security*. Department of Information Systems, University of Melbourne: Victoria, Australia.
- Recognising and avoiding email scams. (1998). [Online]. Available from http://www.antiphishing.org/phishing_archive (Accessed 31 June 2010).
- Roberts, P. (2004). *More Scam Artists Go Phishing*. Available from <http://www.pcworld.com/news/article0>. (Accessed 31 May 2010).
- Russell, K. (1995), "Barricading the Net," *Byte*, April, p. 89.
- Santos, J.R.A. (1999). Cronbach's alpha: a tool for assessing the reliability of scales. *Journal of extension*. Available from www.joe.org.
- Sharma, A., and Sheth, J.N.W. (2004). Web-based marketing: the coming revolution in marketing thought and strategy. *Journal of Business Research*, Vol. 57, No. 7, pp. 696-703.
- Sipior, J.C., Ward, B.T., and Bonner, P.G. (2004). *Should spam be on the menu?* Communications of the ACM: Vol. 47, No. 6, pp. 59-64.
- Smailes, J., and McGrane, A. (2000). *Essential Business Statistics*. England: Pearson Prentice Hall.
- Sophos J. (2004). *Phishing and the threat to corporate networks*. Available from <http://www.sophos.com>. (Accessed 18 May 2010).
- Symantec. (2006). *Internet Security Threat Report – Trends for January 2006 - June 2006*. Vol. 10, September. Available from www.symantec.com. (Accessed 18 May 2010)

- Tsai, C. (2005), Survey: 43 percent of adults get 'phished', [Online] Available from <http://www.siliconvalley.com>, Accessed on the 19th October 2010
- Turban, E., Lee, J., King, D., and Chung, H.M. (2000). *Electronic Commerce: A Managerial Perspective*. Englewood Cliffs, NJ: Prentice-Hall.
- Vegter, I. (2005). Plugging the 'Phishing' hole. *iWeek*, Vol. 5, pp. 16-18.
- Warren, S. (2005), *12 steps to avoid phishing scams*, Available from <http://articles.techrepublic.com>, Accessed on the 17th August 2010
- Wilson, T.V. (2005), *How phishing works*. [Online]. Available at <http://www.howstuffworks.com> (Accessed 12th October 2010).
- White, B. (2000). *Dissertation Skills*. New York: Continuum.
- Young, K. (2004), "*Internet addiction: a new clinical phenomenon and its consequences*", *American Behavioral Scientist*, Vol. 48 No. 4, pp. 402-15.

APPENDIX 1 – VARIABLES USED TO CALCULATE SCORES

		Internet Phishing Classification	Internet Security Classification	At-risk Classification	
I use the Internet for Surfing	1	VL	VL	L	
I use the Internet for Research	1	L	VL	L	
I use the Internet for Communication email Blogs Forums etc	1	L	VL	H	
I use the Internet for Online Banking	1	VH	L	VH	
I use the Internet for Purchasing Online	1	H	L	VH	
I use the Internet for Other reasons	1	M	M	M	
Have you heard of the concept of Internet phishing?	Yes	L	L	VL	
	No	VL	VL	VH	
My understanding of the term Internet phishing	It is a method of acquiring personal information from me over the Internet	VH	VH	VL	
	It is a method of acquiring information data from my computer	H	H	L	
	It is a method of downloading viruses onto my computer	VL	VL	VH	
	I am always at risk as long as my Internet protocol address is available	L	L	H	
My strategy to counteract the problem	I am not at threat because I don't do any transactions over the Internet	VL	VL	VH	
	I am aware of the problem and very cautious when using the Internet	L	L	VL	
	I don't disclose any personal information over the Internet	H	H	VL	
	I use the Internet and just hope that I am not a victim of Internet phishing	VL	VL	VH	
	I have technology that protects me	VH	VH	L	
Unsolicited requests for personal information is a characteristic of Internet phishing	0	VL	VL		
	1	VH	VH		
	Disguised hyperlinks and sender addresses is a characteristic of Internet phishing	0	VL		VL
	1	VH	VH		
	Embedded clickable images in an email is a characteristic of Internet phishing	0	VL		VL
	1	H	H		
	Generic greetings is a characteristic of Internet phishing	0	VL		VL
	1	L	VL		
	Email content that appears genuine is a characteristic of Internet phishing	0	VL		VL
	1	L	L		
I don't know what is a characteristic of Internet phishing	0	VL	VL		
	1	M	M		

Have you been a victim of Internet phishing?	Yes	*L✓VL	L	L
	No	VL	VL	VL
My bank account was cleaned out before I suspected anything Purchases were made on my credit card My computer downloaded a virus and crashed my system	1	*		
	1	*		
	1	✓		
Which of the following statements best describes your awareness of the problem? – having encountered literature on Internet phishing	It was the first time that I was exposed to the problem	VH		L
	I knew about Internet phishing and the article just made me more wary	H		VL
	I knew about Internet phishing and did not bother to read the article	L		VL
	I circulated the article so that others could be made aware of it	H		VL
Do you have Internet Security installed on your computer?	Yes	*H	H	VL
	No	VL	VL	VH
	I don't know	M	M	M
I have Anti-Virus Software installed on my computer I have Anti-Spyware installed on my computer I have Anti-Phishing Software installed on my computer I have a Firewall installed on my computer I have Active Security Updates installed on my computer I have All of the Above installed on my computer I don't know which security is installed on my computer	1		VH	VL
	1		H	VL
	1	*	H	VL
	1		VH	VL
	1		VH	VL
	1	*	VH	VL
	1		M	M
	M		M	M
Number of weights		18	19	17

QUESTIONNAIRE

1. Gender

1. Male
2. Female

2. Race

1. Black
2. Coloured
3. Indian
4. White

3. Age

1. Under 25
2. 25 - 34
3. 35 - 44
4. 45 - 54
5. Over 55

4. Do you use the Internet?

1. Yes
2. No

5. If you have answered “Yes” to question 4, what do you use the Internet for?

1. Surfing
2. Research
3. Communication (Email, Blogs, Forums etc)
4. Online Banking
5. Purchasing Online
6. Other

6. Have you heard of the concept of Internet phishing?

1. Yes
2. No

7. If you answered “Yes” to question 6 above, which of the following statements best describes your understanding of the term?

1. It is a method of acquiring personal information from me over the Internet
2. It is a method of acquiring information / data from my computer
3. It is a method of downloading viruses onto my computer
4. I am always at risk as long as my Internet protocol address is available.

8. If you answered “Yes” to question 6 above, which of the following strategies do you use to alleviate the problem?
 1. I am not at threat because I don’t do any transactions over the Internet
 2. I am aware of the problem and very cautious when using the Internet
 3. I don’t disclose any personal information over the Internet
 4. I use the Internet and just hope that I am not a victim of Internet phishing
 5. I have technology that protects me.

9. Which of the following, in your opinion, are common characteristics of Internet phishing?
 1. Unsolicited requests for personal information
 2. Disguised hyperlinks and sender addresses
 3. Embedded clickable images in an email
 4. Generic Greetings
 5. Email content that appears genuine
 6. I don’t know

10. If you answered “Yes” to question 6 above, have you been a victim of Internet phishing?
 1. Yes
 2. No

11. If you answered “Yes” to question 10 above, how were you affected?
 1. My bank account was cleaned out before I suspected anything
 2. My identity was stolen and used to open retail accounts
 3. Purchases were made on my credit card
 4. My computer downloaded a virus and crashed my system

12. Have you read any literature (newspaper, emails, journals or books) on Internet phishing?
 1. Yes
 2. No

13. If you answered “Yes” to question 12 above, which of the following statements best describes your awareness of the problem?
 1. It was the first time that I was exposed to the problem
 2. I knew about Internet phishing and the article just made me more wary
 3. I knew about Internet Phishing and did not bother to read the article
 4. I circulated the article so that others could be made aware of it

14. Internet Service Providers must advise “prospective subscribers” about Internet phishing before they subscribe.
 1. Strongly Disagree
 2. Disagree
 3. Agree
 4. Strongly Agree

15. In terms of creating Internet phishing awareness, what would be your preferred method of communication?
1. Newspaper Articles
 2. Pamphlets at Banking or retail outlets
 3. Television coverage
 4. Pop-Up Ads on my Internet Browser
16. Do you have Internet Security installed on your computer?
1. Yes
 2. No
 3. I don't know
17. If you answered "Yes" to question 16, which of the following is installed on your computer?
1. Anti-Virus Software
 2. Anti-Spyware
 3. Anti-Phishing Software
 4. Firewall
 5. Active Security Updates
 6. All of the above
 7. I don't know
18. The products listed in question 17 are sufficient to combat the threat of Internet phishing
1. Strongly Disagree
 2. Disagree
 3. Agree
 4. Strongly Agree
19. All secured websites, denoted by https://, are safe from phishing scams.
1. Strongly Disagree
 2. Disagree
 3. Agree
 4. Strongly Agree

THANK YOU FOR TAKING THE TIME TO COMPLETE THIS QUESTIONNAIRE

ETHICAL CLEARANCE CERTIFICATE



**UNIVERSITY OF
KWAZULU-NATAL**

*University of KwaZulu-Natal
Research Office
Govan Mbeki Centre
Westville Campus
University Road
Chiltern Hills
Westville
3629
South Africa
Tel No: +27 31 260 3587
Fax No: +27 31 260 2384
E-mail : naidoo4@ukzn.ac.za*

19 April 2010

Mr R Munien
15 Solly Street
High Ridge
STANGER
4450

Dear Mr Munien

PROTOCOL: Internet Phishing – Hook, Line and hopefully not Sunk...
ETHICAL APPROVAL NUMBER: HSS/0188/2010 M: Faculty of Management Studies

In response to your application dated 16 April 2010, Student Number: **941350264** the Humanities & Social Sciences Ethics Committee has considered the abovementioned application and the protocol has been given **FULL APPROVAL**.

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

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

Yours faithfully

Professor Steve Collings (Chair)
HUMANITIES & SOCIAL SCIENCES ETHICS COMMITTEE

SC/sn

cc: Prof. A M Singh
cc: Mrs. C Haddon