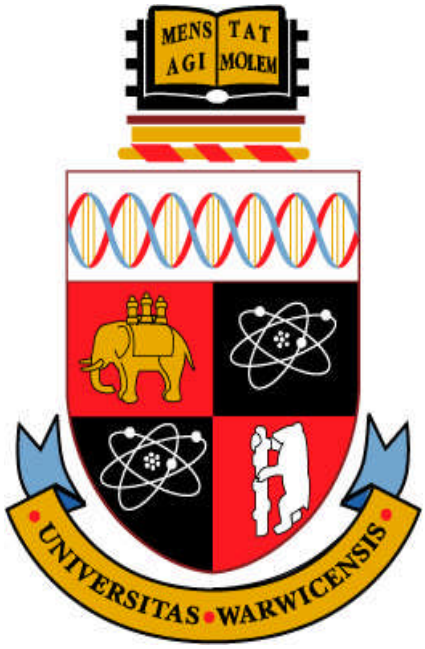
THE UNIVERSITY OF
WARWICK



WHAT CAN E-BUSINESS DO ABOUT PHISHING?

By;

Hamad Mesfer Alfataih

Supervised by;

Jeff Jones

Dissertation submitted in partial fulfilment for the award of the degree of
Master of Science

In

MSc in E-Business management

Project Submission Pro-Forma

NAME: Hamad Mesfer Alfataih

I wish the dissertation to be considered for (tick **one** only)

MSc in Digital Manufacturing Management	❑
MSc in Electronic Business Management	■
MSc in Engineering Business Management	❑
MSc in Engineering Enterprise Excellence	❑
MSc in International Technology Management	❑
MSc in Manufacturing Systems Engineering	❑
MSc in Process Technology & Business Management	❑
MSc in Programmes & Project Management	❑
MSc in Supply Chain & Logistics Management	❑

I have checked that my modules meet the requirements of the above award ■

I confirm that I have included in my dissertation:

An abstract of the work completed	■
A declaration of my contribution to the work	■
A table of contents	■
A list of figures	■
A glossary of terms (where appropriate)	❑
A clear statement of my project objectives	■
A full reference list	■

I am willing for my marked dissertation to be used for staff training purposes ■

Signed: …….. Date: ……..

ASBTRACT

Phishing may be defined as a criminal and fraudulent act designed to obtain confidential information from an individual with the intention of using this gathered information for personal financial or other personal gain. Since the explosion of the internet, which began in the late 1980s, methods of internet fraud and crimes such as phishing have increased dramatically due to the increase in use of digital communication such as emails, credit card usage, etc. Victims respond by sending confidential information to such fake e-mails believing that the information they supplied went to legitimate destinations such as banks. Due to phishing attacks financial losses from 2006 to 2008 had reached $4billion globally, and this figure is likely to increase as the growth in online business continues.

The purpose of this study is to investigate the various forms that phishing takes and to report on the problems, both financial and other, that result with the increase of attacks and the resulting effects that phishing has on individuals and businesses alike. Much research has been undertaken to help understand the increasing problem and to provide possible solutions to these phishing attacks. Many research and expert articles and papers were examined and during the project of the writing of this report surveys were sent out to private individuals and to online businesses as well to gain an understanding of the problem that phishing has on both individuals and businesses and to determine the level of understanding that users have of phishing and the resulting costs to those who have fallen victim to an attack.

ACKNOWLEDGEMENT

I would like to thank Almighty God who provided me the strength and knowledge to reach my target.

I would like to thank my family, especially my parents (Mesfer & Samra) for their support and help during my Master's degree and for their patience of the distance between me and them. Without their assistance and support my education would not achieve my goal. As well as my wife and my son (Kuhla & Ali)

Through my project I faced many difficulties which would not have been resolved without the guidance and support of my supervisor Dr Jeff Jones. I am thankful for these important suggestions and the trust he demonstrated during my period of my project.

I would like to thank all the staff at Warwick Manufacturing Group for their contributions and for sharing their knowledge and experiences.

Finally I would like to thank all my friends in WMG for their useful suggestions.

DECLARATION

I, Hamad Mesfer Alfataih declare that all the work submitted in this dissertation is my own and carried out by me, unless otherwise referenced. And none of the report has been earlier submitted.

TABLE OF CONTENTS

PROJECT SUBMISSION PRO-FORMA **2**

ASBTRACT **3**

ACKNOWLEDGEMENT **4**

DECLARATION **5**

TABLE OF CONTENTS **6**

1. INTRODUCTION **12**

1.1 What Am I Doing? *12*
1.2 Why Am I Doing This? *12*
1.3 How Am I Going to do it? *13*

2. LITERATURE REVIEW: E-BUSINESS AND E-COMMERCE **16**

2.1 INTRODUCTION: 16
2.2 DEFINITIONS OF E-BUSINESS AND E-COMMERCE: 16
2.3 E-COMMERCE: A BRIEF HISTORY 17
2.3.1 E-Commerce 1995-2000: Innovation *18*
2.3.2 E-Commerce 2001-2006: Consolidation *18*
2.3.3 E-Commerce 2006-Present: Reinvention *19*
2.4 TYPES OF E-COMMERCE TRANSACTIONS: 19
2.4.1 Business to Business (B2B) E-commerce: *19*
2.4.2 Business to Consumer (B2C) E-commerce: *20*
2.4.3 Consumer to Consumer (C2C) E-commerce: *20*
2.4.4 Mobile Commerce (M-commerce): *20*
2.5 THE IMPORTANCE AND TRENDS OF E-BUSINESS TECHNOLOGY: 21
2.6 WEB 2.0: 24
2.7 INTERNET AND E-COMMERCE SECURITY: 26
2.7.1 THE PLAYERS: 27
2.7.2 THE SCOPE OF THE PROBLEM: 28
2.7.3 SECURITY PROBLEMS AND THREATS IN E-COMMERCE ENVIRONMENT: 32
1. Malware: *33*
2. Spyware: *33*
3. Hacking and Destroy: *34*
5. Sniffing attacks: *34*
6. Denial of service (DOS) attacks: *34*
7. Credit card theft/fraud: *35*
2.8 SUMMARY: 36

3. LITERATURE REVIEW: PHISHING **38**

3.1 PHISHING: A SOCIAL ENGINEERING ATTACK 38
3.2 DEFINITIONS OF PHISHING: 39
3.3 A TYPICAL PHISHING ATTACK: THE MECHANICS 39
3.3.1 The Lure: *39*
3.3.2 The Hook: *40*
3.3.3 The Catch: *41*
3.4 WHY DOES PHISHING WORK? 42
3.4.1 Lack of Knowledge: *42*
3.4.2 Visual Deception: *43*
3.4.3 Bounded Attention: *43*
3.5 HOW DOES PHISHING WORK? 43
3.6 WHO IS BEHIND PHISHING FRAUDS? 44
3.6.1 Script Kiddies: *44*
3.6.2 White Hat Hackers: *44*
3.6.3 Black Hat Hackers: *45*

3.6.4 Grey Hat Hackers: *45*
3.6.5 Terrorism and Hackers: *45*
3.9 TYPES OF PHISHING ATTACKS: 49
3.9.1 Deceptive Phishing: *49*
3.9.2 Malware-Based Phishing: *50*
3.9.3 DNS-Based Phishing: *50*
3.9.4 Content-Injection Phishing: *51*
3.9.5 Man-in-the-Middle Phishing: *51*
3.9.6 Search Engine Phishing: *52*
3.10 ANALYSIS OF PHISHING E-MAILS: 52
3.11 EMAIL SPOOFING: 52
3.11.1 Using Company Image: *53*
3.11.2 Forged Sender Addresses: *54*
3.11.3 Disguised Links: *55*
3.11.4 Requiring a Quick Response: *56*
3.11.5 Security Promises: *56*
3.11.6 Hiding Host Information: *57*
3.12 SUMMARY: 58

4. INTRODUCTION TO RESEARCH METHODOLOGY: 60

4.1 INTRODUCTION 60
4.2 PARTICIPATION TO KNOWLEDGE 60
4.3 RESEARCH METHODS 61
4.3.1 Case study *61*
4.3.2 Questionnaires *61*
4.4 RESEARCH OBJECTIVES 61
4.5 RESEARCH PLAN: 62
4.6 QUALITATIVE AND QUANTITATIVE RESEARCH 62
4.7 RESEARCH METHODS 63
4.7.1 Case Study *63*
4.7.1.1 The advantages of using case study: 64
4.7.1.2 Phishing E-mail Case Study: 64
4.7.3 Surveys *64*
4.8 METHODS OF DATA COLLECTION: 65
4.8.1 Companies Questionnaire *65*
4.8.2 Users Questionnaire *65*
4.8.3 The advantages of Online Survey *66*
4.8.4 The disadvantages of Survey *66*
4.9 QUESTIONNAIRE DESIGN 66
4.10 SAMPLE SIZE 69
4.11 RESEARCH RESULTS 69
4.12 SUMMARY 69

5. ANALYSIS AND DISCUSSION 72

5.1 INTRODUCTION TO SURVEY RESPONSES: 72
5.1.1 Have you heard of online phishing? *72*
5.1.2 Online shopping: *74*
5.1.3 How many times in the last year have you received phishing email? *76*
5.1.4 Have you ever been fallen victim to a phishing email? *77*
5.1.5 How much did you lose? *79*
5.1.6 Which of the following actions should you take if you have responded to phishing e-mail? *81*
5.1.7 After falling victim to phishing have you continued shopping online? *84*
5.1.8 Are you satisfied with the action taken by the business/bank against your complaint? *85*
5.1.9 What precautions do you think businesses should take in order to prevent phishing related incidents? *89*
5.1.10 Does your bank provides free software to help prevent phishing? *91*
5.1.12 Do you know whether a web site offers security to protect your confidential data? *95*

5.1.13 If yes, which of the following Security are you aware of? *96*
5.1.14 National wide Bank phishing E-mail: *99*
5.1.15 HSBC Bank E-mail: *101*
5.2 PHISHING CASE STUDY: 103
5.2.1 Phishing email detail: *103*
5.2.2 Phishing Email: *104*
5.2.3 REASONS FOR SELECTING THIS CASE: *105*
5.2.5 Phishing Email Explanation: *106*
5.2.5.1 The “From:” Address 106
5.2.5.2 The "To:" Address 106
5.2.5.3 The Message "Subject:" 107
5.2.5.4 E-Business Logos 107
5.2.5.5 Message Body of the Email 107
5.2.5.6 The Web Link 107
5.2.5.7 The Message Body 108
5.2.6 Comparisons Between Legitimate and Phishing Emails *109*
5.2.7 Guarantee Trust Bank Phishing website *111*
5.2.8 Phishing Website Explanation: *112*
5.2.8.1 The Address Type (HTTP vs. HTTPS) 112
5.2.8.2 The URL or Web Address 112
5.2.8.3 GTbank Logos 112
5.2.8.4 Asking for your Cash Card Number 112
5.2.9 Comparisons between Legitimate and Phishing Websites *113*
5.2.10 Anti – Phishing Email Chart: *115*
5.2.11 Genuine and Phishing Email Trail *115*
5.3 PHISHING COUNTERMEASURES: 118
5.3.1 Detecting a likely attack: *118*
5.3.2 Preparing for a likely attack: *118*
5.3.3 Email Filtering: *119*
5.3.4 Email Authentication: *119*
5.3.5 Cousin Domain Rejection: *119*
5.3.6 Secure Patching: *120*
5.3.7 Padlock and http: *120*
5.3.8 Customer Education and Awareness: *120*
5.4 SUMMARY: 120

6. CONCLUSION 123

7. LIMITATIONS AND RECOMMENDATIONS: 127

7.1 LIMITATIONS: *127*
7.2 RECOMMENDATIONS: *128*
7.2.1 Recommendations for Online business: 128
7.2.2 Recommendations for online Users: 129

8. REFERENCES 132

APPENDIX: 138

Online Users Survey: *138*
Online Businesses Survey: *143*
Online Businesses E-mails List: *149*

List of tables:

TABLE 1: HAVE YOU HEARD OF ONLINE PHISHING? 72
TABLE 2: ON AVERAGE, HOW OFTEN EACH MONTH DO YOU USE AN ONLINE SHOPPING OR BANKING WEB SITE? 74
TABLE 3: HOW MANY TIMES IN THE LAST YEAR HAVE YOU RECEIVED PHISHING EMAIL? 76
TABLE 4:HAVE YOU EVER BEEN FALLEN VICTIM TO A PHISHING EMAIL? 77
TABLE 5: HAVE YOU EVER BEEN FALLEN VICTIM TO A PHISHING EMAIL?* HOW MANY TIMES IN THE LAST YEAR HAVE YOU RECEIVED PHISHING EMAIL? CROSSTABULATION 77
TABLE 6: HOW MUCH DID YOU LOSE? 79
TABLE 7: WHICH OF THE FOLLOWING ACTIONS SHOULD YOU TAKE IF YOU HAVE RESPONDED TO PHISHING E-MAIL? 81
TABLE 8: WHICH OF THE FOLLOWING ACTIONS SHOULD YOU TAKE IF YOU HAVE RESPONDED TO PHISHING E-MAIL? 83
TABLE 9: AFTER FALLING VICTIM TO PHISHING HAVE YOU CONTINUED SHOPPING ONLINE? 84
TABLE 10: ARE YOU SATISFIED WITH THE ACTION TAKEN BY THE BUSINESS/BANK AGAINST THE PHISHING IF YOU RESPONDED TO IT? . 85
TABLE 11: ON AVERAGE, HOW OFTEN EACH MONTH DO YOU USE AN ONLINE SHOPPING OR BANKING WEB SITE?* ARE YOU SATISFIED WITH THE ACTION TAKEN BY THE BUSINESS/BANK AGAINST THE PHISHING IF YOU RESPONDED TO IT? CROSS TABULATION 86
TABLE 12: CHI-SQUARE TESTS 87
TABLE 13: WHAT PRECAUTIONS DO YOU THINK BUSINESSES SHOULD TAKE IN ORDER TO PREVENT PHISHING RELATED INCIDENTS? 89
TABLE 14: WHAT PRECAUTIONS DO YOU THINK BUSINESSES SHOULD TAKE IN ORDER TO PREVENT PHISHING RELATED INCIDENTS? 89
TABLE 15: DOES YOUR BANK PROVIDE FREE SOFTWARE TO HELP PREVENT PHISHING? 91
TABLE 16: HAVE YOU DOWNLOADED ANTI-PHISHING SOFTWARE FROM YOUR BANK WEBSITE? 93
TABLE 17: DO YOU THINK IT IS SAFE TO FILL PERSONAL INFORMATION INTO POP-UP WINDOWS? 94
TABLE 18: DO YOU KNOW WHETHER A WEB SITE OFFERS SECURITY TO PROTECT YOUR CONFIDENTIAL DATA? 95
TABLE 19: WHICH OF THE FOLLOWING SECURITY ARE YOU AWARE OF? 97
TABLE 20: WHICH OF THE FOLLOWING SECURITY ARE YOU AWARE OF? 98
TABLE 21: COULD YOU READ THE EMAIL ABOVE AND ANSWER THIS QUESTION: DO YOU THINK THIS E-MAIL IS? (PHISHING OR LEGITIMATE NATIONALWIDEBANK E-MAIL) 100
TABLE 22: COULD YOU READ THE EMAIL ABOVE AND ANSWER THIS QUESTION: DO YOU THINK THIS E-MAIL IS? (HSBC BANK PHISHING OR LEGITIMATE E-MAIL)? 102

List of figure:

FIGURE 1: A THREE STAGE E-COMMERCE DEVELOPMENT HISTORY FROM 1995 – TILL PRESENT (LAUDON AND TRAVER, 2009). 19
FIGURE 2:U.S FORECASTED MOBILE COMMERCE REVENUES FROM 2009 TO 2015. ADAPTED FROM A REPORT BY CODA RESEARCH CONSULTANCY (2010). 21
FIGURE 3: U.S ONLINE RETAIL SALES GROWTH. ADAPTED FROM THE INTERNET RETAILER (2010A). 22
FIGURE 4: BROADBAND ACCESS IN THE U.S. ADAPTED FROM INTERNET RETAILER, (2010B). 23
FIGURE 5: INTERNET SALES IN THE UK, AS A PROPORTION OF TOTAL SALES, 2004 TO 2008. OFFICE OF NATIONAL STATISTICS, UK (2008). 23
FIGURE 6: COMPARISON BETWEEN WEB 1.0 AND WEB 2.0 APPLICATIONS (HAMID, 2007). 25
FIGURE 7: POINTS THE ATTACKER CAN TARGET. KHUSIAL AND MCKEGNEY (2005). 27
FIGURE 8: ONLINE REVENUE LOSSES DUE TO FRAUD IN THE U.S FROM 2000 TO 2009. ADAPTED FROM CYBERSOURCE ANNUAL FRAUD REPORT (2010). 29
FIGURE 9: YEARLY COMPARISON OF COMPLAINTS RECEIVED VIA THE IC3 WEBSITE. ADAPTED FROM IC3 INTERNET CRIME REPORT (2009). 30
FIGURE 10: PERCENT OF REFERRALS BY MONETARY LOSS. ADAPTED FROM IC3 INTERNET CRIME REPORT (2009). 30
FIGURE 11:2009 TOP 10 MOST REFERRED IC3 COMPLAINT CATEGORIES (PERCENT OF TOTAL COMPLAINTS REFERRED). ADAPTED FROM IC3 INTERNET CRIME REPORT (2009). 31
FIGURE 12: TOP 10 BY COUNTRIES BY COUNT: CRIMINALS (NUMBERED BY RANK). ADAPTED FROM IC3 INTERNET CRIME REPORT (2009). 32

FIGURE 13: ATTACKER SNIFFING INFORMATION BETWEEN THE SHOPPER AND SERVER (KHUSIAL AND MCKEGNEY, 2005). 34
FIGURE 14: DENIAL OF SERVICE ATTACKS (KHUSIAL AND MCKEGNEY, 2005). 35
FIGURE 15: EXAMPLES OF PHISHING. ADAPTED FROM SPAM-IP.COM/PHISHING-EXAMPLES. 40
FIGURE 16: A SAMPLE BOGUS E-MAIL. ADAPTED FROM: TIPS FOR QUICKLY SPOTTING AND AVOIDING PHISHING SCAMS (PACCHIANO, 2010). 41
FIGURE 17: VISUAL SECURITY INDICATORS IN MOZILLA FIREFOX (HEARST, ET AL. 2006). 42
FIGURE 18: SEVEN STEPS OF THE PHISHING PROCESS (EMIGH, 2005). 43
FIGURE 19: MALICIOUS ACTIVITY BY COUNTRY (SYMANTEC, 2010). 47
FIGURE 20: DATA BREACHES LEADING TO IDENTITY THEFT BY CAUSE AND IDENTITIES EXPOSED (SYMANTEC, 2010) 48
FIGURE 21: A TYPICAL DECEPTIVE PHISHING EMAIL MESSAGE (MICROSOFT, 2010). 49
FIGURE 22: MAN-IN-THE-MIDDLE PHISHING ATTACK (EMIGH, 2005). 51
FIGURE 23: A SAMPLE PHISHING EMAIL (DRAKE, ET AL. 2004). 53
FIGURE 24: SAMPLE PHISHING EMAIL. AN EXAMPLE OF PAYPAL SCAM (DRAKE, ET AL. 2004). 54
FIGURE 25: BARCLAYS BANK PHISHING EMAIL (YOUL, 2004). 55
FIGURE 26: FRAUDULENT EBAY EMAIL (DRAKE, ET AL. 2004). 55
FIGURE 27: TRUSTE SYMBOL USED BY DIFFERENT FRAUDULENT WEBSITES (DRAKE, ET AL. 2004). 57
FIGURE 28: RESEARCH PLAN 62
FIGURE 29: METHODS OF DATA COLLECTION 65
FIGURE 30: HAVE YOU HEARD OF ONLINE PHISHING? 73
FIGURE 31: ON AVERAGE, HOW OFTEN EACH MONTH DO YOU USE AN ONLINE SHOPPING OR BANKING WEB SITE? 75
FIGURE 32: HOW MANY TIMES IN THE LAST YEAR HAVE YOU RECEIVED PHISHING EMAIL? 76
FIGURE 33: HAVE YOU EVER BEEN FALLEN VICTIM TO A PHISHING EMAIL?* HOW MANY TIMES IN THE LAST YEAR HAVE YOU RECEIVED PHISHING EMAIL? CROSSTABULATION 78
FIGURE 34: HOW MUCH DID YOU LOSE? 80
FIGURE 35: WHICH OF THE FOLLOWING ACTIONS SHOULD YOU TAKE IF YOU HAVE RESPONDED TO PHISHING E-MAIL? 82
FIGURE 36: WHICH OF THE FOLLOWING ACTIONS SHOULD YOU TAKE IF YOU HAVE RESPONDED TO PHISHING E-MAIL? 83
FIGURE 37: AFTER FALLING VICTIM TO PHISHING HAVE YOU CONTINUED SHOPPING ONLINE? 84
FIGURE 38: ARE YOU SATISFIED WITH THE ACTION TAKEN BY THE BUSINESS/BANK AGAINST THE PHISHING IF YOU RESPONDED TO IT? 86
FIGURE39: ON AVERAGE, HOW OFTEN EACH MONTH DO YOU USE AN ONLINE SHOPPING OR BANKING WEB SITE?* ARE YOU SATISFIED WITH THE ACTION TAKEN BY THE BUSINESS/BANK AGAINST THE PHISHING IF YOU RESPONDED TO IT? CROSS TABULATION 88
FIGURE 40:WHAT PRECAUTIONS DO YOU THINK BUSINESSES SHOULD TAKE IN ORDER TO PREVENT PHISHING RELATED INCIDENTS? 90
FIGURE 41: ARRANGING THE ABOVE RESULTS IN ORDER OF PRECAUTION MEASURES 90
FIGURE 42: DOES YOUR BANK PROVIDE FREE SOFTWARE TO HELP PREVENT PHISHING? 92
FIGURE 43: HAVE YOU DOWNLOADED ANTI-PHISHING SOFTWARE FROM YOUR BANK WEBSITE? 93
FIGURE 44: DO YOU THINK IT IS SAFE TO FILL PERSONAL INFORMATION INTO POP-UP WINDOWS? 95
FIGURE 45: WHICH OF THE FOLLOWING SECURITY ARE YOU AWARE OF? 99
FIGURE 46: COULD YOU READ THE EMAIL ABOVE AND ANSWER THIS QUESTION: DO YOU THINK THIS E-MAIL IS? (HSBC BANK PHISHING OR LEGITIMATE E-MAIL)? 102
FIGURE 47:PHISHING E-MAIL. ADOPTED FROM HOTMAIL ACCOUNT(2010) 105
FIGURE 48:COMPARISONS BETWEEN LEGITIMATE AND PHISHING EMAILS. ADOPTED FROM: PERSONAL INFORMATION AND SCAMS PROTECTION REPORT (ROYAL CANADIAN MOUNTED POLICE , 2007) 109
FIGURE 49:GUARANTEE TRUST BANK PHISHING WEBSITE. ADOPTED FROM: HOTMAIL ACCOUNT(2010) 111
FIGURE 50: COMPARISONS BETWEEN LEGITIMATE AND PHISHING WEBSITE. ADOPTED FROM: PERSONAL INFORMATION AND SCAMS PROTECTION (ROYAL CANADIAN MOUNTED POLICE , 2007) 113
FIGURE 51:ANTI – PHISHING EMAIL CHART 115

CHAPTER 1

INTRODUCTION

1. INTRODUCTION

1.1 What Am I Doing?

This project will cover the relevant points that form a major part of the project and will explain what represent E-business is, how E-business works and its importance to both commercial enterprises and individuals alike, an overview to and examples of online crime and phishing and the techniques used.

The report continues with an introduction to and methodology of internet threats and pays particular attention to phishing; which itself represents the base of the project. Several examples are offered as evidence to highlight the problems of phishing scams and finally this review will present features to support this evidence and to prove that phishing has a detriment effect on E-business.

1.2 Why Am I Doing This?

Phishing attacks that look like as a company's official web site weaken the company's online brand and discourage customers from using the real web site of the online companies scared of become phishing victim. In addition to the direct costs of fraud losses, online businesses may also risk a drop in online revenues due to decreasing customer trust.

In 2004 the online newspaper[1], The Author, said that almost three in four online account holders (74%) who responded to an online survey by software developer Cyota said they were less likely to shop online because of the risk of phishing. Cyota's poll revealed that 75% of account holders would be less likely to respond to emails from their banks, and over 65% said they would be less likely to sign up, or continue to use, their bank's online services as a result of fraud fears. Only 30% of the respondents to the survey said that they would be able to distinguish a real email from a fraudulent one (Leyden, 2004)[2].

Companies who are the primary targets of repeated phishing attacks find that investors respond more negative compared with the early ones. This indicates

[1] http://www.theregister.co.uk/2004/05/05/phishing_fears_survey/ accessed at 10.08.2010
[2] http://www.mekabay.com/iyir/2004.pdf accessed at 10.08.2010

that an investors' awareness of phishing has been heightened in recent years and therefore they tend to penalise those firms which are unable to prevent phishing. This gives a signal to e-commerce firms to be better prepared against phishing so as to prevent any potential loss in market value (Alvin, 2008).

In 2007, a survey carried out by CNET found that, about 70% of the people surveyed have changed their online behaviour. Of that 70%, 20% said that in the future they will decrease the amount of transactions that they do online. With fewer transactions online with a number as large as 20%, could have great impact on internet commerce. That gets to the core of this research, and the message from this report is on better education the online user, said (Bassam Khan, vice president of marketing for Cloudmark).

1.3 How Am I Going to do it?

Chapter 1: Introduction

This chapter provides the problem of phishing and background of the paper. A short background of e-commerce and e-businesses and threats of security has been discussed with some evidence like previous survey by author and why I am doing this project briefly and how I will reach my target in the end.

Chapter 2: Literature Review of E-business and E-commerce

This chapter explain what is e-business and e-commerce actually are and how e-commerce work included types of transactions of e-commerce. The importance of e-business and e-commerce are in global markets and their benefits. The chapter highlights the brief history of e-commerce and provides some successful examples by selling and buying goods and products through the internet. With the success of the internet, also comes the security threats such as malware, spyware, and sniffing attacks, are being highlighted in this chapter.

Chapter 3: Literature Review of Phishing

This chapter gives explanation and description of phishing and its mechanics. The chapter also discusses forces behind phishing frauds and how does it work and what is their target. This chapter also gives detailed analyse of phishing types, fraud e-mailing techniques such as e-mail spoofing.

Chapter 4: Research Methodology

This chapter provides explanation of research objectives and the plans and tools used to reaching these objectives. The chapter explains tools such as questionnaire and case studies based methods in gathering the data to meet research objectives and why theses where chosen. This chapter explains the design of questionnaire and how the data was being collected and analysed with the help of a case study in getting to the final results of this research.

Chapter 5: Analysis & Discussion

The results of survey have been analysed through the charts and tables and discussed in the way of literatures. The chapter has been explained and analysed with the help of a case study as well.

Chapter 5: Conclusion

This chapter discusses the concluding remarks of this research work and explains the damages done by internet frauds especially phishing technique and ways of countering this threat, certain future directions as well as educating and increasing consumer awareness in fighting this crime.

Chapter 6: Recommendations and Limitations

No research paper can be completed without citing out and highlighting the limitations that the research faced and the recommendations in making future researches more reasonable and logical. Similarly this paper also highlights certain limitations and recommendations for consumers as well as businesses to counter the threat of phishing and in making necessary arrangements in mitigating the threat before it even starts.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction:

This literature review covers the most important or relevant points that will form a major part of the project and explain what represents E-business, how E-business works and its importance to both commercial enterprises and individuals alike, an overview to and examples of online crime and the techniques used.

The development of the internet witnessed over the last decade has led to limitless opportunities and possibilities, which range from necessary services to distance learning. On one hand ecommerce development has facilitated many businesses in growing by providing useful product and services on a global scale while on the other hand this medium has also opened a wide array of criminal activities and conducts leading towards customer as well as business losses (Goueff, 2000).

The report continues with a greater look at internet fraud and pays particular attention to phishing which itself represents the base of the project. Several examples are offer as evidence to highlight the problems of phishing scams and finally this review present aspect to support this evidence and to show that phishing has a harmful effect on E-business.

2.2 Definitions of E-Business and E-Commerce:

The terms e-business and e-commerce are more or less used interchangeably but these are two separate concepts. According to Rayport and Jaworski (2003), E-commerce normally involves those transactions that go after organisational boundaries including customers, suppliers, external partners, sales and marketing etc. Whereas E-business is the part of E-commerce that primarily covers a firm's internal commerce processes, for example online inventory control, development of product, human resource etc.

Laudon and Traver (2009), defines E-commerce and E-business as:

E-Commerce:

"The use of the internet and the web to transact business. More formally, digitally enabled commercial transactions between and among organizations and individuals".

E-Business:

"The digital enabling of transactions and processes within a firm, involving information systems under the control of the firm".

However they more explain the fact that e-commerce and e-business involve similar infrastructure and skill sets. These two concepts merge together at a point where internal industry organisation systems connect with external customers and suppliers, for example e-business infrastructure transforms into e-commerce where the exchange of values take place.

As discussed above, E-business and E-commerce are two distinct concepts as Rodgers et al (2002) explains of E-commerce relies on the web to link up customers with companies, while E-business relies on website as well as other ways required to connect the information system and data streams of an organisation both internally and externally. Moreover E-commerce requires human intervention and involvement for example during the purchasing or procurement procedures, where as E-business relies more on automated systems which brings efficiency in the channel by avoiding human errors.

2.3 E-Commerce: A brief History.

Although E-commerce is a new experience and the internet was opened to commercial use during the early 1990s, it has a short history. The fast growth of the website and internet servers by 1995, joint with the spread of private computers (PCs) in homes and businesses led to the creation of a communication infrastructure that was supportive of business transaction as never before (Schneider, 2002).

The history of E-commerce can be separated into three phases, as Laudon and Traver (2009) explain below:

2.3.1 E-Commerce 1995-2000: Innovation

The early 1990s witnessed the improvement and discovery of key e-commerce concepts. The formation of thousands of dot-com companies around the globe was a major development in the growth of e-commerce while the increase in the popularity of home PCs was equally supported by a growth of local area networks. Initially businessmen and financial backers thought of E-commerce as a new tool of shopping which would give immediate cost benefits and generate unexpected profits, but after losses of years.

The early days of e-commerce suggest that venture capitalists and commercial interests in developing e-business was largely motivated by visions of quick profit making and capturing of a major market share on a massive levels through the use of this technology. It was a true that previous way 'traditional' businesses were too stuck and slow in old fashioned techniques and therefore e-business would be too competitive for them, and such online businesses would achieve secure first mover advantage (Varian, 2000).

Not many dot-com companies formed since 1995 have survived and only a very few of these survivors are profitable (Laudon and Traver, 2009). The crash in the stock markets around the world throughout 2000 can be seen as a marker for ending the boom and great growth of the e-commerce industry and now consumers have grown more aware and have understood to use the website as a main source of extracting all the information about goods and products that they really buy during other sources and channels (Tedeschi, 2007).

2.3.2 E-Commerce 2001-2006: Consolidation

Before 2000 the concept of e-commerce was more of a "technology driven" concept where as the post 2000 era saw a shift to a rather more clever "business driven" concept (Laudon and Traver, 2009). Businesses now focus more on the use of the website and the internet to strengthen their market position while the strengthening and extensioning of their brands for the financing of new ventures and businesses have become difficult.

2.3.3 E-Commerce 2006-Present: Reinvention

This period of development extends during the current times and into the unsure future. The reinvention phase as is witnessed currently involves business models based primarily on customer generated contents and pages, social networking and interactions, and virtual online lives. Sites such as YouTube, Facebook, and MySpace have expanded massive popularity in a short period of time. This period is said to be more of a sociological phenomenon, as it is business phenomenon or a technological.

Figure 1: A three stage e-commerce development history from 1995 – till present (Laudon and Traver, 2009).

Researchers and experts believe that the basic contribution that e-commerce has brought is the reduction in transaction costs (Schneider, 2002). Cost that is incurred while buyers and sellers gather information and negotiate purchasing-sale transaction is known as transaction cost. Businesses have grown smarter and have started to utilise the website as a tool to reduce transaction costs that occur in virtually every phase and step of commerce.

2.4 Types of E-Commerce Transactions:

There is an array of different forms of e-commerce. Each one is different with regards to the market connection or relationship – who is selling to or who is buying from whom. Some of the distinguished types of e-commerce are explained below by Turban, (2008):

2.4.1 Business to Business (B2B) E-commerce:

The commerce involved in B2B focuses on companies selling to other companies. B2B e-commerce is now generally recognised as being the e-commerce segment with the largest potential for growth (Lord, 2001). According to Laudon and

Traver, (2009), an estimated figure of $16trillion worth of business to business transactions and exchanges both offline and online of various kinds across the globe took place in 2007, which suggests that B2B has a strong potential for growth.

Andam (2003) further repeats the importance of B2B by projecting the practices by global giants such as Cisco Systems which, for instance, receives 90% of its goods and products orders through the internet.

2.4.2 Business to Consumer (B2C) E-commerce:

B2C commerce refers to the connection that online companies attempt to make in reaching individual customers. It involves customer information gathering; purchasing touchable goods or information goods such as electronic materials i.e. software, e-books etc (Andam, 2003). According to the U.S census bureau (2010), B2C e-commerce transactions have crossed $290billion in 2008.

2.4.3 Consumer to Consumer (C2C) E-commerce:

C2C is a way of conducting business transactions among consumers and customers to buy and sell to each other which may include private individuals and consumers. C2C sites such as eBay, generated a figure of more than $60billion in gross merchandise volumes worldwide in 2007 (Laudon and Traver, 2009).

2.4.4 Mobile Commerce (M-commerce):

Mobile commerce refers to the buying and selling of goods through wireless digital devices i.e. cellular phones, PDAs and personal computers (Andam, 2003). According to a report by Stambor, (2010) published in Internet Retailer.com, the U.S mobile commerce sales figures are expected to reach $2.42billion by the end of 2010, compared to $1.20billion in 2009.

The figure below by Coda Research Consultancy (2010), shows the forecasted figures of the U.S mobile commerce revenues from 2009 to 2015.

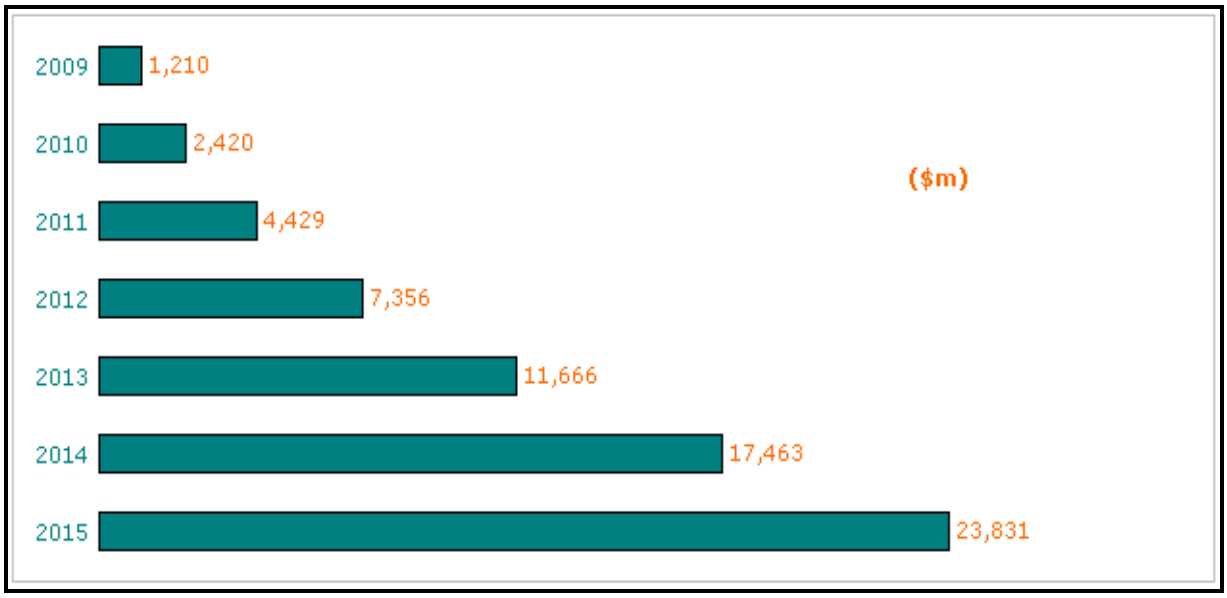


Figure 2:U.S forecasted mobile commerce revenues from 2009 to 2015. Adapted from a report by Coda Research Consultancy (2010).

2.5 The Importance and Trends of E-business Technology:

The importance of e-commerce/business can be seen from the fact that the value proposition that drives e-business includes the formation of new market opportunities through electronic channels. Damanpour (2001), stated that these electronic channels facilitate in enabling firms to:

1. Lower transaction costs.
2. Reduce delivery times.
3. Improve customer services.
4. Improve efficiency through quick responsiveness.
5. Permits transactions to cross cultural and national boundaries / geographical coverage.
6. Better management information through online reporting of sales data.
7. Integration with suppliers and vendors.
8. Better market understanding through extraction of customers buying behaviors.

The importance of E-business is also witnessed by the fact that in 2007 online consumer sales experienced a sharp increase of 25% to an estimated figure of $230billion globally (Laudon and Traver, 2009). According to retail sales figures on E-Marketer (2010), Europe is leading the e-commerce sales and by 2012, retail sales would cross over $200billion mark. Similarly the retail e-commerce sales in the US market according to e-marketer (2010), would witness an estimated growth of 12.7% on volume of $152billion by the end of 2010. It is further mentioned and interesting to note that the US retail market is estimated to cross $210billion mark by 2012.

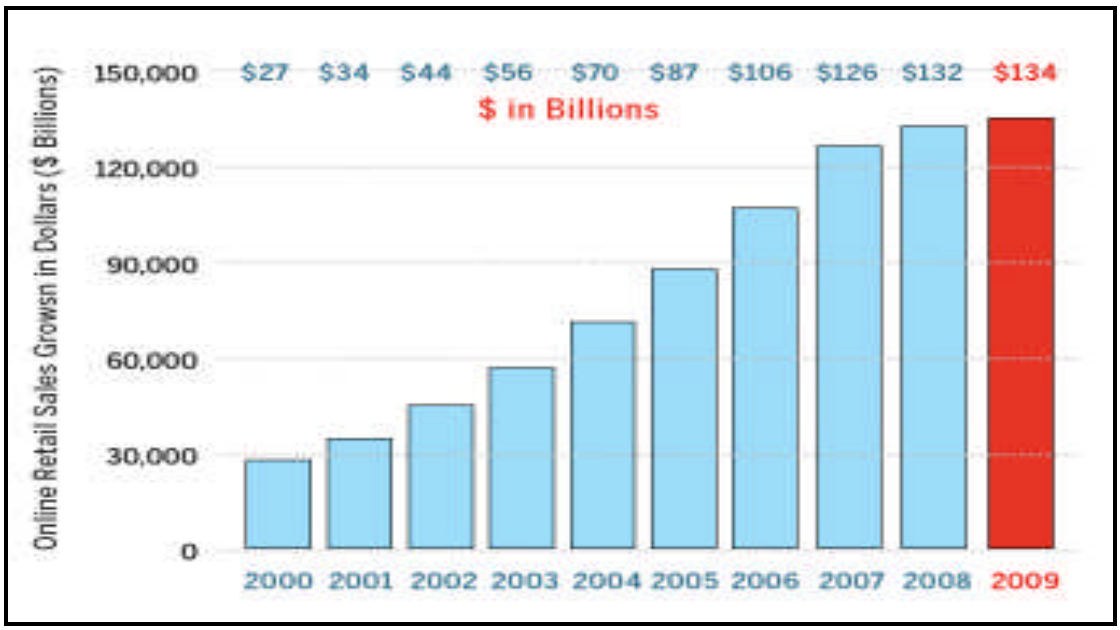


Figure 3: U.S online retail sales growth. Adapted from the Internet Retailer (2010a).

The figure above shows the U.S online retail sales growth from 2000 to 2009. The retail sales have grown at a sharp rate and gained $28.3billion in the last 4 years, which is a gain of 20% per year.

The internet is a tool which allows consumers and businesses to connect with one another in an inexpensive, quick and reliable manner. The internet has become an enabler for e-commerce to grow, and therefore its growth is highly dependent on the growth of the internet as a whole (Andam, 2003).

The figure below shows the spread of the broadband technology across the U.S from 2002 to 2010. The growth of the internet seems synonymous to the growth of e-commerce retail sales in the U.S if both figures 3 and 4 are compared.

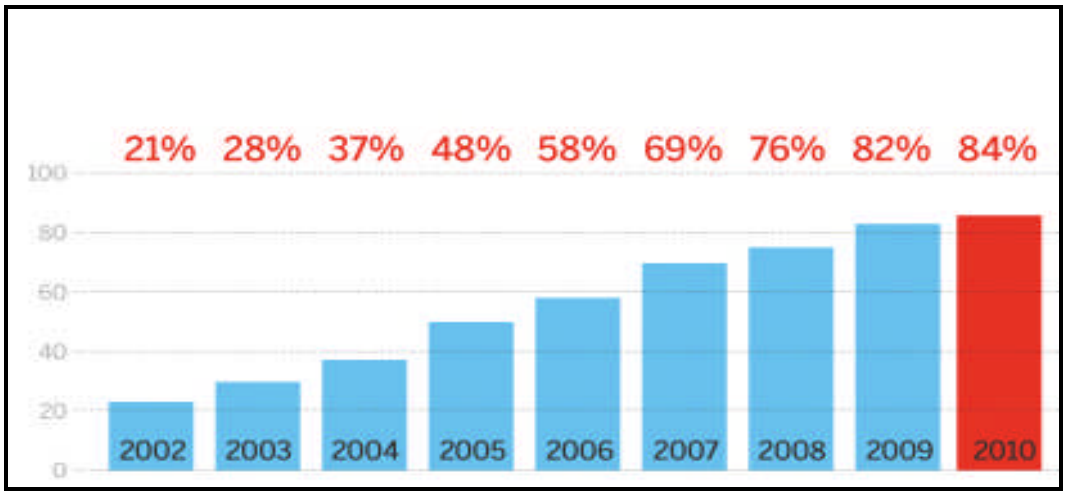


Figure 4: Broadband access in the U.S. Adapted from Internet Retailer, (2010b).

According to the Statistical Bulletin, Office of National Statistics, UK (2008), total internet sales increased in 2008 by 9.8% as compared to 7.7% in 2007. The value of these sales stood at £222billion compared to £163billion in 2007.

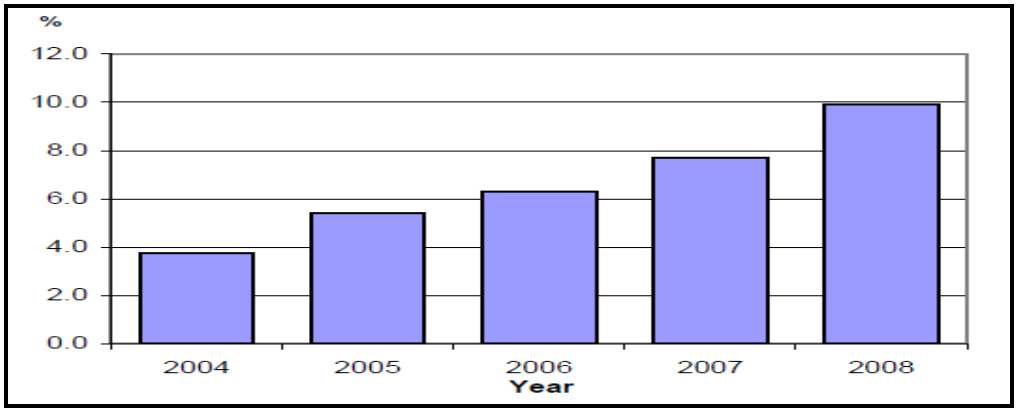


Figure 5: Internet sales in the UK, as a proportion of total sales, 2004 to 2008. Office of National Statistics, UK (2008).

2.6 Web 2.0:

Many of the features present on the internet today, including e-commerce and many business functionalities, are supported by virtual applications and social technologies, and one of these applications is known as Web 2.0 (Rudman, 2009). The internet started out in the 1990s as a means to transfer files and support emails among remote computers. The internet was used to display simple pages and users could go to different web sites as pages were linked electronically. This can be said to be the Web 1.0 – the first web (Laudon and Traver, 2009).

The internet has evolved to the point where the end users are capable through interactive technology to create, share, edit, and distribute contents on the internet to millions of surfers and build online lives and communities. This new web phenomenon is given the name "**Web 2.0**" which has already moved into the main stream, with well known and celebrated companies embracing it (Burton, 2008).

The figure below compares the workings of Web 1.0 with Web 2.0 and shows a clear evolution in the internet technology which has developed the web culture where interactions between users and webmasters is no longer limited to just direct means of communications, instead a whole new system of social interaction and communication has evolved using syndications such as RSS feed and other social networking websites (Hamid, 2007).

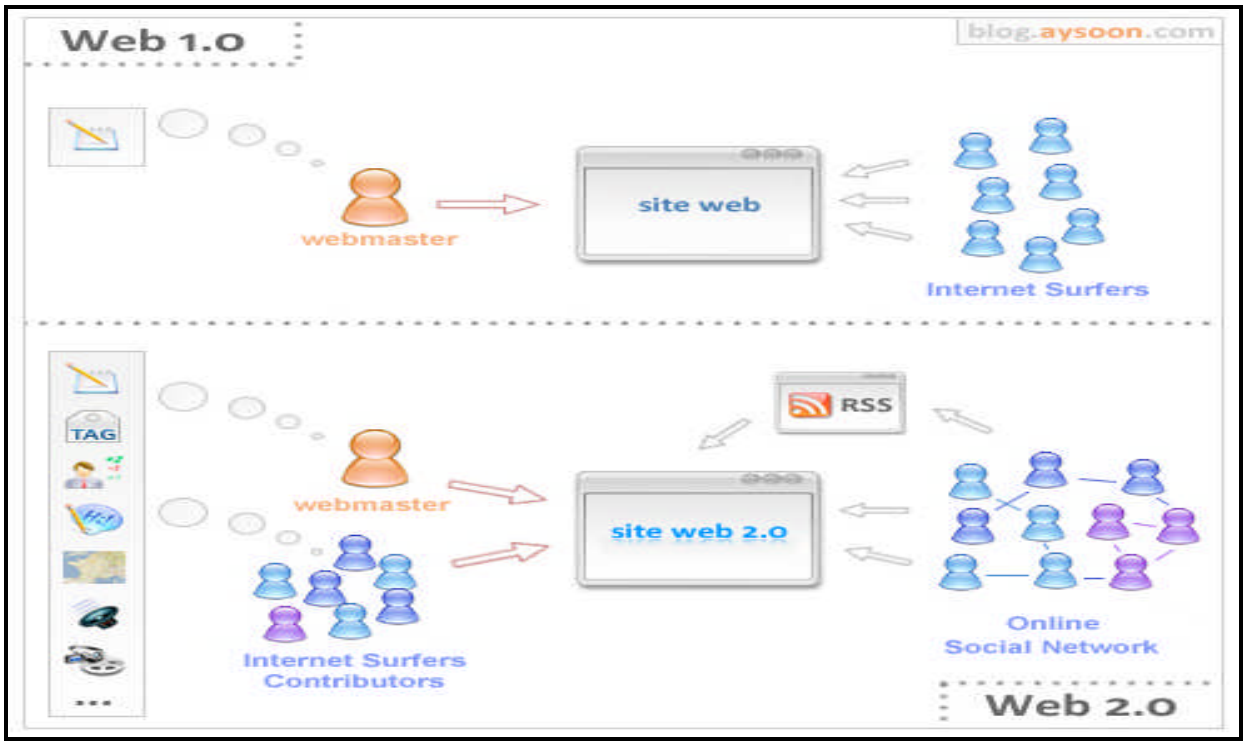


Figure 6: Comparison between Web 1.0 and Web 2.0 applications (Hamid, 2007).

While Web 2.0 draws heavily on the old Web 1.0, it is however a clear advancement from the past. Some of the examples of Web 2.0 in form of websites and applications are briefly explained below (Laudon and Traver, 2009):

1. YouTube, which is owned by Google, has grown to be the largest online user generated video posting site.
2. Facebook founded in 2004, is a social networking website which has expanded massive popularity and has surpassed 400million users worldwide in this short span of time (www.facebook.com/press.php).
3. MySpace maintains being the second largest online social networking site with active members in access of 125million worldwide.
4. Google being the most famous and commonly used search engine, has approximately 780million users worldwide (Kawamoto, 2009).

According to McKinsey Quarterly (2007), Web 2.0 offers the following technologies:

- ***Blogs:*** short for (web logs) and include online journals, diaries often hosted on websites and distributed to other sites using RSS feed.

- ***Mash-ups:*** is the collection or aggregation of contents from different online sources and put together in one place as a new service.
- ***Podcasts:*** collection of videos and audio recordings distributed through aggregator, such as iTunes.
- ***RSS (Really Simple Syndication):*** allows users to subscribe to online news, podcasts, blogs etc.
- ***Social networking:*** allows users of a particular networking site to share information, knowledge, and learns about other members. Some examples include Facebook and LinkedIn.
- ***Wikis:*** are systems of collaborative information gathering and publishing. Wikipedia allows many authors to contribute to a profile, discussion, topic, or a document.

2.7 Internet and E-commerce Security:

The effective operations of the internet, the web and e-commerce applications largely depends on the security cover that they can offer. Security issues and threats currently surfacing the global e-commerce market include access control abuses, data alterations, integrity violations, data contamination, damage, fraud, denial attacks, and infrastructure attacks etc (Clifton et.al, 2002).

Computer security, especially for the purpose of securing e-commerce transactions, is a complex and broad issue and research on logical security such as antivirus, and software etc is an ongoing process and needs regular review (Schneider, 2002). It is generally clear that the internet is revolutionising the way businesses are being carried out online, and that e-commerce technologies are being improved and developed every day, but the current internet security technologies and backup plans be unsuccessful to meet the needs of the e-customers and end users (Al-Slamy, 2008).

2.7.1 The Players:

As Khusial and Mckegney (2005) explain in a very simple and logical manner, an e-commerce transaction typically has the following 4 major players:

1. **Player 1 (SHOPPER):** is the shopper who visits a website, browses a catalogue and makes a purchase.
2. **Player 2 (B2C WEBSITE):** the site is operated by a trader, also a player, whose business is to sell the products and make profit.
3. **Player 3 (SOFTWARE VENDOR):** the trader business as in Player 2, sells goods and services but does not develop their own software. This software they buy most from a third party software vendor. This software vendor is the last of the three legitimate players.
4. **Player 4 (ATTACKER):** The attacker is the player whose main goal is to exploit the three legitimate players and make illegitimate gains through:

- *Blockading the players.*
- *Damaging resources through different schemes.*
- *Attack vulnerable points of the systems.*

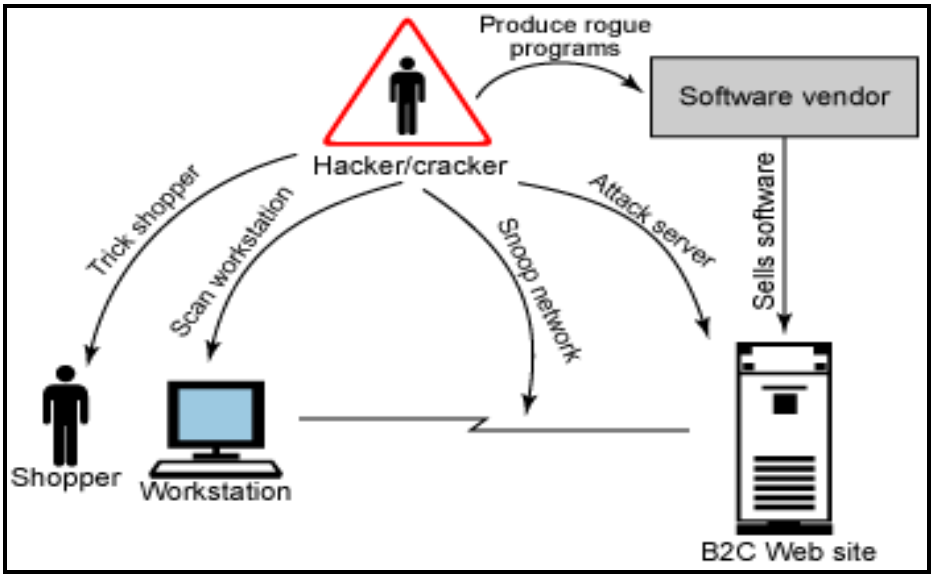


Figure 7: Points the attacker can target. Khusial and McKegney (2005).

The figure above shows how an attacker can target the vulnerable parts of the e-commerce system. The attacker can target points such as:

- The shopper.
- Shopper's computer.
- Attack network connection between websites and shoppers.
- Website server.
- Software vendor.

2.7.2 The scope of the problem:

Over the years cyber crime has become an important problem for both customers and organisations and researchers have been warning about the dangers of intentionally deceptive practices on the internet (Grazoili, 2004). Malware, Denial of Service attacks, Phishing (financial or personal information obtained from victims usually via emails), identity theft, spyware and credit card fraud are just some of the internet crimes that have been creating every day headlines (Laudon and Traver, 2009).

The internet has some technical problems; many of these can be traced back to communication protocols (Chou et.al, 1999). These set of protocols are the laid down rules on the basis of which networks interact with each other. One of the main protocols in use today is TCP/IP, and unfortunately there are many vulnerabilities and weaknesses associated to this protocol. Chou et.al (1999) pins down the following weak points of this protocol:

1. Failure to confirm identity and personality of communication parties.
2. Lack of ability to save and protect confidentiality of data on the internet.

As certain businesses may be undecided in divulging crime reports due to fear of losing confidence of their consumers, it becomes difficult to quantify the exact amounts of cash being lost due internet frauds.

According to CyberSource Annual Online Fraud Report (2010), between 2006 and 2008 revenue losses in the U.S and Canada, combined reached an estimated figure of $4 billion due to online payment frauds. The report also suggests that as the U.S

post recession economy is showing signs of recovery, there is a likelyhood of an increase in the number of online payment frauds, leading to higher fraud losses.

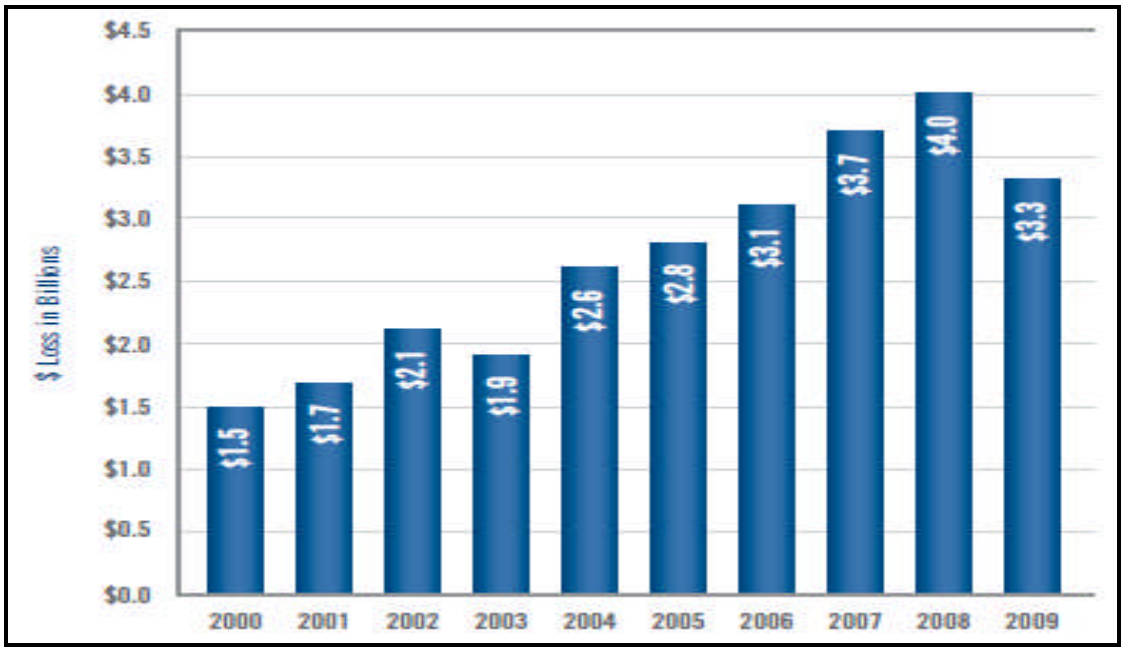


Figure 8: Online revenue losses due to fraud in the U.S from 2000 to 2009. Adapted from CyberSource Annual Fraud Report (2010).

The trend suggests that the online fraudulent losses have declined from $4billion in 2008 to $3.3billion in 2009, showing a fall of approx 18%. IC3 (Internet Crime Complaint Center), 2009, in collaboration with National White Collar Crime Center and the Federal Bureau of Investigation (FBI), suggests that between January 2009 till December 2009, IC3 received 336,600 complaint submissions which meant an increase of 22.3% as compared to the complaints in 2008.

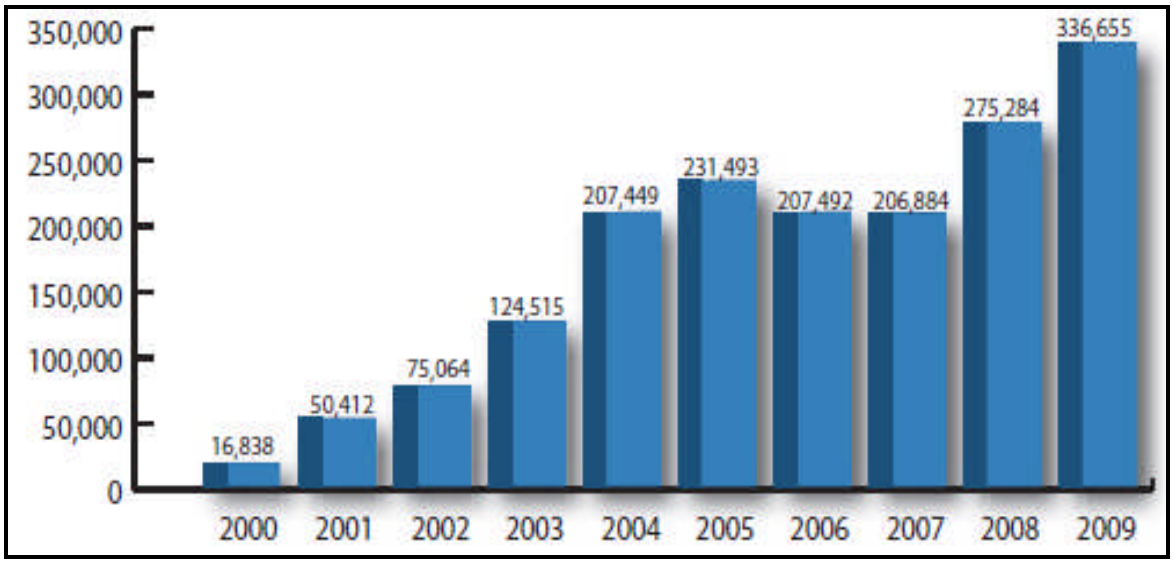


Figure 9: Yearly comparison of complaints received via the IC3 website. Adapted from IC3 Internet Crime Report (2009).

An interesting fact mentioned in the IC3 (2009) report is the average financial loss that is incurred by the complainants contacting IC3. The report suggests that out of 146,000 referrals during 2009, 100,296 of the cases reported having financial loss. The full amount dollar loss during 2009 reported to law enforcement by IC3 was $559million, compared to $264million in 2008.

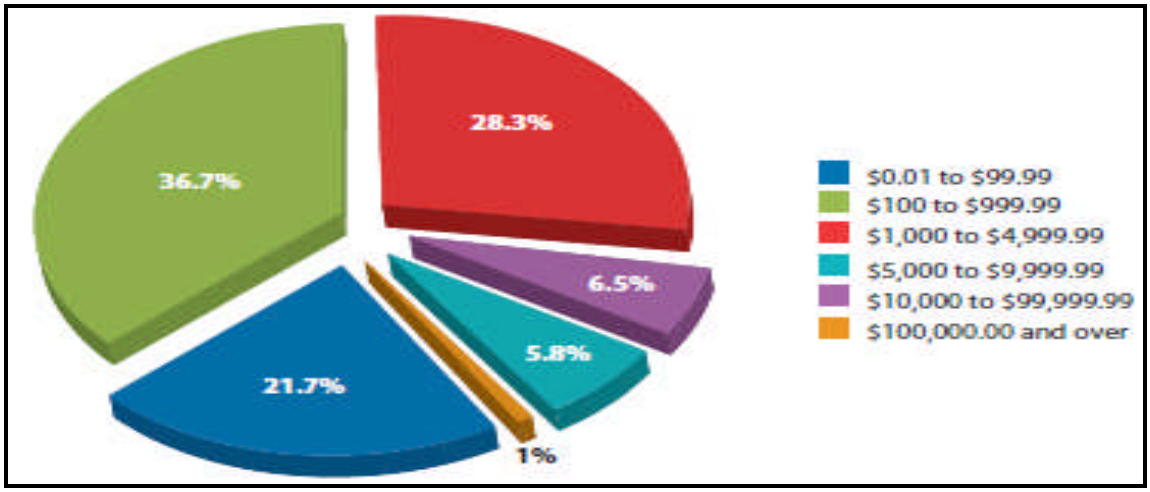


Figure 10: Percent of referrals by monetary loss. Adapted from IC3 Internet Crime Report (2009).

The highest dollar loss category per complaint was recorded by ***Overpayment Fraud*** with an average loss of $2500, ***Investment Fraud*** with an average loss per

complainant of $1850 and ***Advance Fee Fraud*** with an average loss per complainant of $1500.

Similarly the figure below shows the non delivery of products as the most reported to IC3, comprising 19.9% of all complaints of crime. Identity theft represented 14.1% of complaints. Credit/debit card fraud made up an extra 10.4% of complaints. It is important to mention here that according to IC3 reporting, complaints may not always provide correct picture of the nature of crime. It depends on the awareness of consumers, and individuals may describe an incident in different ways.

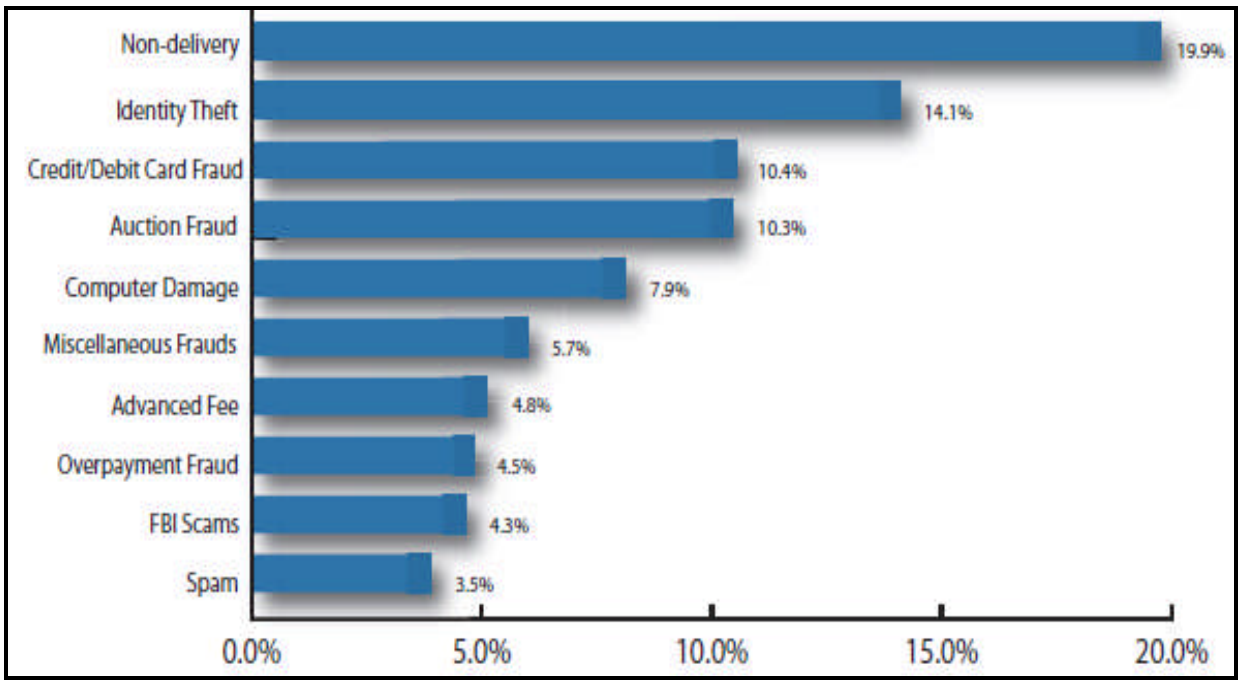


Figure 11:2009 top 10 most referred IC3 complaint categories (percent of total complaints referred). Adapted from IC3 Internet Crime Report (2009).

Apart from the importance of measuring the financial losses, it is also necessary to have an insight into who are the actual criminals (IC3, 2009). The report suggests that the majority of crimes carried out originate from within the U.S while criminals carrying out internet frauds have also been identified as residing in the Canada, Nigeria, Malaysia UK and Ghana. The figure below gives a picture of the

percentage of criminals carrying out internet fraud from different parts of the world.

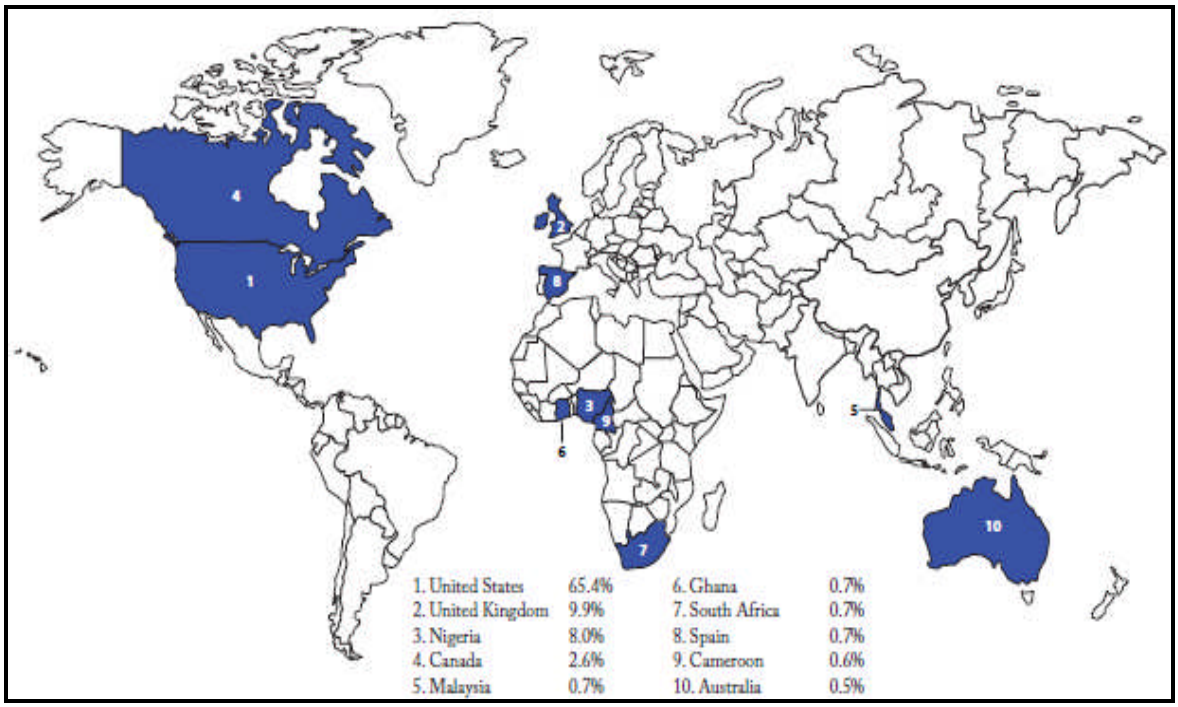


Figure 12: Top 10 by countries by count: Criminals (Numbered by rank). Adapted from IC3 Internet Crime Report (2009).

2.7.3 Security Problems and Threats in E-commerce Environment:

Over the past few years internet crimes have become more sophisticated, advanced, organised, and motivated by financial gains (VeriSign Inc, 2004). The attackers are not only gaining more knowledge and being more creative, they are also expanding their network and becoming increasingly more persistent.

Spam has become increasingly aggressive, and is a primary vehicle for each of the webs identity theft crimes, such a fee fraud, credit card frauds, phishing fraud, etc (Schneider, 2002). Identity theft is a way of stealing personal information of an individual, with intention to commit fraud or a crime. Traditionally identity theft is carried out by accessing information acquired from public records, credit cards, improper use of databases, shoulder surfing, and business record theft. With identity theft, an attacker can misuse the information in the following ways (OECD, 2008):

- ***Misuse of existing accounts:*** Attackers may use victims existing accounts including, credit card accounts, email accounts, other payment accounts etc.
- ***Opening of new accounts:*** the attackers can use a victim's information to open new accounts, loan accounts, insurance accounts, and telephone accounts etc.
- ***Commit other fraud:*** the information can be used to get medical treatment, passing it on to the police when charged with an offence, using it in obtaining government benefits or employment opportunities etc.

Examples of e-commerce threats are explained below:

1. **Malware:**

   Malicious Software, or malware as it is known, includes a variety of threats such as Computer Viruses, Trojan Horses, Bots and Worms (Barik, et.al, 2005). The use of malware in the past was often intended to harm computers, spread by lone hackers, but recently the intentions have been motivated by financial greed and email fraud where logon credentials, stealing personal information etc, are being hacked for this purpose (Laudon and Traver, 2009).

- ***Virus***: viruses are the most publicised threat to client systems (Tront and Marchany, 2002). A virus is a program that has the ability to replicate itself and spread over the system and infecting other files.
- ***Worm***: A worm is also a type of virus, but instead of spreading from file to file, it is designed to spread from computer to computer.
- ***Trojan Horse***: Trojans are not as harmful as viruses, nor do they replicate, but their aim is to break the working of a computer's operating system. Hackers use this tool to control, examine, and target any information on a target computer (Tront and Marchany, 2002).

2. **Spyware:**

   Spywares allow attackers to perform a detailed watch and control of their target which helps them to plan a complex identity theft, such as apply for fraudulent loan or mortgage in the victims name (VeriSign Inc, 2004). The attacker can easily obtain email copies, user's keystrokes, and take screenshots to capture username and password or any other confidential data.

3. **Hacking and Destroy:**

Gaining illegal access to a computer system or a domain is called hacking (OECD, 2005). The term ***cracker*** is usually used to indicate a hacker having a criminal goal, although both terms are used interchangeably (Laudon and Traver, 2009). Hackers typically break into government websites while others commit cyber vandalism by destroying, unsettling, and damaging websites.

5. **Sniffing attacks:**

These attacks are meant to monitor the data transfer between the vendor's server and the shopper's computer. It's a class of eavesdropping program that records information that passes through the network. This way the attacker gathers data easily about the shopper such as credit card details and personal information (Khusial and Mckegney, 2005).

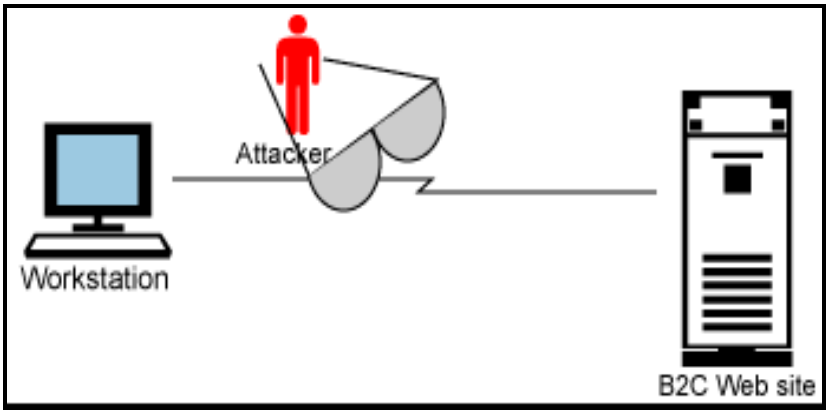


Figure 13: Attacker sniffing information between the shopper and server (Khusial and McKegney, 2005).

6. **Denial of service (DOS) attacks:**

DOS are the most common type of attacks available on the web. These are highly effective and are the simplest means to implement threats and which work by flooding the website or email message boxes with useless and heavy traffic to overcome and slowdown the network (Tront and Marchany, 2002).

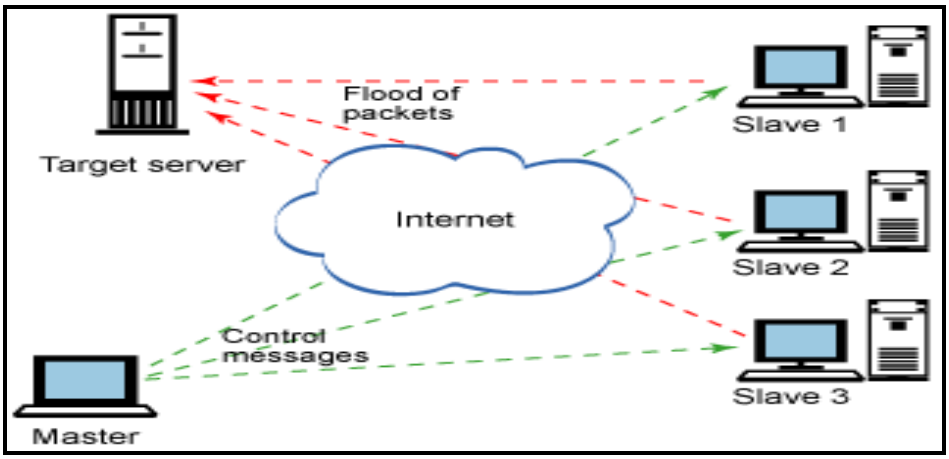


Figure 14: Denial of service attacks (Khusial and Mckegney, 2005).

Figure 14 above gives a comprehensive image of the nature of DOS attack. In this kind of crime the hacker damages the computers on the internet through malware attachments, viruses or other means. The infected computers are then controlled by the criminals and hackers and at a determined time they attack the server with useless and resource intensive needs. The attack not only disrupts the targeted server but also affects the performance of the entire internet.

7. **Credit card theft/fraud:**

Credit card fraud has been a worldwide threat for many years. Its effect is not just limited to the victims but also the credit card companies and the businesses (Barker et.al, 2008). Fear that the card information may be leaked on the internet makes many users hesitant in using their cards online. According to the online theft report by IC3 (2010), 10.4% of all reported complaints are relating to credit card frauds. Today the most frequent cause of credit card thefts is the hacking and stealing of the corporate servers and information regarding millions of cards is stolen and statistics from Association of Certified Fraud Examiners (ACFE) have shown that credit card crimes had reached an estimated figure of $3billion in U.S alone (Barker et.al, 2008).

2.8 Summary:

This chapter covers and discusses the fundamentals of e-commerce and e-business. The growth of e-commerce has granted timeless opportunities to entrepreneurs in expanding their business horizon while offering consumers a new medium to connect with business online in transacting goods and services. The chapter covers the history of e-commerce, types of transactions done on e-commerce platform, current trends in the e-business technology and so forth.

The significance of this chapter lies in the fact that it discusses key security issues faced by internet usage and linking it with one of the most disturbing crimes currently making news around the globe, called as phishing. The chapter also discusses the scope of this crime and gives some references of certain internet crime reports to show the scale of the problem. Some of the other security threats being faced by businesses and consumers are also highlighted later in the chapter.

CHAPTER 3

LITERATURE REVIEW

3.1 PHISHING: A SOCIAL ENGINEERING ATTACK

Social engineering attacks are those that take advantage of human interaction. The word social is used here because it involves an attacker's social skill to trick the victim into a carrying out a compromising activity, such as revealing personal information or accessing an infected email (Kanellis, 2006). It can also be said that social engineering attacks are often simple and low technique but they can cause huge amounts of damage to society as they are surprisingly effective if executed well. In the past social engineering attacks were carried out through the use of telephone, but these days emails have taken over due to low risk and low cost of spreading these among masses. Recently, a type of social engineering attack called phishing has gain frequency and has spread across the online world in the last decade.

Phishing is one of the more threatening and therefore successful social engineering techniques available to e-commerce hackers around the world (Granova and Eloff, 2005). This problem on the web is continuing with no signs of reducing and the volume of phishing attacks worldwide is likely to increase. (Price, 2008).

Phishing is a type of online identity theft where an individual's confidential information such as user name & password, social security numbers, credit card information bank account numbers, and other relevant information are obtained through fraudulent means (Emigh, 2005). The attacker's objective is to convince the victim, through the use of deception techniques; in disclosing their private information and credentials, so that the phisher can use them to carry out malicious acts, mainly financial fraud. (Youl, 2004).

According to a Kaspersky Lab Ltd, (2006), Phishers replicate a chosen financial institutions website that is almost 100% perfect. They use legitimate logos of the institutions, good business style and even make references of real names of the people from the senior management of the institution. Tippingpoint.com (2005),

reports that the global fraud losses caused by phishing range from $500million to $2billion approximately.

3.2 DEFINITIONS OF PHISHING:

A comprehensive definition by Granova and Eloff, (2005) states phishing activity as:

"The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft".

Similarly Anti Phishing Working Group (APWG, 2009), defines phishing as:

"Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials".

APWG further explains that social engineering methods use email spoofing reflected to being sent from legitimate sources and leads consumers to fake websites and attract them into divulging private information and financial data. On the other hand the technical trick employs schemes where crime ware is planted onto computers to steal credentials directly and often uses systems to intercept consumers online account information such as username and password, while misdirecting the consumers to fake websites, where the attackers monitor their behaviours through controlled proxies.

3.3 A TYPICAL PHISHING ATTACK: THE MECHANICS

According to Jakobsson and Myers (2008), phishing attacks can generally be characterised by three components: the lure, the hook, and the catch. These are explained below.

3.3.1 The Lure:

The phishing process starts when spammers attract online users with emails that in a convincing way appears to be from a legitimate website. The emails have links encouraging the recipient to click on them and follow instructions. The hyperlinks on these emails are controlled by the hackers and request the user to provide

certain private information. The hyperlinks present on these emails often mark a spoofed URL of a legitimate website (Price, 2008).

The figures below show that the attackers go on in instructing the users not to share their information such as username and password, and to make reasonable effort in protecting those. The statement on the fraudulent webpage gives useful advice to make the lure convincing enough. If a user follows such advice, these phishing scams would not harm them as they would be taking precautions (Youl, 2004).

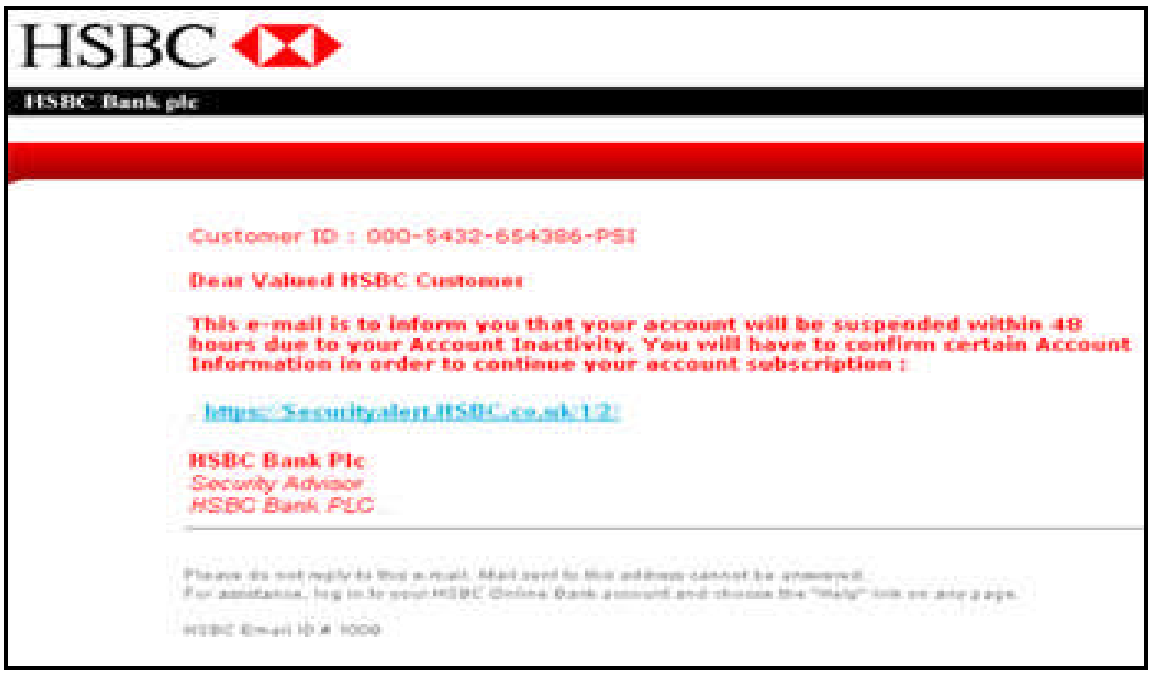
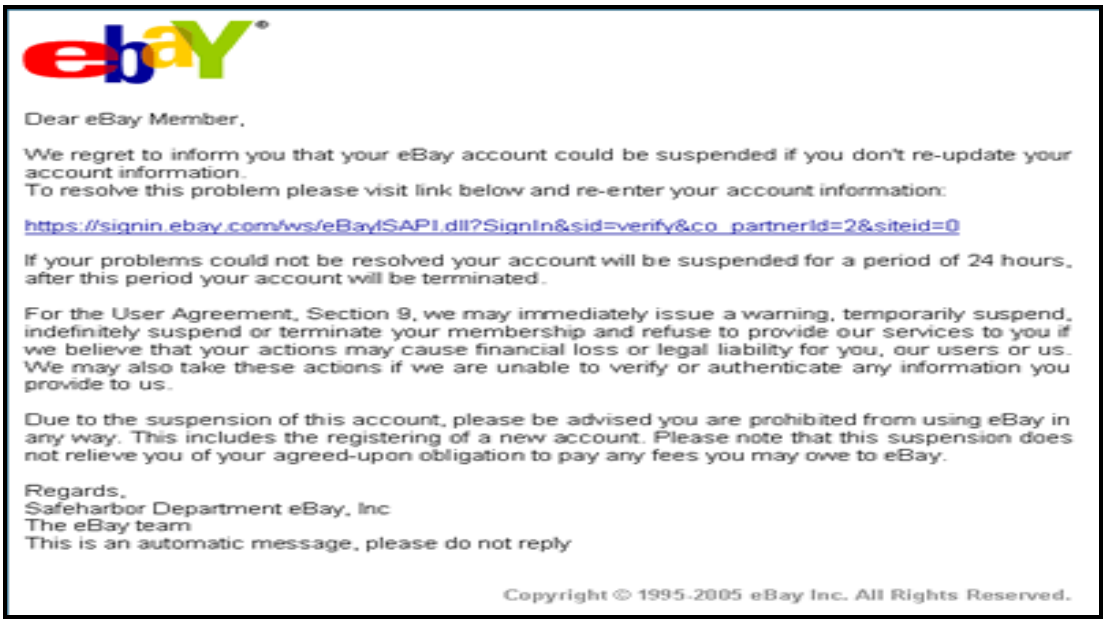


Figure 15: Examples of Phishing. Adapted from Spam-ip.com/phishing-examples.

3.3.2 The Hook:

The hook typically consists of a malicious website that is designed to look like a legitimate institution website. The main aspect of the hook is that it is designed to look exactly like the original and is as impossible to differentiate from the target as possible. These websites then ask and convince the user to divulge information which is private and confidential in nature such as username and passwords, account numbers etc. Most often the hook is similar URL which looks exactly like the targeted legitimate website, which actually is controlled by the attacker (Fitzgerald, 2008).

The fraudulent websites are designed to look exactly like the real pages, the one it is trying to mimic. This idea of imitating a legitimate webpage is known as web spoofing (Wheelock, 2005).



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Copyright © 1995-2005 eBay Inc. All Rights Reserved.

Figure 16: A sample bogus e-mail. Adapted from: Tips for quickly spotting and avoiding phishing scams (Pacchiano, 2010).

3.3.3 The Catch:

At this point the attacker gets hold of the user's information collected from the hook and uses this for carrying out dangerous intentions such as identity theft or illegal financial fraud (Price, 2008). The more personal and financial information that is gathered by the attackers the more benefit that can get back from the exercise. This is because more information gives the attackers to commit fraud easily and with a lot of freedom, as just a name of credit card holder and number isn't enough in carrying out a fraud without having the victims complete billing address and 3 digit security number (Montalbano, 2007). The attackers face risk in this kind of fraud as someone amongst them has to pick the purchased goods or the transferred money, and for this purpose they usually ship the goods to (Jakobsson and Myers, 2008):

1. International locations with no electronic fraud laws.
2. Locations with such fraud laws but not being strictly enforced.

3.4 WHY DOES PHISHING WORK?

The technical skills of the attackers or criminals are far from being the only reason why phishing works and grows so increasingly (Harley and Lee, 2007). It can be said that the general levels of phishing presentations have improved dramatically, but still the continuing success of Nigerian (419 type) scams, suggest the fact that poorly presented fraud cases does not always reduce gullibility (Peel, 2006). Social engineering techniques are equally relevant, perhaps the most important element that makes a crime successful is simply because the victims are not educated enough and remain aloof and confused about the nature of the problem (Hearst, et al. 2006). Some of the reasons how phishing keeps growing are explained below.

3.4.1 Lack of Knowledge:

Many users lack the underlying knowledge as to how their PCs operating system, emails, and web applications work. The attackers exploit such ignorance and make gains out of it. Simple indicators such as legitimate and fraudulent URLs and email headers are not even understood by most of the online users. Similarly users do not understand the security indicators on their web browsers. For example, SSL certificates and padlock icons indicate that the page viewed is securely delivered by SSL. The figure below shows the padlock icons on the browser address bar.

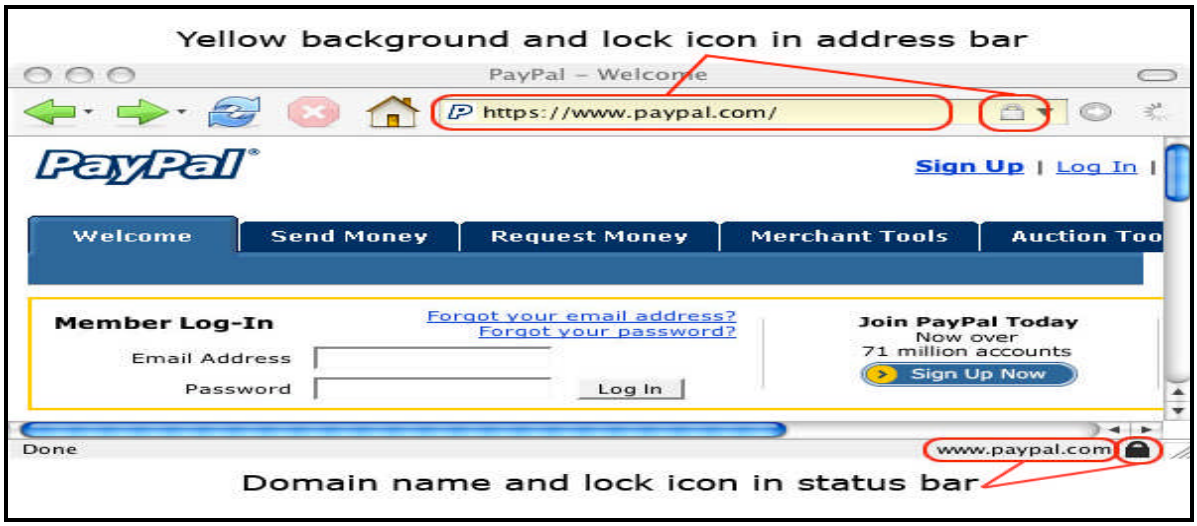


Figure 17: Visual Security Indicators in Mozilla Firefox (Hearst, et al. 2006).

3.4.2 Visual Deception:

Attackers use smart visual deception tricks and techniques to mimic legitimate text, images, and web pages. Users get fooled by deceptive syntax texts such as e.g. www.lloydstsb.com instead of www.lloydstsb.com . Similarly images are used to mask the underlying tests and also images with deceptive look and feel that mimic browser windows.

3.4.3 Bounded Attention:

Even if the users are aware and have knowledge and can detect visual deceptions mentioned above, they may get fooled if they fail to understand the security indicators. The security indicators shown in Figure 3 are not easily noticeable when users are focused on their primary tasks. Similarly users do not reliably notice the absence of these padlock security indicators.

3.5 HOW DOES PHISHING WORK?

Phishing scams work when attackers transmit large numbers of fraud emails targeting many users. These emails have web links which are under the control of the attackers, and when a user clicks on the link, he or she is presented with the fraudulent webpage mimicking the legitimate page of the institution, and this way they acquire the information passed on to them by the victims themselves (Moore, 2007). According to Emigh, (2005) the phishing process can be explained in 7 steps from start to finish:

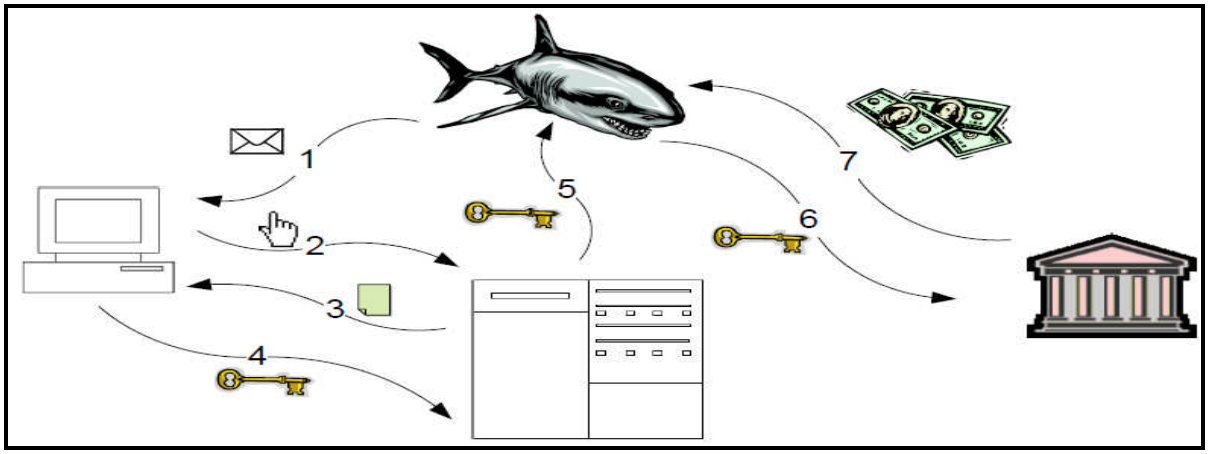


Figure 18: Seven Steps of the Phishing Process (Emigh, 2005).

1. The phisher starts and prepares for the attack. A malicious email arrives from some transmission source.
2. The users take action by responding to the email, making them vulnerable to an information compromise.
3. The users are encouraged/ prompted in divulging confidential information, either by a remote site or a web Trojan.
4. The users get lured and enticed by the fraudulent web content and confidential information is then compromised.
5. This security, financial, or confidential information then moves on and transmitted from malicious servers to the attackers.
6. This information once received is used to impersonate the victims and get access to the confidential material.
7. The attackers then use this information in committing financial frauds and crimes and therefore get monetary benefits.

3.6 WHO IS BEHIND PHISHING FRAUDS?

According to the IBM Developer Works, (2010), there are different types of phishers, attackers, hackers, or also called as crackers.

3.6.1 Script Kiddies:

Despite the name, script kiddies are hackers that are beginners in this field and has nothing to do with age. They have fewer skills and resources in carrying out attacks. These attackers have little information, expertise, and knowledge of the system they are attacking. They usually use tools employed or developed by practiced hackers and think that they know a whole lot more than they really do. They are less threatening but that can create disaster on systems that are unprotected and unsecured (Rachael and Russel, 2005).

3.6.2 White Hat Hackers:

These are the technical and experienced hacker that attack systems just for the fun of it. They are often referred to being called as 'old school hackers'. While others call them as "good hackers", as they often help organisations and crime fighting

institutions to locate and fix security flaws (Laudon and Traver, 2009). According to Wiles, (2008), the Computer Security Institute, reported that in 2006 organisations reported losses of $52million due to breaches in computer security systems. These 'good hackers' are often employed by multinational and financial companies as 'penetration testers' (ethical hackers) to hack into systems to check for weak spots and later recommend ways in protecting the systems in preventing future attacks by actual hackers.

3.6.3 Black Hat Hackers:

These are similar to White Hat hackers in that they possess equal amounts of technical knowledge, but their intentions in attacking a system is more devious as they access systems for harmful and malicious purposes. They simply embarrass their victims, often big organisations, by means of destroying, corrupting and damaging their computer systems.

3.6.4 Grey Hat Hackers:

These hackers have similar skills as the white hackers, and their intentions are usually similar to that of the white hat hackers. But these hackers can become nasty and break into systems to accomplish their own agenda or revenge. They also break into systems and reveal system flaws by publishing them without disrupting the working of the systems (Rachael and Russel, 2005).

3.6.5 Terrorism and Hackers:

The linkage between terrorism and hackers is difficult to confirm, but membership in the most highly skilled hacking community is often very difficult and exclusive as these hackers possess, develop, demonstrate, and share highly sophisticated techniques and hacker tools. These groups remain off the limelight and often do not seek attention, and prefer maintaining secrecy as they may be involved or facilitating in vicious terrorist activities (Linden, 2007).

3.7 *THE SCOPE AND TRENDS OF PHISHING:*

Determining the exact cost of phishing attacks would be a difficult task. The total figure in order to be accurate requires inputs from all the quarters affected by phishing, and as many victims do not acknowledge being victimised due to fear of humiliation, or legal liability, it becomes a difficult task to compile the exact numbers (Abad, 2006). Certain published facts, losses, costs and trends of phishing are explained below.

A leading multinational group known as Anti Phishing Working Group (APWG) focuses on phishing and issues quarterly reports on global phishing trends. According to the APWG (2009) report:

- Number of phishing reports submitted dropped from 40,621 in 3rd quarter of 2009 to 28,900 in the last quarter of 2009.
- 46,000 unique phishing emails were received during the last quarter of 2009.
- The financial industry is the most targeted, receiving 39% of the total phishing attacks. Followed closely by the payment industry at 33%, and then the auction industry by 13%.
- USA leads all the countries hosting the most number of phishing sites with 72.9% of the total phishing traffic. China is 2nd at 5.25% of the world's phishing websites followed by Canada at 3.65%.

According to the Symantec Global Internet Security Threat Report, (2010), USA and China have ranked in the top two in malicious hubs. The figure below gives a detailed view of the country rankings involved in variety of crimes.

Overall Rank 2009	Overall Rank 2008	Country	Percentage 2009	Percentage 2008	2009 Activity Rank: Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Figure 19: Malicious Activity by Country (Symantec, 2010).

Brazil has witnessed a sharp increase in malicious activities during the last few years, forcing the country in proposing a new cybercrime bill tackling this crime. Similarly the report also suggests that India has moved from 11th position in 2008 to 5th in 2010 as the country is experiencing a surge in malicious crimes. Malicious activities in countries like the United Kingdom and Germany were found to be quite regular with previous year.

Similarly according to the report, 60% of the identity attacks in 2009 comprised of hacking. The majority of these attacks were caused due to the successful breach of a single credit card payment processor (Krebs, 2009), which resulted in theft of nearly 130million credit cards numbers.

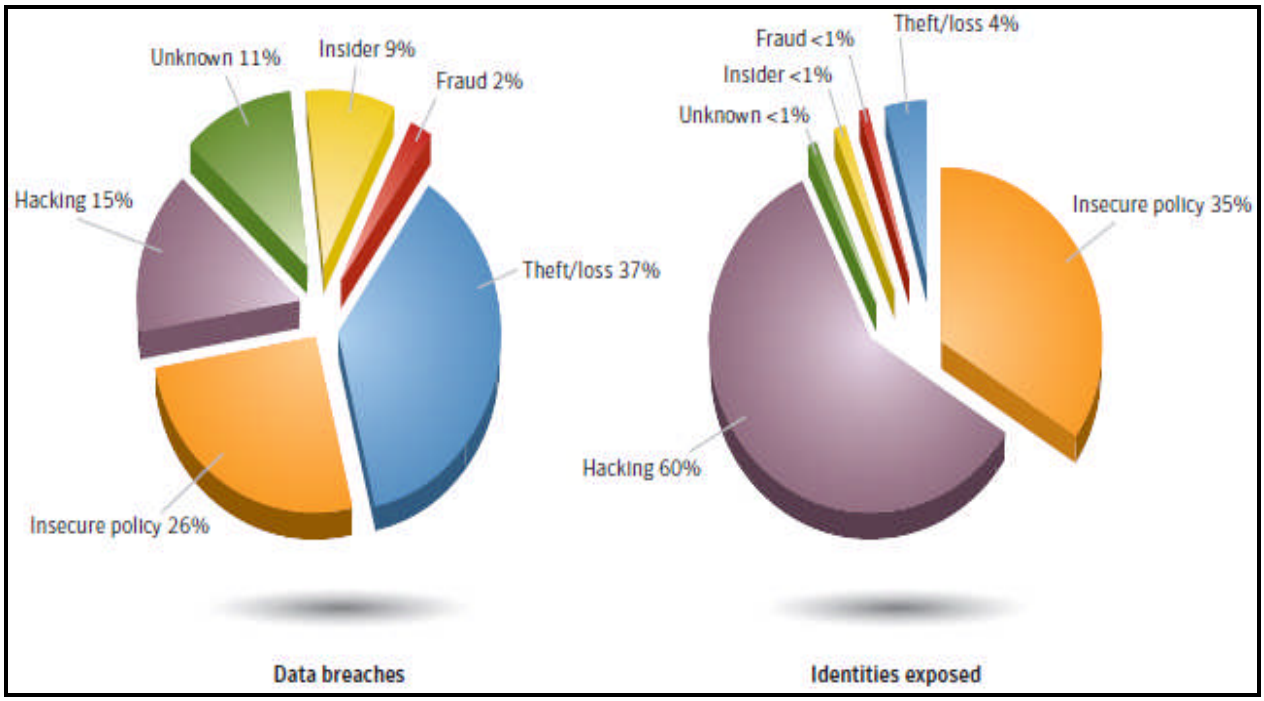


Figure 20: Data breaches leading to identity theft by cause and identities exposed (Symantec, 2010)

Certain other findings by the Symantec report (2010) are as follows:

- Symantec created 2,895,802 new malicious code signatures during 2009, an increase of 71% compared to signatures in 2008.
- Out of the top 50 malicious codes reported in 2009, 51% of the volume comprised of Trojans.
- Of all the phishing attacks in 2009, 74% accounted were targeting the financial services sector.
- 59,526 phishing hosts were detected by Symantec in 2009, an increase of 7% over 2008.
- In 2009, spam made up 88% of all emails observed.
- Mozilla Firefox had the most reported vulnerabilities in 2009 with 169, while Internet Explorer has just 45, but still Internet Explorer was the most attacked browser, as Symantec suggests, attacks on software is based more on the market share of the product and also the availability of exploiting areas.

3.9 TYPES OF PHISHING ATTACKS:

Phishing can be carried out in many different ways. Phishers have developed skills, are more innovative and with fraudulent monetary gains to support them, they can also afford to invest in sophisticated technology. Phishers employ different attack techniques varying as per the nature of the attack and the skills of the attackers. Different variety of phishing attacks utilising multiple technologies are explained below (Jakobsson and Myers, 2008):

3.9.1 Deceptive Phishing:

The most common mechanism in carrying out a deceptive phishing attack is through an email. In this form of attack, the phisher sends deceptive emails to multiple users and requests that they respond by clicking on a link provided in that email. The instructions on the email can include:

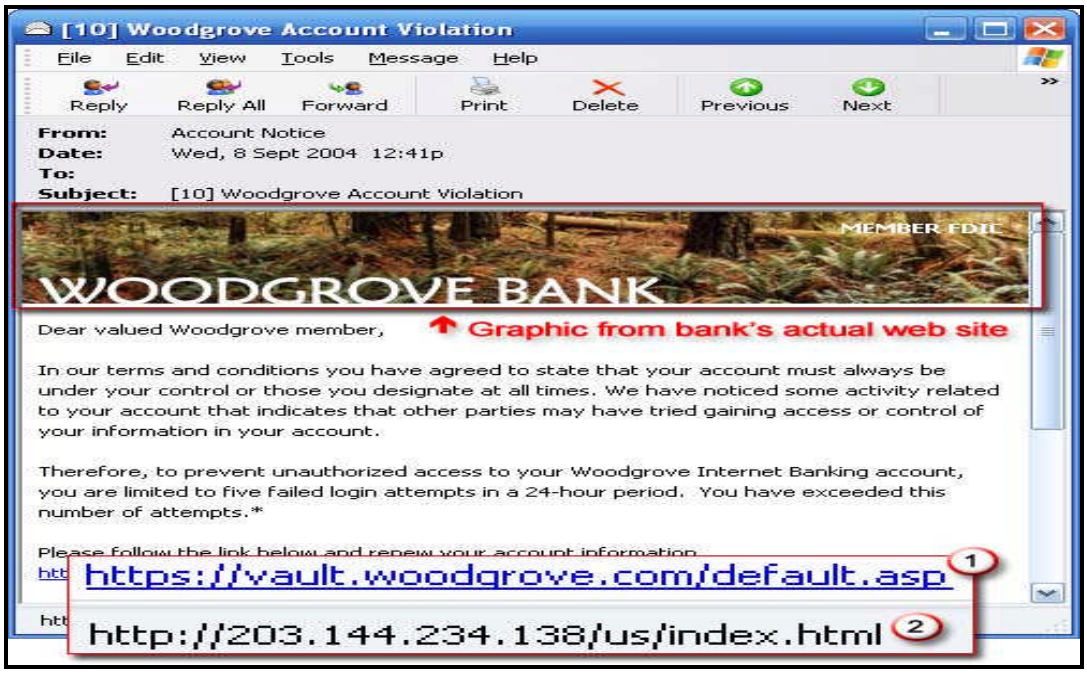


Figure 21: A typical Deceptive Phishing Email message (Microsoft, 2010).

- A statement that might suggest that the user's account is at risk of blockage or expiry.
- An invoice for merchandise with a link to "cancel" the order.
- A fraudulent notice to a user informing them of a change made to their account with a link to "dispute" the unauthorised change.

Figure above shows a deceptive email, where the attacker entices the users to fill in their confidential information by following a link. To make the phishing email legitimate, the attacker may place a link which appears to go with the legitimate website (1), but once clicked the link takes the user to a phony scam site (2), or maybe a popup window looking exactly like the official site. The information once received, can be used to impersonate the victim, or may resell the illegally obtained information in a secondary market.

3.9.2 Malware-Based Phishing:

Malware based attacks usually infects the user's machine with malicious software. Malware software is designed to steal personal information from computers without the user's knowledge. Malware is a typical social engineering attack, where the attacker encourages the user to open an email attachment from a fraudulent site (Rao, et al. 2007).

3.9.3 DNS-Based Phishing:

It is a type of phishing attack that corrupts and interferes with the domain name server (DNS). This also includes the corruption of the host file, although that is not part of the DNS. The DNS based phishing attack also corrupts the user's DNS cache with incorrect information and would direct the user to incorrect locations set by the attacker (Kerner, 2005).

The process of DNS-based phishing can be explained with the following example (McAfee.com, 2006):

1. The phisher sends out spam for www.phish-attacker.com
2. A DNS query is then made for www.phish-attacker.com
3. The www.phish-attacker.com DNS also returns data for www.thebank.com, which gets stored in DNS.
4. When anyone using the same ISP tries to connect to www.thebank.com, they get directed to www.phish-attacker.com.

[It should be noted that www.phish-attacker.com is imitating www.thebank.com in a near perfect and convincing way].

3.9.4 Content-Injection Phishing:

In this type of attack the attacker adds malicious contents into a legitimate website. This malicious content can be redirected to other sites and install malware on a user's computer. Three types of content injection phishing attacks are typically used (Jakobsson and Myers, 2008):

1. A server can be attacked and legitimate contents can be replaced or increased by malicious content.
2. Malicious content can be inserted into a legitimate site through cross-site scripting. This happens where phishers use errors in a legitimate website's own script against the victim (Frost and Sullivan, 2009). When injected the script directs the user to sign in to their own legitimate and trusted website, but in reality the link is crafted by the attackers to carry out the attack.
3. Content-injection attacks can also be spread by SQL injection vulnerabilities. This way database commands get executed on a remote server causing information leakages.

3.9.5 Man-in-the-Middle Phishing:

In man-in-the-middle attack, the phisher positions themselves in between the user and the legitimate web source. This is one of the most successful vectors for gaining illegal access to the user based information, by monitoring and observing all the transactions that the user makes (Ollmann, 2004).

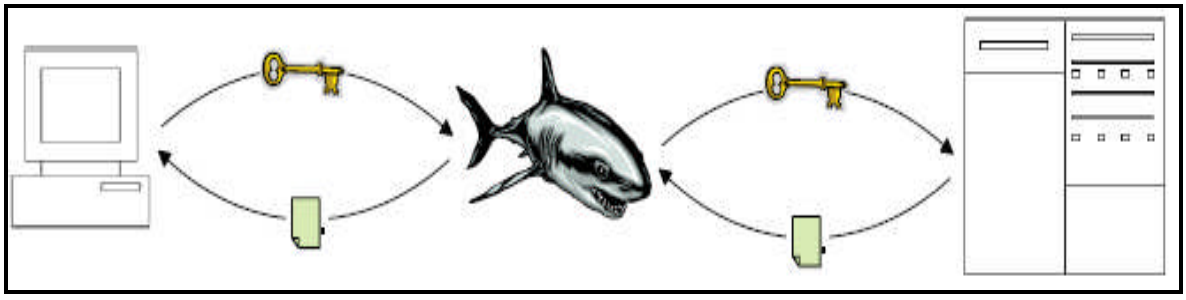


Figure 22: Man-in-the-Middle Phishing Attack (Emigh, 2005).

This type of attack is successful for HTTP communications. The attacker gains information when the user connects to the malicious server planted by the attacker, as if it was a legitimate website. The attacker server connects with the real website and proxies all information between the user and the legitimate web application server in real time.

3.9.6 Search Engine Phishing:

In this approach the attackers create web pages for fake products and get the page indexed by a search engine. They put the lure and wait for the users to fill in confidential information. Such pages usually offer products at prices that are too good to be true (Emigh, 2005).

3.10 ANALYSIS OF PHISHING E-MAILS:

According to Ollmann, (2004) the most common types of phishing attacks are started through emails. Through emails phishers can transfer malicious contents to millions of users. In most of the cases the list of addresses used to deliver email spam are purchased from sources as the conventional spam. Attackers use the well known errors in the common mail server and are able to create emails with fake headers and are able to impersonate any organization of their target.

Email delivery infrastructure is similar to that of a typical post office delivery (James, 2005). Successful delivery requires the user to have a routable address enabling the mail to be delivered. The mail server is similar to the human mail carrier, and mail client is the user walking up to their mail box to collect it.

3.11 EMAIL SPOOFING:

Spoofed emails are those that claim to be originating from one source when actually it was sent from another (Jakobsson and Myers, 2008). How does an attacker spoof a particular email address? They can because it's all present in the software (Miller, 2008). There are spoofing programs available today that makes the job easy for the attacker as they just have to insert the email address into the spam message's header. Spoofing creates a lot of problems for individuals and companies because when trusted sites are spoofed they are less likely to be filtered by a spam blocker and this way the user is more likely to access the spoof

when it seems to be coming from a trusted website they already know of. Phishers use these email spoofing techniques to lure users in giving away useful information. Some of the mechanics of spoofing used by attackers are explained below:

3.11.1 Using Company Image:

When attackers spoof a company, they not only claim to be from trustworthy company but also copy the visible branding. Many fraudulent website imitate images from legitimate websites. One sample fraud email pulled from EarthLink logo is shown below (Drake, et al. 2004):

”<img alt=”Yahoo!
Auctions”src=”http://www.earthlink.net/i3/gnav/earthlink_logo.gif”
border=”0” width=”299” height=”39”>

NOTE: *This is a spoofed EarthLink email, but the fraudster set the alternate text for the image to “Yahoo!” This type of error is another indication that this is a fraudulent email.”*

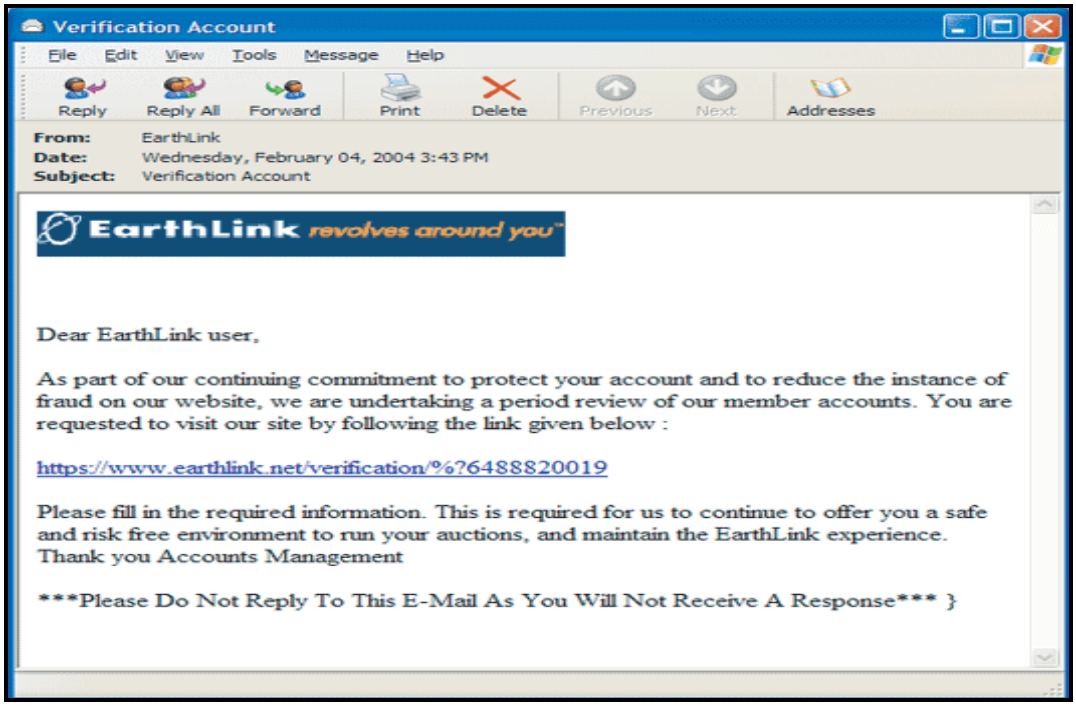


Figure 23: A sample phishing email (Drake, et al. 2004).

Similarly another example of PayPal email shown in figure below showed that the links in the email are of the actual PayPal website except for the "click here" link in the middle of the text.

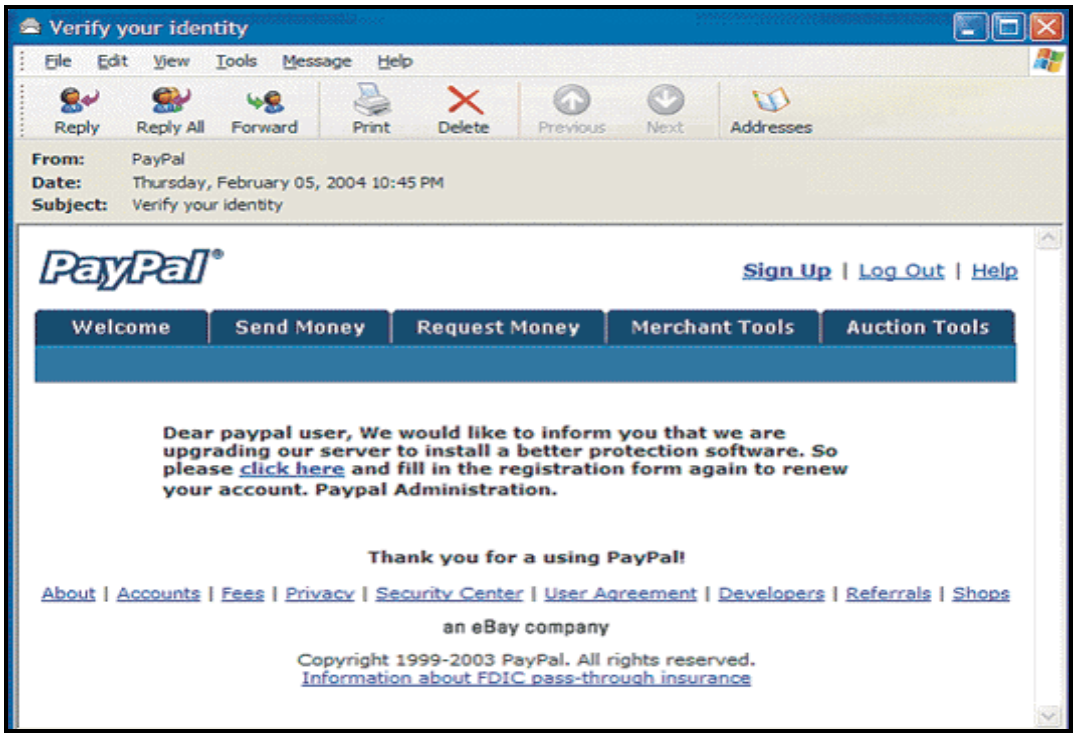


Figure 24: Sample phishing email. An example of PayPal scam (Drake, et al. 2004).

3.11.2 Forged Sender Addresses:

Forging of addresses is a successful deception technique. The email declares to be from a legitimate source but in true is set to reply to a fake reply e-mail address (Leyden, 2004). The following are some examples from fraud e-mails:

From: EarthLink Security Dept.
Reply-To: earthlink8770@1-base.com

From: Citibank
Reply-To: citibank3741@collegeclub.com

These phishing deception emails generally have forged sender addresses appearing as though they are sent from a legitimate institution. The figure below shows a Barclays Bank phishing email, and it can be clearly seen that the subject line, forged sender address, legitimate looking content and faked links, are all indications of a deception technique employed.

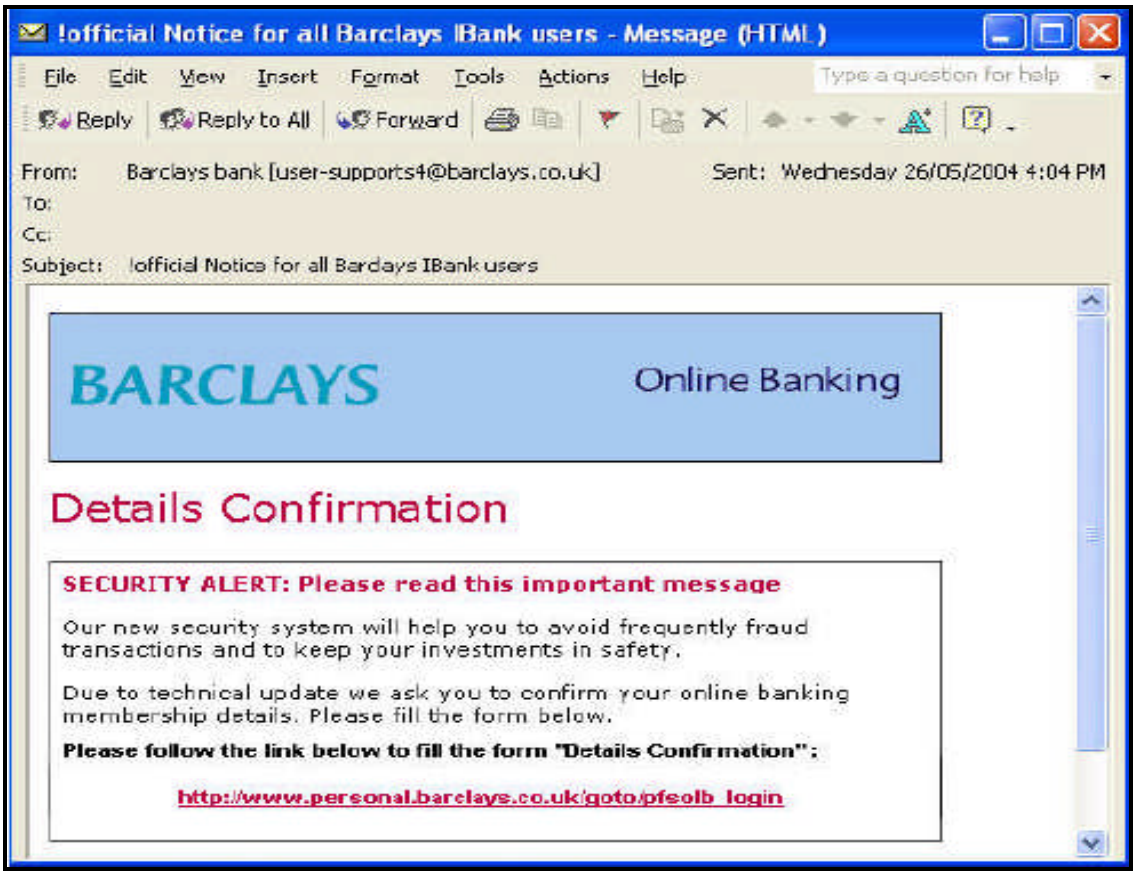


Figure 25: Barclays Bank Phishing email (Youl, 2004).

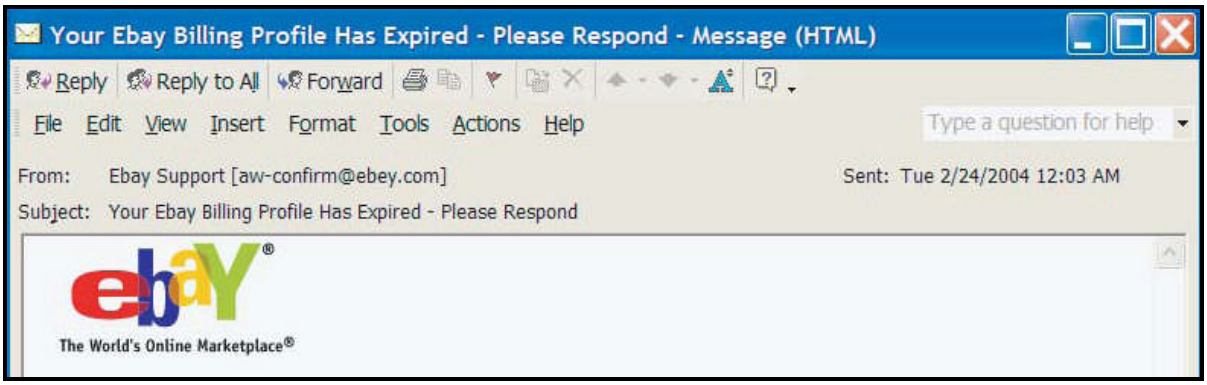


Figure 26: Fraudulent eBay email (Drake, et al. 2004).

The figure above shows an eBay fraud email that claims to be from eBay support team, but the reply email is shown as: aw-confirm@ebey.com . The attacker has also used "ebey" instead of "ebay".

3.11.3 Disguised Links:

Attackers use disguised links in the email to deliberately fool the users in getting caught into the hook. In text only emails, users do not notice the long URL's and

those having "@" before the actual website. For example a link may be displayed as:

"http://www.genuine-site.com-Verify83kcmdj30dk>Secure32902ds;lkjasdfkljad@fraud-site.com"

The URL above may look valid and legitimate but the address after the '@' sign means that it would take the user to www.fraud-site.com instead of www.genuine-site.com

3.11.4 Requiring a Quick Response:

The fraudsters have to get the required information from user as quickly as they can, before their sites are shut down. So for this purpose they pressurise and convince the users to respond quickly to their emails. For this purpose fraudulent quick response catchy lines in emails are used such as (Kirby, 2004):

"If you don't respond within 24h after receiving this Mail Information your account will be deactivated and removed from our server (your account suspension will be made due to several discrepancies in your registration information as explained in Section 9 of the eBay User Agreement."

3.11.5 Security Promises:

Phishers use clever techniques and usually assure users in emails that the transactions carried out are secure. It is a way of gaining the recipient's trust. The following email line is another way of gaining the trust of the users in divulging their personal information on the links provided (Kirby, 2004):

"Remember: eBay will not ask you for sensitive personal information (such as your password, credit card and bank account numbers, social security number, etc.) in an email."

It is also an interesting fact that email fraudsters use all kinds of symbols, logos, and signs to make their malicious web pages look legitimate. Fraudulent websites also use the TRUSTe symbol at the bottom of the emails (Drake, et al. 2004):

This symbol is meant to be used by those businesses that agree to maintain high standards in securing consumer confidentiality and personal information. (For details see http://www.truste.org/). This symbol is also used by attackers to make their website look authentic and secure. This symbol is used in the following fraudulent websites:

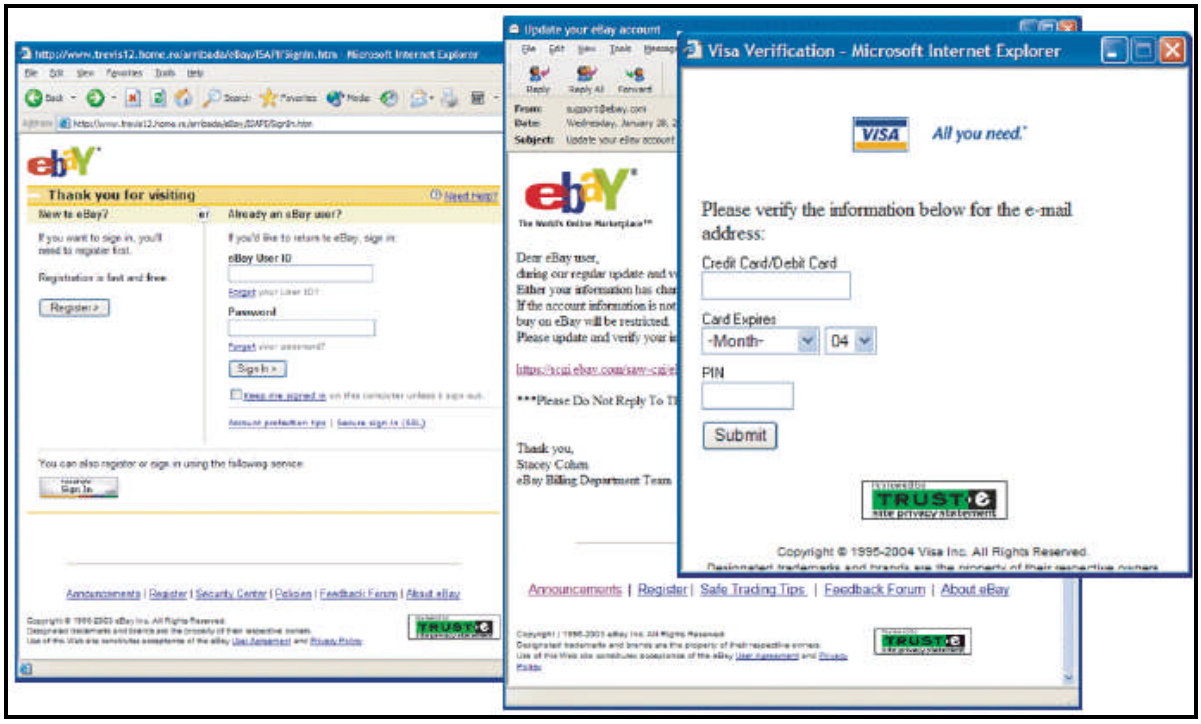


Figure 27: TRUSTe symbol used by different fraudulent websites (Drake, et al. 2004).

3.11.6 Hiding Host Information:

Fraudsters sometimes use tricks by inserting null or other unprintable characters before the "@" symbol, thus preventing the host information from being displayed in the URL of the browser. If the <userinfo><null>@<host> format is used in email links then some Internet Explorer versions may not be able to display the host information (Munro, 2004).

3.12 Summary:

This chapter in continuation of the last chapter discusses the social engineering attacks; phishing in particular. The discussion is supported by certain definitions of phishing and well as mechanics on the basis of which phishers employ this method in luring and catching their victims. Some of the reasons why phishers are so successful in organising this technique; is the fact that internet users, both businesses and individual fall into the trap because of lack of knowledge and get trapped in the deceptive techniques employed by the phishers. The chapter also includes how phishing attacks are started, motivations behind it, latest trends, and different types of phishing attacks.

The chapter also discusses the platform of emails through which phishers carry out most of their attacks. Email spoofing is fast gaining momentum as different methods under it such as disguised links, forged sender addresses, false company imagery, etc are being used to make fraud emails look like legitimate ones, which is the best way of trapping users. Lastly the countermeasures of tackling this issue are also being discussed to make the readers aware of the problem as well as getting equipped in mitigating this threat.

CHAPTER 4

RESEARCH METHODOLOGY

4. INTRODUCTION TO RESEARCH METHODOLOGY:

4.1 Introduction

The aim and objective of this report is to undertake research into phishing and to evaluate the feedback given by users in order to explore what users think is being done by businesses in order to protect their data. This research offers ideas of how aware users are of phishing and what methods do they observe have been adopted by businesses to protect data, and what developments are been made to enhance security. In addition this research will highlight the different types of methods and techniques used to identify the possible areas where businesses need more concentration and further research. The identification and the evaluation would help to highlight which areas need more concentration by businesses i.e. gaining trust of users by clearly marking the security features on the website and how can user awareness be increased. Based on the evaluation of the existing feedback, suggestions can be made in order to improve security measures and to increase user awareness.

According to Batanov, (2008) research is, "the systematic investigation into and study of materials, sources, etc, in order to establish facts and reach new conclusions". This helps to evaluate the current situation and facts by the scientific study and after critical investigation reach a conclusion. It is extremely important that the research is conducted in the most effective way possible in order to yield best possible results.

4.2 Participation to Knowledge

In this research the aim is to ensure that there is plenty of awareness amongst individuals about phishing and what methods are best suited for the awareness. This research will also address what businesses need to do in order to ensure that their customers data are kept safe and out of reach of hacking and take effective countermeasures against phishing. This aspect is very crucial because it is impossible to educate every single user using the web but phishing websites can be controlled up to an extent (Bidgoli, 2004).

4.3 Research methods

The topic being researched can be researched and studied via a variety of methods as per the researcher's opinion, but methods such as questionnaires and case study give a greater insight and depth into the research (Bernard, 1995). The rationale for selecting those research methods was because there was sufficient amount of data which could be collected and this data can be analysed and converted into a meaningful graphical form. The methods selected are briefly explained below:

4.3.1 Case study

Case studies give an in-depth review of a given subject. Therefore the purpose of selecting a case study in this research is to have a comprehensive understanding of the research object; an understanding that is as close to the practical world as possible.

4.3.2 Questionnaires

The data was gathered from individuals and their opinions and views about the researching topic were taken into consideration. The reason why this method was selected was that the results collected would be from a large group of individuals who might belong to different cultures or graphical areas thus their opinions would differ. This would help to explore how aware individuals are about the topic of phishing and thus provide results of different degree.

4.4 Research objectives

The goals of this project are as follows:

1. To carry out a detailed literature review on e-commerce & e-business and the phishing concept.
2. To investigate the impact of phishing activities in relation to e-commerce and e-business.
3. To collect data from users and companies that have or haven't fallen victim of phishing attacks and how or if they have been able to provide a solution to this.
4. To carry out a detailed analysis based on phishing activities case study.

5. To provide possible solution to specific phishing problems based on answered questionnaire from selected companies and individual.

4.5 Research plan:

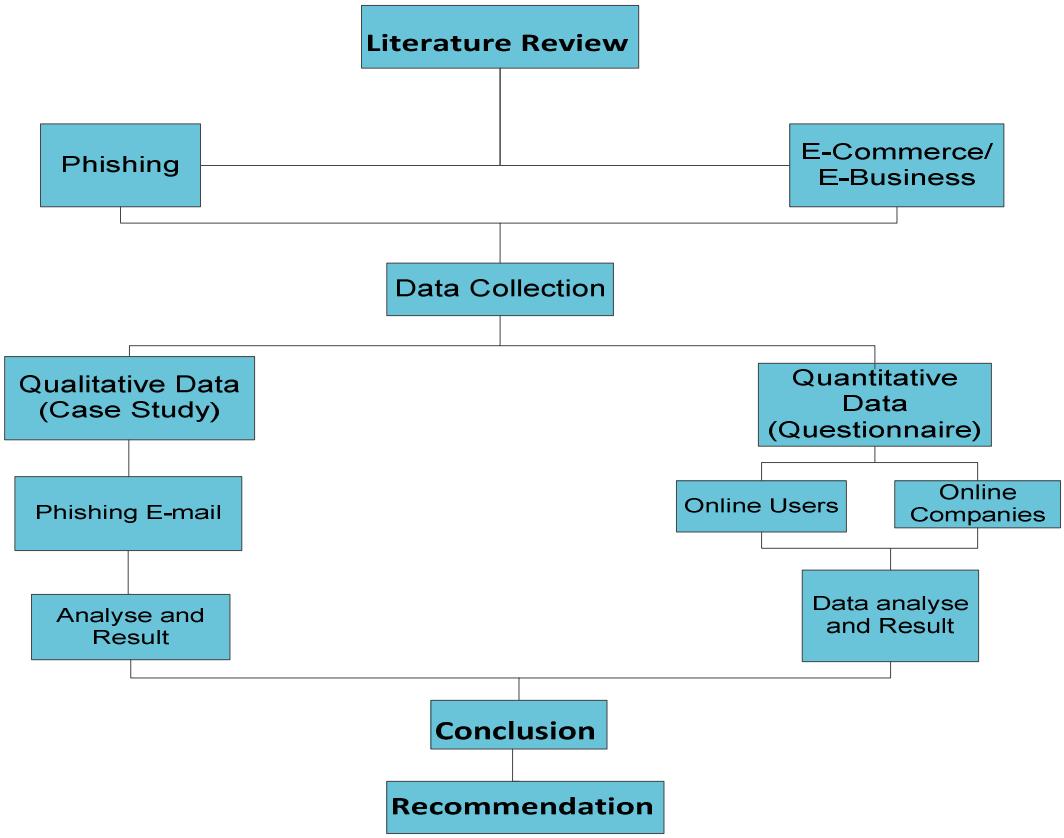


Figure 28: Research Plan

4.6 Qualitative and Quantitative Research

It is extremely vital that the right type of research is selected and what type of data should be used in order to fulfil the objectives of the research being carried out. If the right methods are not used it would result in inaccurate results being captured. The research methods used can either be qualitative or quantitative techniques or both of them (Biggam, 2008).

Qualitative research techniques can be expressed using case studies or interviews methods in order to gather information (Lakshman, 2000). This method involves

in the collection of data, compiling it, breaking it down into a simpler form and analysing it according to the research being carried out.

Quantitative research technique on the other hand involves the different data collection from experiments and questionnaires and analysing techniques (Morgan, 2001). It is quite similar to the qualitative technique because both methods involve gathering data from the users or experts or researchers in order to reach a conclusion. But quantitative research outshines the qualitative research because it involves the analysis of the numerical data collected (Maxwell, 1996). Any individual carrying out qualitative research is concerned with the process of the research rather than the outcome or the products and the aim is to get more information about the individuals i.e. how do they think and analyse things and based on that a conclusion is reached. The numbers used in the quantitative research is continuous and because of this it is considered as a difficult analysis technique compared to the qualitative method.

4.7 Research Methods

4.7.1 Case Study

A case study can be referred to as collecting data and presenting the detailed information collected about a particular topic. This form of qualitative research technique gathers information from a small group of individuals and based on the responses collected a conclusion is drawn. The sole purpose of case study is to explore and analyse the different types of information gathered without taking into consideration any other factors which might affect the case study in any respect. But it gives an in depth information and even the minute most detail about the case under study.

4.7.1.1 The advantages of using case study:

1. Case studies can easily be regarded as a good chance for innovation**.**
2. It helps to study the situation without any constraints.
3. Helps to challenge the different theories in place and there is a possibility of them being changed

4.7.1.2 Phishing E-mail Case Study:

The email that forms the basis of the study contained certain hints which gave indications that the email was a phishing scam rather than an original message from the bank itself. Some noticeable items were the "From:" address, the "To:" address, the message "Subject:" e-business logos, who the email is addressed to, the web link and the message body.

When the users accessed the website, there were other noticeable differences in comparison to a legitimate bank's website such as the address type (HTTP Vs. HTTPS), the URL or web address, the GTbank Logos and asking for details of the cash card number. None of these features would be present on the legitimate bank's website and this caused an uncertainty of a certain type amongst the users.

4.7.3 Surveys

Surveys are generally used to gather some information from a large group of individuals and the data collected is a combination of the individual's ideas, their views and their attitude to the research topic. Survey is a method of quantitative research which means that there won't be any right or wrong answer but the views would be matched against a quantitative hypothesis and a conclusion would be reached.

Questionnaires are used in this instance where the data being collected would be from various individuals and they might have some weaknesses such as no detailed responses and cannot guarantee that the individual answered with sincerity. But questionnaires help to spread it over a larger audience, reduces the chances of the biased and uniform presentations, responses would be gathered in

a particular standardised way, information is easy to be collected and they offer individuals the freedom of how to reply in their free time.

4.8 Methods of data collection:

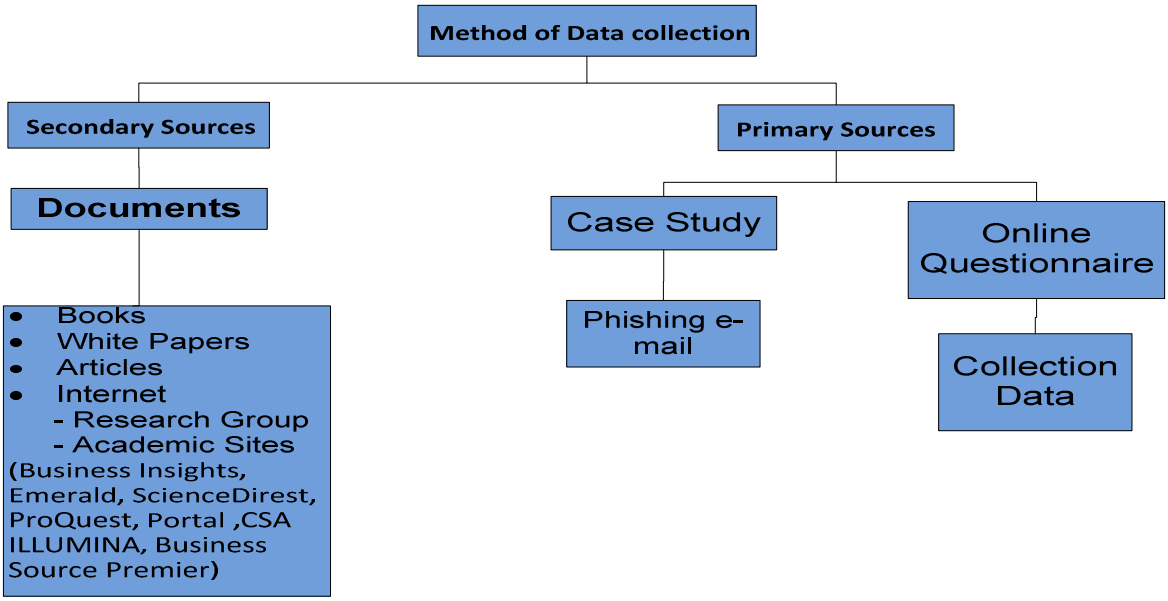


Figure 29: Methods of data collection

4.8.1 Companies Questionnaire

They were sent out to companies in order to analyse what security measures are being taken by them in order to protect user data. The questionnaires designed are quite specific to the subject and the information gathered will be thoroughly studied to conclude the status of the company.

4.8.2 Users Questionnaire

Individuals were given questionnaires and asked for their views regarding the scenario. They have got the freedom to give their views and different type of views collected will then analysed and plotted into a user friendly graphical formation.

4.8.3 The advantages of Online Survey

1. They are quite cost effective and are the quickest medium for spreading the questionnaires
2. Can be spread over a larger scale without much input or large amount of money being spent
3. The chance of influencing a researcher's way of thinking onto respondents is mitigated.
4. Respondent's identity remains anonymous, thus they can answer sensitive answers easily.

4.8.4 The disadvantages of Survey

1. It is quite hard to develop questions which are general enough to be appropriate for all the respondents.
2. Surveys are quite inflexible and once created they cannot be changed anytime throughout the process of data collection.
3. Large amounts of feedback are required to have a valid conclusion.

4.9 Questionnaire design

The questionnaire being designed is developed bearing in mind the research objectives. The questionnaires are different for both the companies and the users as both the profiles would answer differently. There are 15 questions in the questionnaires and most of the questions had sub divisions in order to gather as much information as possible. Some questions were a simple yes or a no whereas some were to select from a list of options. Overall the questionnaire was designed to make the questions a lot easier to understand, to be easily interpreted and to get most information from users. Most of the questions used were open ended where the views of the individuals were collected like what they felt about the situation in question, and any suggestions they could think of. Apart from that there were only two close ended questions with a yes, no answers or a list of answers to select from.

This paper researches the menace of phishing and the affects it carries in terms of damage and losses. This required the study to carry out an investigation where

responses could be gathered from a population that uses Internet as a source of buying or carrying out financial transactions on a frequent basis. In order to meet the research objectives, it was necessary to find out how many of the respondents actually use e-commerce and from those results, how many had heard of the threat or were victims of phishing. The level of awareness and preparedness among respondents was also gauged from this survey and how seriously they take this phenomenon. The psychological impact on victims was also briefly touched upon in the survey as well as what can be done to improve user experience which transacting online. The questionnaire was developed keeping in mind the above mentioned points.

Serial	Survey Questions	Purpose of Question	What was done with given answers?
1	**How often do you use online shopping/ banking websites each month?**	To find out the percentage of respondents who use e-commerce as a way of transacting.	This question gives us the results that 100% of the respondents use e-commerce and a significant number i.e. 65% use it 1-10 times/month, which authenticates that they may have a potential of facing phishing especially in case of unawareness.
2	**Have you heard of online phishing?**	Gives us the level of awareness of phishing among the respondents.	Help us analyze whether awareness of phishing or lack of it has anything to do with becoming a victim.
3	**How many times in the last year have you received phishing email?**	To check the frequency of attempted phishing emails being received by users.	To find out whether phishing is significant enough to become a cause of concern or not.
4	**Have you ever been fallen victim to a phishing email?**	Gives us those individuals who have fallen victims and this helps in gaining further insight into their experience.	Leads to the details of experiences, reactions, and behaviors among victims.
5	**How much did you lose?**	Gives a rough idea regarding the level of damage done to the victims.	The answer leads to relating of losses to other researchers conducted and checking deviations or similarities.
6	**Which of the following actions should you take if you have responded to phishing e-mail?**	Purpose was to find out user reactions to phishing emails.	The answer was used whether users were following good practices or not.

7	**After falling victim to phishing have you continued shopping online?**	The question checks for the psychological impact that victims may show after falling prey to phishing.	The answers were used to check whether phishing changes the behavior of victims towards e-commerce or not.
8	**Are you satisfied with the action taken by the business/bank against phishing if you responded to it?**	To check whether satisfactory actions are taken by businesses in case customers report phishing.	To analyse whether current post-phishing actions by businesses are appropriate or not.
9 **9a**	**What precautions do you think businesses should take in order to prevent phishing related incidents?**	To find out whether users have some suggestions to improve data security.	The results will be used to find out if people have appropriate knowledge in securing their data.
10	**Does your bank provide free software to help prevent phishing?**	Aim is to finds out whether banks are more prone to phishing or not.	The answers will be used to find out the preparedness of banks towards phishing.
11	**Do you think it is safe to fill personal information into pop-up windows?**	Purpose is to find out the level of confidence among respondents especially under the prevailing pervasive phishing.	To check the seriousness and maturity levels among respondents. Whether they take phishing threats seriously or casually.
12 **12a**	**Do you know whether a web site offers security to protect your confidential data?**	Gives us the level of awareness and preparedness of phishing among the respondents.	Answers will be used to check whether respondents are aware of security symbols shown on websites.
13 **14** **14a** **15** **15a**	**Sample of Phishing emails**	The aim is to find out if respondents have the ability to differentiate between a legitimate or a phishing email.	The answers of this question will be used to authenticate and verify previous responses of respondents regarding awareness, knowledge etc.

Table 0: Questionnaire Design

4.10 Sample size

The accuracy of the results is usually based on how the results were gathered and the reason behind selecting a realistic sampling size is that the response rate can be measured effectively and gives a reflection of the overall survey conducted. The strength and the weakness should be measured before the research begins in order to have an effective and accurate result. There were 69 samples which were collected via the questionnaires by Snap 9 Professional Software from individuals, which is not high to obtain a conclusion. The data was collected and analysed by SPSS Statistical Software using Frequencies variable for single question and Cross tabulations variable for Multiple questions.

The questionnaire was targeted at users who transact on the internet more often and for this purpose a sample from the University of Warwick MSc and BSc students from different areas (Africa students, Middle East students, Europe Students, Asia Students), friends working in companies across UK, friends of friends, and Warwick communities on facebook etc. A sample size of 400 students could be reached as the respondents' population remains unknown and the survey was being emailed to these potential respondents. A total of 69 responses were received which constitutes to about 18% response rate.

4.11 Research results

The data which is collected has a relation between it and this is presented in a user friendly format so that it is easily understood. Different techniques can be used in order to publish the findings such as with help of charts and percentage ratings which overall gives the concluding result.

4.12 Summary

The research methodology used to cover this paper involves a quantitative analysis technique. The objectives of the research were to investigate the impact of phishing activities on users and to study the approach of taken by victims of phishing and how they have acted in minimizing the risk in future. A cases study and questionnaires were floated in order to gather the data to be analyzed for the paper.

The questionnaire involves 15 questions with subdivisions in order to gather more useful information. 69 survey responses were gathered and a Chi Square test was being used to find the relationship between to variables. This chapter also covers the advantages of case studies and surveys as well.

This chapter uses diagrams and graphical representations to make the data understandable and at the same time highlights other methods in collecting the phishing data which include consulting journals, online papers, articles, academic websites, library books and journals etc.

CHAPTER 5

ANALYSIS AND DISCUSSION

5.1 Introduction to Survey Responses:

This survey focused in finding out how much individuals knew about phishing and how can they be helped in order to protect their data and protect them from falling victims of phishing. Individual were asked various questions ranging from how often they shopped online to how secure they felt that businesses protected their data. 69 individuals were surveyed and their results were analysed in order to highlight factors which might need more attention. The 69 responses gathered can be considered as a weak response rate for the survey and gathers a representation not entirely reflective of the wider audience. In order to calculate the results SPSS software was used where frequencies of single questions and cross tabulation for comparison questions was used and this helped to give a graphical response of the data gathered. The cross tabulation tables used display the relationships between two or more categorical variables. The size of the table would be determined by the number of distinct values for each of the variable in which each of the cells in the table is used to represent the unique combination of the values. There are different statistical tests available which would determine whether there is any type of relationship available between the variables represented in the table.

5.1.1 Have you heard of online phishing?

Have you heard of online phishing?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		2	2.9	2.9	2.9
	No	9	13	13	15.9
	Yes	58	84.1	84.1	100
	Total	69	100	100	

Table 1: Have you heard of online phishing?

The above table gives the response rate of the target audience. The results gathered can be interpreted by suggesting that nearly 84% of the respondents might have been aware of the term online phishing, as a total of 58 respondents said to have heard of the term which shows that there ***may*** exist reluctance amongst those while shopping online. All this would mean that they may be hesitant when passing details online and especially if the website did not look genuine. Businesses can overcome this by creating effective layouts, security checks, and authentication procedures etc.

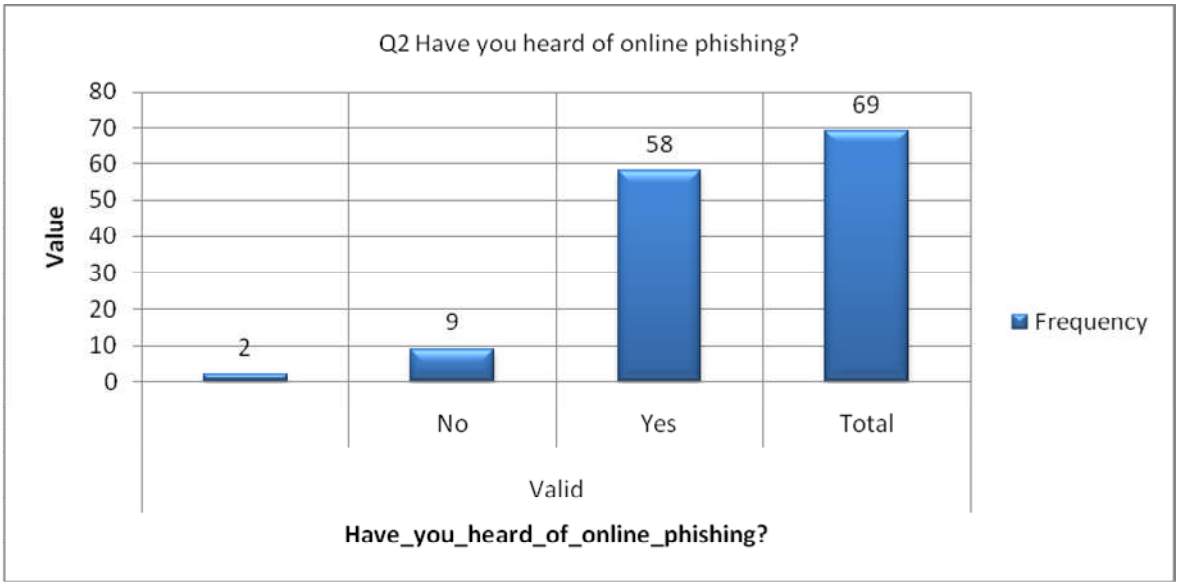


Figure 30: Have you heard of online phishing?

According to a report published by *Websense Security Labs in December 2006,* a computer worm was released by attackers which took over myspace pages altering the links and redirecting them to websites designed to steal login details. But by ensuring prompt and effective after sales would definitely help to increase customer's confidence and they would know that the site is genuine and not a scam. Further more customer feedback can be recorded and displayed on the website along with recording other statistics like user rating of a particular product or of the entire website.

Looking at the data in figure 30, 58 individuals knew what online phishing was as opposed to 9 individuals who had not heard about it. Businesses on the other hand need to assure the customers that they would get what they are viewing (quality)

and in the time frame mentioned thus increasing the trust. Another method of ensuring customer's trust is to have returns policy clearly mentioned with all contact details, have a privacy statement and a good and effective web design, thus avoiding web spoofing (Wheelock, 2005).

An important aspect for both the user and businesses is that if the website does not provide sufficient amount of security, it could result in the user losing their identity and money while business may incur losses due to lack of customer visits. 58 respondents out of 69 seem to know what online phishing is which also means that they would be particularly interested in how their data would be handled and protected. An incident of this nature is of attackers who broke into TD Ameritrade's database which contained 6.3 million social security numbers, account numbers, email addresses and all personal information related to an individual. This article was published in sophos website and can be found on the following link [3]

5.1.2 Online shopping:

On average, how often each month do you use an online shopping or banking web site?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-10 time	45	65.2	65.2	65.2
	11-25 time	15	21.7	21.7	87.0
	26-50 time	7	10.1	10.1	97.1
	>51 time	2	2.9	2.9	100.0
	Total	69	100.0	100.0	

Table 2: On average, how often each month do you use an online shopping or banking web site?

[3] http://www.sophos.com/pressoffice/news/articles/2007/09/ameritrade.html accessed at 15.May.2010

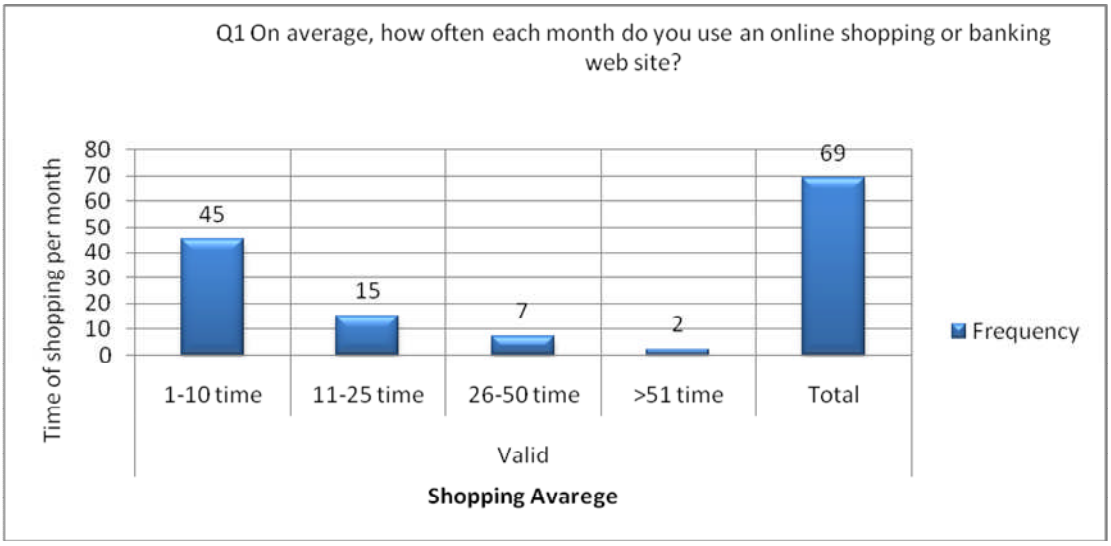


Figure 31: On average, how often each month do you use an online shopping or banking web site?

The response rate shown above may suggest that majority of the respondents i.e. 65% shop online between 1-10 times in a month while the rest i.e. approx 34% of the respondents carry out internet transactions more than 10 times in a month. Companies can include customer counters on their websites in order to show that how much of traffic is on the website as higher numbers would indicate that the website is frequently accessed.

The shopping pattern depicts that many customers prefer online shopping as e-commerce technologies are being improved and bettered every day, but at the same time the security that these technologies provide becomes questionable and at times fail to meet the security needs of the customers (Al-Slamy, 2008).

Fewer respondents i.e. 2.9% shop more than 50 times a month, may suggest that customers either prefer shopping while visiting stores, or they may be reluctant to shop more frequently because of the internet security issues, or they may not require that many online transactions in a month's time. These perspectives can be looked into in more detail in future researches.

5.1.3 How many times in the last year have you received phishing email?

How many times in the last year have you received phishing email?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	4.3	4.3	4.3
	1-10	33	47.8	47.8	52.2
	11-25	12	17.4	17.4	69.6
	26-50	14	20.3	20.3	89.9
	>51	7	10.1	10.1	100.0
	Total	69	100.0	100.0	

Table 3: How many times in the last year have you received phishing email?

Looking at table 3, 47.8% of the respondents received phishing emails as per the survey response. This frequency shows that there may be a lot of phishing emails being sent out to individuals by portraying as an established business and attracting customers into buying fake or low quality products and in some cases not delivering the products at all. The lure that these phishers create looks convincing and entices the customers into divulging useful information online (Youl, 2004).

Figure 32: How many times in the last year have you received phishing email?

User's trust is needed to be gained with all those phishing emails being sent out as only 3 respondents out of 69 did not receive any emails, where as rest of them were emailed at least once up to 51 or more times. The business needs to firmly include its privacy statement with every email being sent and respond quickly if any phishing scam is discovered which could harm the business's credibility.

Effective measures need to be taken so that none of the stored data is lost to hackers. This would ensure that any information provided by the customers is safely secured and that no one has access to it apart from the database administrator. Other security measures can be taken such as usage of Secure Socket Layers, encryption and decryption of data and when the transaction is being carried out it is done in a secure and locked layer.

5.1.4 Have you ever been fallen victim to a phishing email?

Have you ever been fallen victim to a phishing email?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	60	87.0	87.0	87.0
	Yes	9	13.0	13.0	100.0
	Total	69	100.0	100.0	

Table 4:Have you ever been fallen victim to a phishing email?

		How many times in the last year have you received phishing email?				
		1-10 e-mail	11-25 e-mail	26-5 e-mail	51> e-mail	Total
Have you ever been fallen victim to a phishing email?	No	30	9	11	7	57
	Yes	3	3	3	0	9
Total		33	12	14	7	66

Table 5: Have you ever been fallen victim to a phishing email?* How many times in the last year have you received phishing email? Crosstabulation

According to table 5, 66 individuals were surveyed and asked about whether they had received phishing email in a year and nearly 50% of them received between 1 to 10 emails in a year and 3 fell victim of it. About 13 % responses suggest being targeted by phishing emails. These numbers show that individuals still fall for phishing emails irrespective how many times have they being emailed, which is a great threat to e-commerce because the business would only operate via the internet and the customers would only view what is shown to them and might hesitate shopping online once falling a victim.

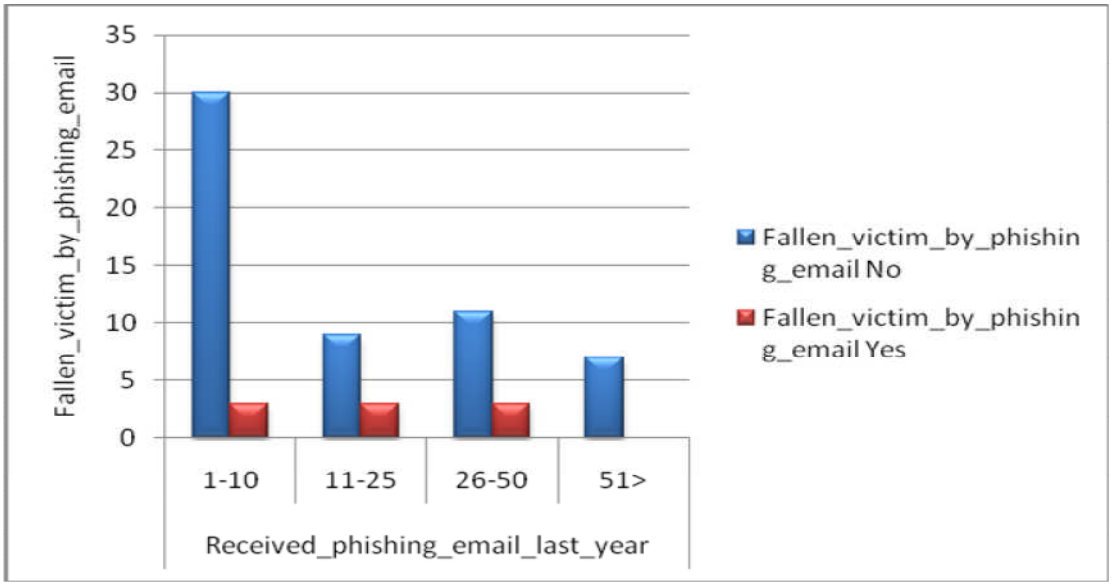


Figure 33: Have you ever been fallen victim to a phishing email?* How many times in the last year have you received phishing email? Crosstabulation

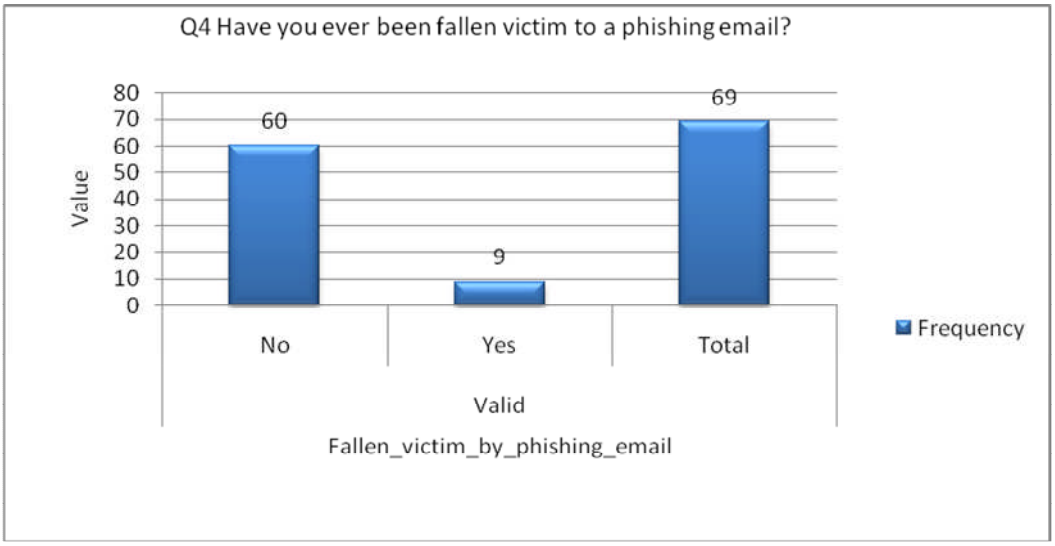


Figure 4.1: Have you ever been fallen victim to a phishing email?

According to figure 33, only 3 individuals out of 33 fell victims of phishing email when emailed up to 10 times meaning that customers would be hesitant when opening any sorts of emails sent out by businesses as it might be a popular scam. These numbers could be reduced by businesses using their trademark logos and copyrighted electronic signatures in every email to assure the user that the email was genuine.

Similarly as Hearst, et al. (2006) explains that users need to increase their knowledge of the website, its security indicators and at the same time find out more about the business before purchasing an item. Business on the other hand can make the order fulfilment process much more easily and ensure that it is completed in a single process rather than sending out emails for validation and verifications.

Table 4 interesting tells that when individuals were emailed more than 50 times none of them fell victims probably because they got aware of how the phishing scams worked or they had taken some sorts of security countermeasures.

5.1.5 How much did you lose?

How much did you lose?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		39	56.5	56.5	56.5
	£100 - £1000	8	11.6	11.6	68.1
	prefer not to say	22	31.9	31.9	100.0
	Total	69	100.0	100.0	

Table 6: How much did you lose?

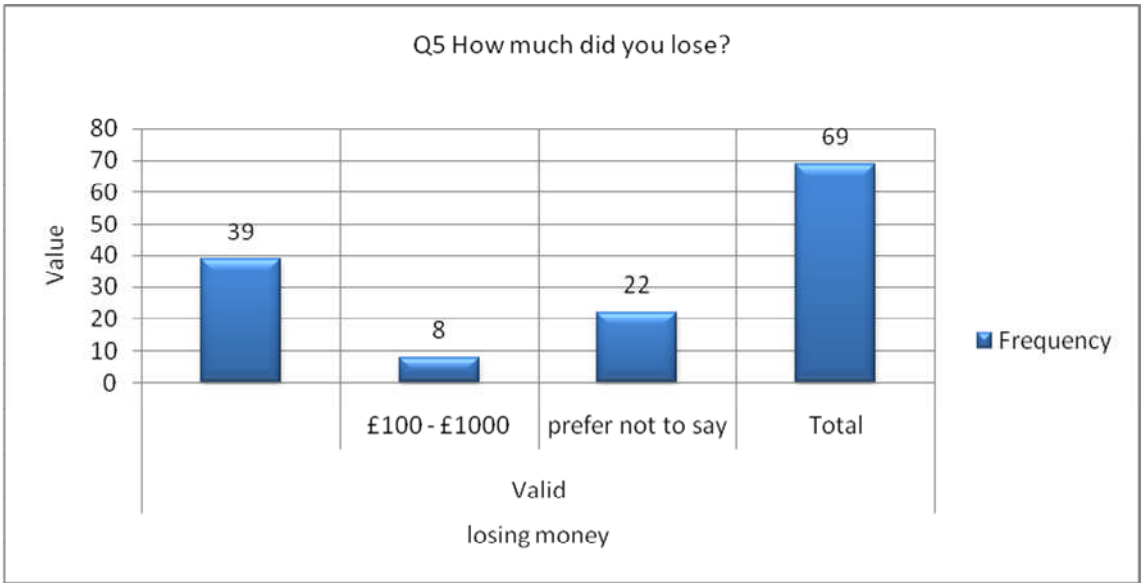


Figure 34: How much did you lose?

The figure34, above shows that 11.6% of the respondents lost between £100 and £1000; whereas the majority of the responses i.e. 56.5% did not lose anything and 31.9% declined to reveal their losses. In light of e-commerce even a pound being lost as a result from phishing is a delay as businesses compete in a real competitive environment and with 11.6% individuals losing unto a £1000 means that those individuals might move away from online shopping in future and this can have an impact on the businesses. These 11.6% of the respondents who faced losses in pounds may correspond with the report by IC3 (2009) if seen in U.S dollars, that 36% of the complaints received by IC3 bureau, lie in the loss figures between $100 and $1000.

There were 22 individuals out of 69 who preferred not to say how much they lost and this might due to a number of reasons such as the amount might be too large or too small to mention, it might be cause of privacy whether they might not want to be named.

5.1.6 Which of the following actions should you take if you have responded to phishing e-mail?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		4	5.8	5.8	5.8
	1	1	1.4	1.4	7.2
	1,2	1	1.4	1.4	8.7
	1,2,3	2	2.9	2.9	11.6
	2	4	5.8	5.8	17.4
	2,3	6	8.7	8.7	26.1
	2,3,4	7	10.1	10.1	36.2
	2,4	2	2.9	2.9	39.1
	3	11	15.9	15.9	55.1
	3,4	5	7.2	7.2	62.3
	4	1	1.4	1.4	63.8
	5	25	36.2	36.2	100.0
	Total	69	100.0	100.0	

Table 7: Which of the following actions should you take if you have responded to phishing e-mail?

SCALE:

1: Report it to police.

2: Change your passwords.

3: Contact your bank immediately.

4: Report to online trader involved.

5: All of the above.

An interesting outcome of the above responses shows that victims of phishing may take several steps in sequence rather than just one. The results in table 7 and

figure 35 show some interesting facts of how individuals would respond to phishing emails. Majority of the individuals (36.2%) would take complete measures to ensure that their information is completely protected and that they are safe. The next most preferred action (15.9%) is to contact the bank immediately and this is extremely important because individuals would be at risk of losing important and sensitive information and even money in the extreme cases. According to results (table 8 and figure 36) broken down by the type of actions taken by customers the popularity were as follows:

1. Contact your bank account immediately (28%)

2. Report it to the online trader involved (bank, credit card company etc) (26%)

3. All of the above (25%)

4. Change your passwords (22%)

5. Report it to police (4%)

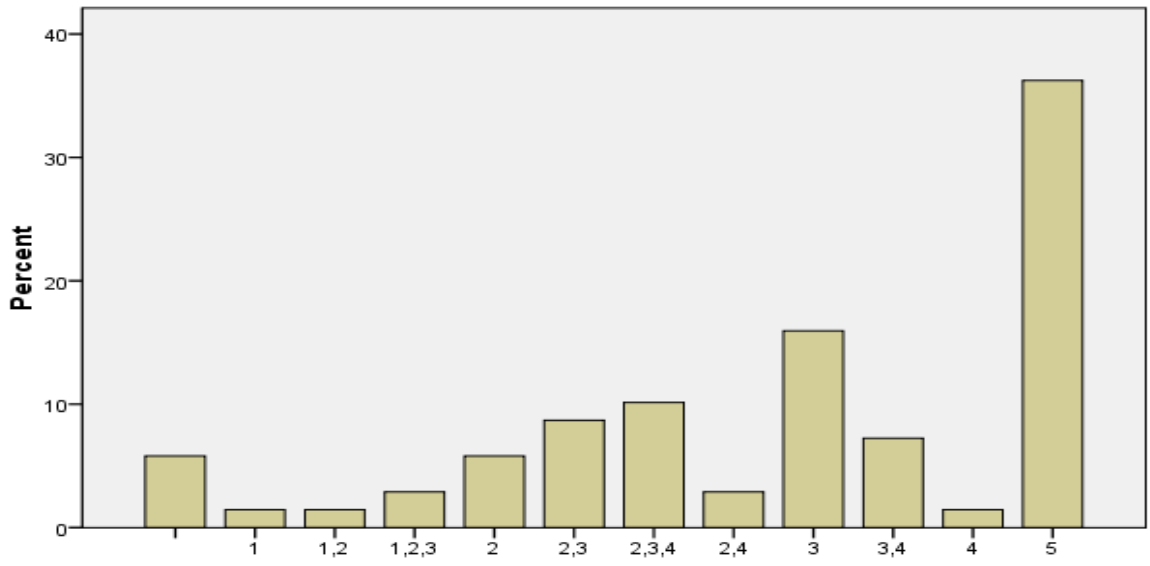


Figure 35: Which of the following actions should you take if you have responded to phishing e-mail?

1. Report it to police
2. Change your passwords
3. Contact your bank account immediately
4. Report it to the online trader involved (bank, credit card company etc)

5. All of the above

Kind of responded	Time
1	4
2	22
3	28
4	26
5	25

Table 8: Which of the following actions should you take if you have responded to phishing e-mail?

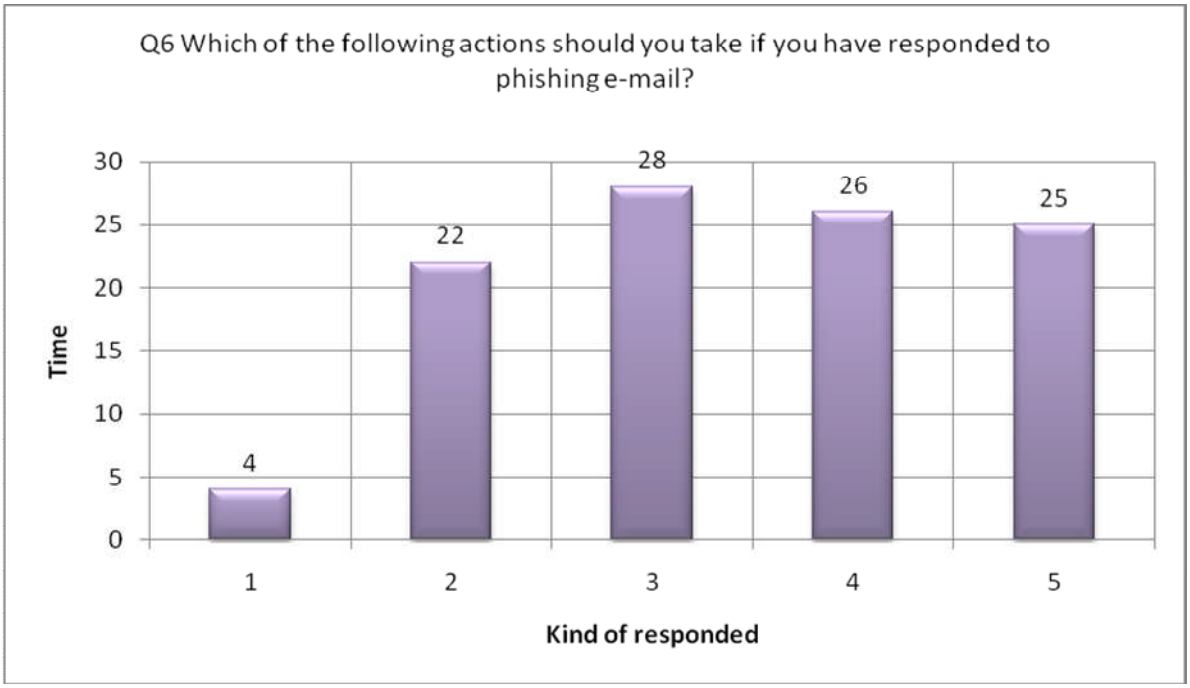


Figure 36: Which of the following actions should you take if you have responded to phishing e-mail?

5.1.7 After falling victim to phishing have you continued shopping online?

After falling victim to phishing have you continued shopping online?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		6	8.7	8.7	8.7
	No	6	8.7	8.7	17.4
	no answer	40	58.0	58.0	75.4
	Yes	17	24.6	24.6	100.0
	Total	69	100.0	100.0	

Table 9: After falling victim to phishing have you continued shopping online?

When individuals were asked if they would still shop online after falling victims of online crime, 8.7% responded with a no, 58% avoided from giving their opinions where as 24.6% were still confident enough to carry on shopping online.

The individuals who responded with a "NO" for the above question (8.7%) accounted for a very small portion. A major reasoning behind this can be linked to the negative psychological behaviour of the victims. Similarly a well coordinated and timely response to a victims call may have a positive effect in improving their confidence in the business (Allison et.al 2005).

Figure 37: After falling victim to phishing have you continued shopping online?

5.1.8 Are you satisfied with the action taken by the business/bank against your complaint?

Are you satisfied with the action taken by the business/bank against the phishing if you responded to it?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		28	40.6	40.6	40.6
	No	6	8.7	8.7	49.3
	Yes	34	49.3	49.3	98.6
	Y,N	1	1.4	1.4	100.0
	Total	69	100.0	100.0	

Table 10: Are you satisfied with the action taken by the business/bank against the phishing if you responded to it?

According to table 10, nearly half (49.3%) of individuals were satisfied with the actions taken by the businesses against phishing where as 8.7% of individuals thought there wasn't enough done by the business where as 40.6% of individuals did not respond to the question.

The result shows that the trust levels amongst individuals are still high and that individuals still trust the security measures deployed by the business which would result in them purchasing in the future. Interestingly as shown in figure 38 below 6 out of 69 individuals were not satisfied by what countermeasures were taken by the business in order to protect their data from being lost as a result of phishing and this might be of concern because businesses would lose customers meaningless profits.

Figure 38: Are you satisfied with the action taken by the business/bank against the phishing if you responded to it?

Breaking the above mentioned results further down in order to compare the relationship between the amount of times an individual shopped online as opposed to how satisfied were they by the actions taken by the business. The results from the relationship are shown in the table 11 below:

		Are you satisfied with the action taken by the business/bank against the phishing if you responded to it?			
			No	Yes	Y,N	Total
On average, how often each month do you use an online shopping or banking web site?	1-10		6	18	1	45
	11-25		0	10	0	15
	26-50		0	5	0	7
	51>		0	1	0	2
Total			6	34	1	69

Table 11: On average, how often each month do you use an online shopping or banking web site?* Are you satisfied with the action taken by the business/bank against the phishing if you responded to it? Cross tabulation

The above table 11 shows that the only individuals who were not satisfied with the actions taken by business against phishing were those who shopped 1 to 10 times in a month. The numbers was merely 6 out of 45 which meant that the individuals who believed not enough was done to protect their data avoided from shopping or shopped at a lesser rate in comparison to those who shopped a lot more. Table 12 shows that the significance value is high that is .659, which means that it would appear that the two variables are, indeed, related, accepted significance level of = (0.05).

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.789[a]	9	.659
N of Valid Cases	69		

Table 12: Chi-Square Tests

Figure 39, displayed below shows the figures when accumulated in the form of a graph and it can be observed that the satisfaction level is much higher when the frequency of shopping online is low. The graph would have been different because 28 individuals did not reply when asked the question and their opinions would have definitely contributed in shaping up the graph thus giving a lot more in-depth of the situation.

Figure39: On average, how often each month do you use an online shopping or banking web site?* Are you satisfied with the action taken by the business/bank against the phishing if you responded to it? Cross tabulation

By analysing Figure 39: Table 11, This is mainly to do with the fact that the business and banks increase the security measures in order to protect the user data and can warn the users if any similar emails are sent out in the future. And if an individual reports of any legitimate site then the business would report the website to the relevant authorities to be shut down.

5.1.9 What precautions do you think businesses should take in order to prevent phishing related incidents?

What precautions do you think businesses should take in order to prevent phishing related incidents?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		9	13.0	13.0	13.0
	1	8	11.6	11.6	24.6
	1,2	1	1.4	1.4	26.1
	1,2,3	15	21.7	21.7	47.8
	1,3	7	10.1	10.1	58.0
	2	6	8.7	8.7	66.7
	2,3	7	10.1	10.1	76.8
	3	16	23.2	23.2	100.0
	Total	69	100.0	100.0	

Table 13: What precautions do you think businesses should take in order to prevent phishing related incidents?

When provided the individuals with the question of what was the best possible precaution to prevent phishing, nearly 23.2% pointed out the fact that the businesses need to develop a much more secure website. Nearly 22% of individuals thought that businesses needed to implement all the 3 measures in order to gain user confidence. The table is as below

What precautions do you think businesses should take in order to prevent phishing related incidents?	Selected
1	31
2	29
3	35

Table 14: What precautions do you think businesses should take in order to prevent phishing related incidents?

1. Anti-phishing department
2. Better encryption of personal data
3. Developing a more secure website

Only 29 individuals believed that encryption was the best possible way to protect the data and 31 suggested that the anti-phishing department would be the best solution. These results are better projected on the graph below

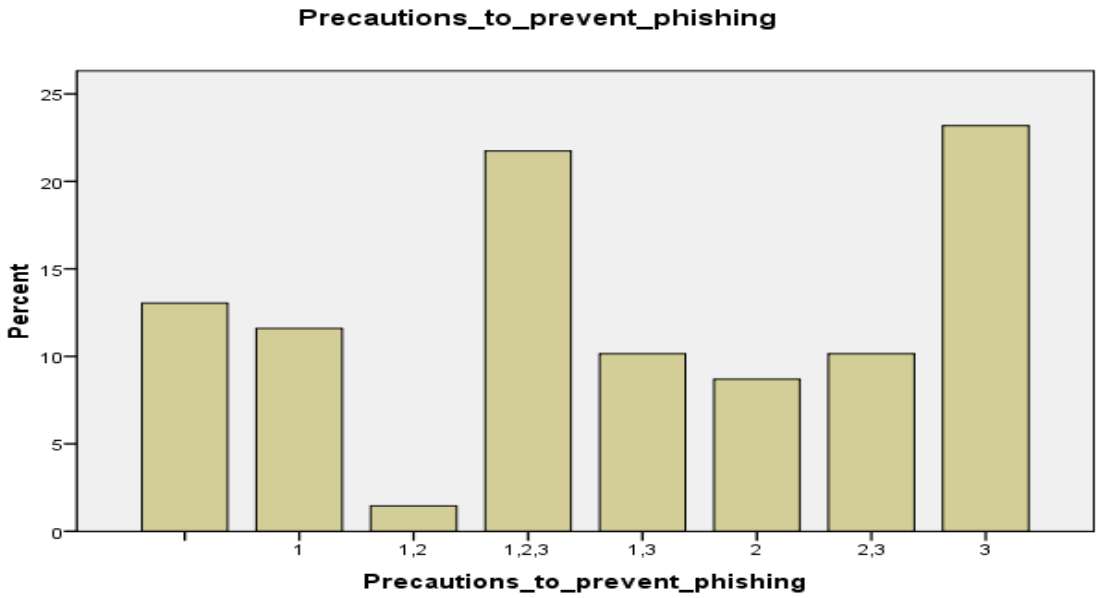


Figure 40:What precautions do you think businesses should take in order to prevent phishing related incidents?

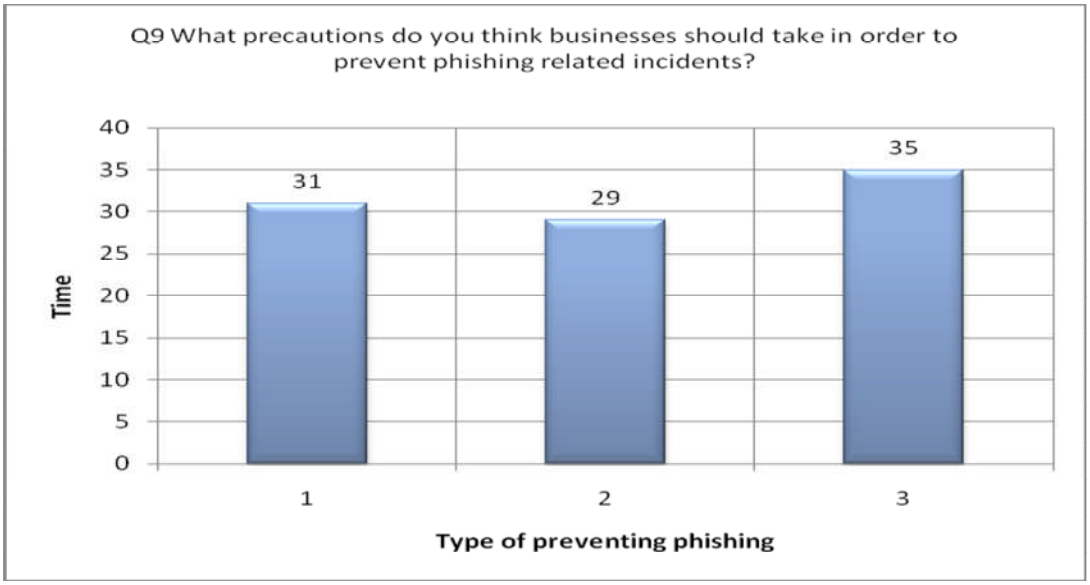


Figure 41: Arranging the above results in order of precaution measures

What can be analysed from the graph is the fact that when the users pass over their personal information on the website it is believed that the business operating the website is responsible for the security of the data. 11.6% of individuals answered that any phishing related incidents should be reported to the anti-phishing department which is justified with the underlying reason that the incident can be reviewed, measures taken before any other individual falls a victim of any such incident and the individuals behind it can be caught and brought to justice. 1.4% of the individuals believed that the not only the anti-phishing department be involved but the data should be encrypted via a better method. By creating a website which has got secure channels when processing a transaction and much easier/safer browsing through the website would not only allow the business to gain trust of the individual but also help the business to grow in the e-commerce environment (Clifton et.al, 2002).

5.1.10 Does your bank provides free software to help prevent phishing?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	4.3	4.3	4.3
	No	4	5.8	5.8	10.1
	Don't Know	25	36.2	36.2	46.4
	Yes	37	53.6	53.6	100.0
	Total	69	100.0	100.0	

Table 15: Does your bank provide free software to help prevent phishing?

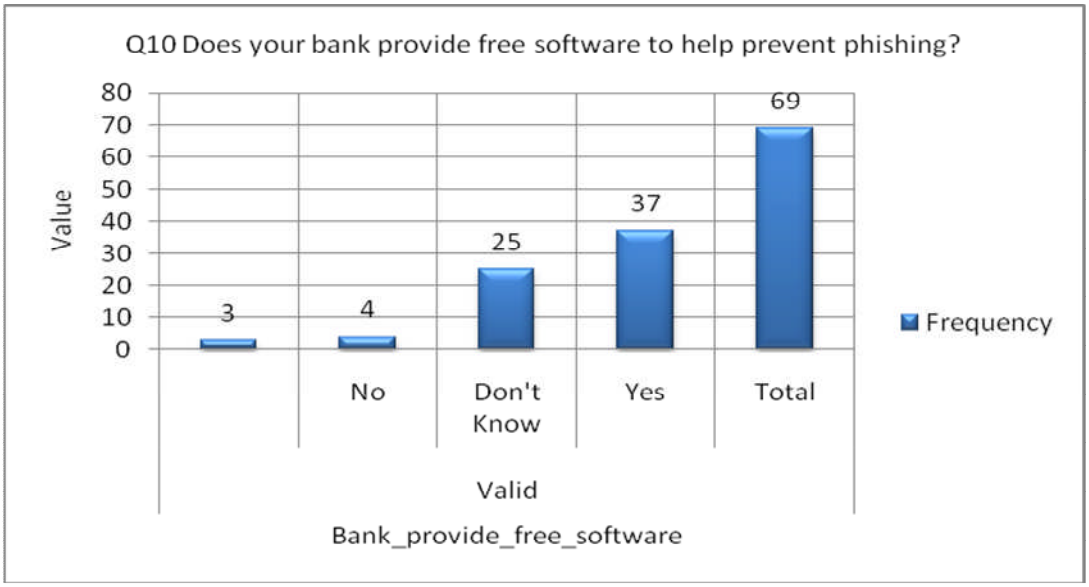


Figure 42: Does your bank provide free software to help prevent phishing?

Looking at the above table 53.6% of the respondents were aware of the fact that their banks provided free software to them in order to protect them from threats. Nearly one third (36.2%) of individuals were unaware of the fact that whether their bank provided any sort of free software or not.

Table 16 and figure 43 below show that the individuals who answered yes that they were aware of their bank providing the software were asking if they had downloaded the software off the bank website and only 34.8% answered yes which means that nearly 32% of individuals either did not download or were not aware of it. This number is quite high as the individuals may not be taking advantage of the free software available to them in order to protect their data. Users are required to effectively protect their own data at all times and take countermeasures even when the data has been saved on the business's server.

Have you downloaded anti-phishing software from your bank website?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		23	33.3	33.3	33.3
	No	22	31.9	31.9	65.2
	Yes	24	34.8	34.8	100.0
	Total	69	100.0	100.0	

Table 16: Have you downloaded anti-phishing software from your bank website?

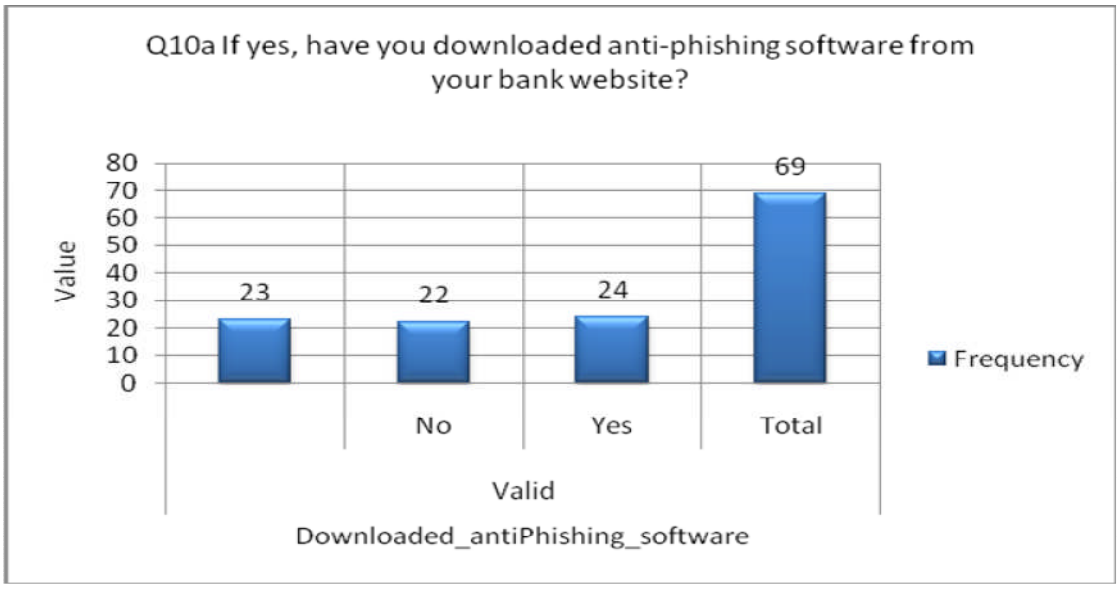


Figure 43: Have you downloaded anti-phishing software from your bank website?

According to figure 43 there were 22 individuals out of total 69 who answered **"No"** when asked if they had ever downloaded the anti phishing software. The reasons ranged from the fact that they already had anti-phishing software; may not be aware of what anti-phishing software is; or did not know if it was important to have it installed; not being a victim yet but would take precautions to protect the data; bank may not have educated its customers etc.

5.1.11 Do you think it is safe to fill personal information into pop-up windows?

Do you think it is safe to fill personal information into pop-up windows?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		4	5.8	5.8	5.8
	No	56	81.2	81.2	87.0
	Yes	9	13.0	13.0	100.0
	Total	69	100.0	100.0	

Table 17: Do you think it is safe to fill personal information into pop-up windows?

Remarkably 81.2% of individuals thought that it was not safe to fill in their personal information in the pop up windows in comparison to only 13% who thought it was safe to share their information. These numbers show that it was highly unlikely that individuals would fall for phishing as they would not enter their personal details on the pop ups. Pop up windows may act as a deceptive mean of obtaining illicit information and later in impersonating the victims (Jakobsson and Myers, 2008).

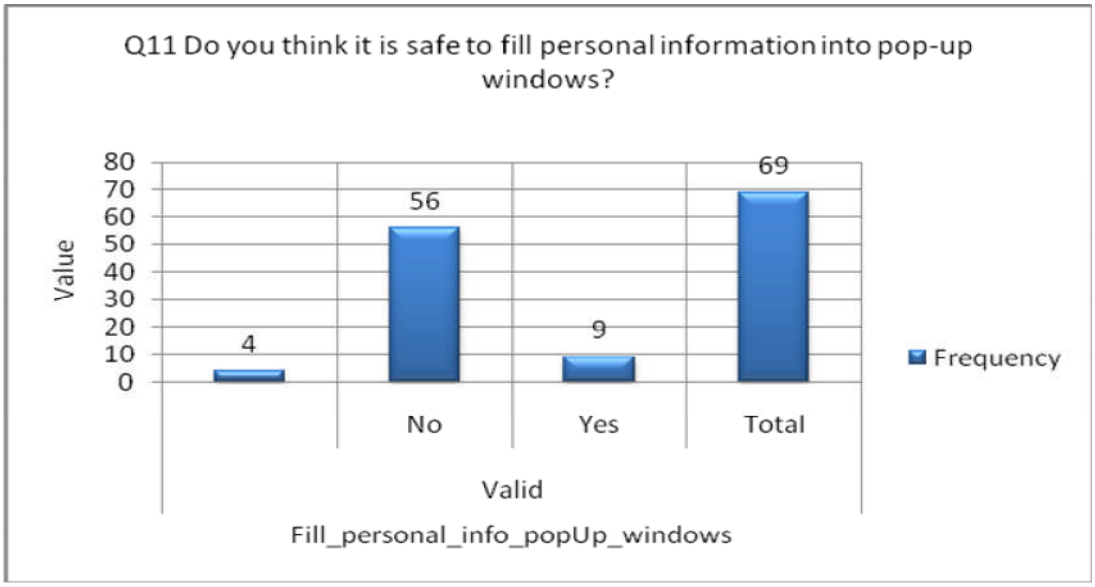


Figure 44: Do you think it is safe to fill personal information into pop-up windows?

5.1.12 Do you know whether a web site offers security to protect your confidential data?

Security is an important aspect from both the businesses and the individuals prospective. When the individuals were asked whether the website provided security to protect their data a total of 56.5% of individuals replied yes where as 37.7% said that their websites did not offer any security (Table 18 and figure 46).

Do you know whether a web site offers security to protect your confidential data?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		4	5.8	5.8	5.8
	No	26	37.7	37.7	43.5
	Yes	39	56.5	56.5	100.0
	Total	69	100.0	100.0	

Table 18: Do you know whether a web site offers security to protect your confidential data?

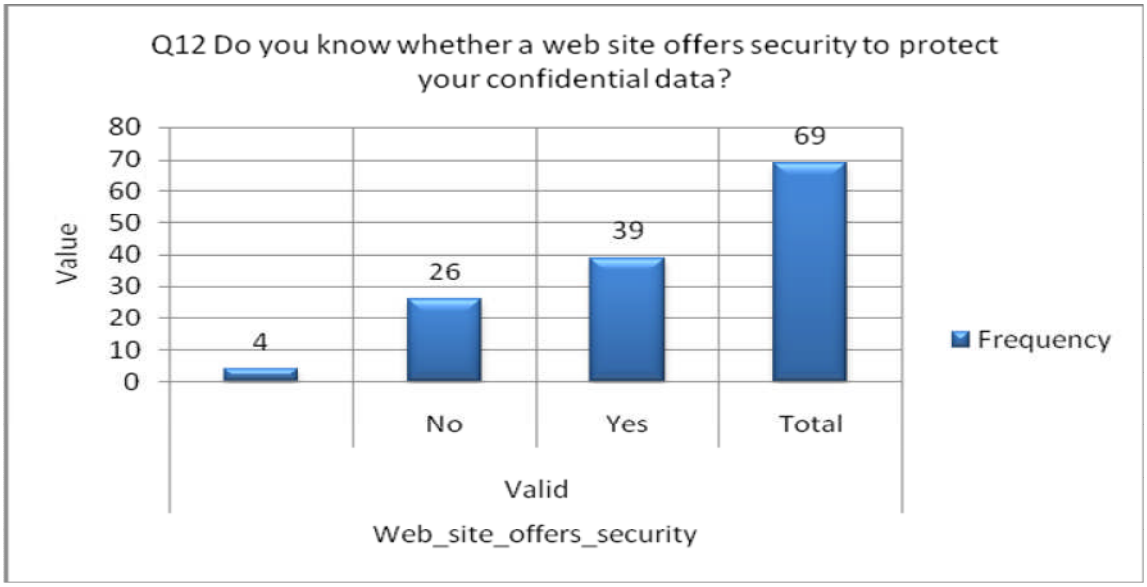


Figure 46: Do you know whether a web site offers security to protect your confidential data?

5.1.13 If yes, which of the following Security are you aware of?

Of the individuals who answered "***yes***" to the question of whether they were aware if the website offered any security were further asked a question of which security measures were they aware of and the following result was obtained.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		25	36.2	36.2	36.2
	1	9	13.0	13.0	49.3
	1,2	1	1.4	1.4	50.7
	1,2,3,4,5	1	1.4	1.4	52.2
	1,2,3,4,5,6	2	2.9	2.9	55.1
	1,2,6	1	1.4	1.4	56.5
	1,3,4	1	1.4	1.4	58.0
	1,3,4,5	1	1.4	1.4	59.4
	1,3,5	1	1.4	1.4	60.9
	1,3,6	1	1.4	1.4	62.3
	1,4,5	6	8.7	8.7	71.0
	1,4,5,6	1	1.4	1.4	72.5
	1,5	3	4.3	4.3	76.8
	1,6	1	1.4	1.4	78.3
	2	1	1.4	1.4	79.7
	3	2	2.9	2.9	82.6
	3,4	1	1.4	1.4	84.1
	3,5	1	1.4	1.4	85.5
	4	2	2.9	2.9	88.4
	4,5	2	2.9	2.9	91.3

	5	3	4.3	4.3	95.7
	6	3	4.3	4.3	100.0
	Total	69	100.0	100.0	

Table 19: which of the following security are you aware of?

Table 19 helps to identify that most of the individuals were aware of the closed padlock which existed in the browser followed by the web address being prefixed. These two were the most common and popular options witnessed by the users when using the website. Users also selected multiple security measures that they noticed and 8.7% voted for 1, 4, and 5. Looking into depth at these results, it can be witnessed that when the security measures were shown clearly the users identified them and automatically trusted the website to be safe which meant that the users may return to the website in future because a customer-business link was created.

Analysing the results in table 19 in more detail, 13% of individuals were aware of the fact that there was a closed padlock sign in the right bottom of the browser window. This high number tells that if the security being offered by the bank is clearly marked and visible to the user then it increases the trust levels in the user and they would feel more confident in browsing through the website.

8.7% of the individuals were awake that the security measures taken by the website were a closed padlock sign, the security certificate matching the name of the website and the web address prefixed with https. This high percentage again shows that individuals would react at the more high security features such as the padlock sign and the https prefix and notice details such as the name on the certificate matching to the name of the website. These three factors would give individuals more sense of security and ensure them the business has taken measures in order to protect their data and that the website is

Completely secure.

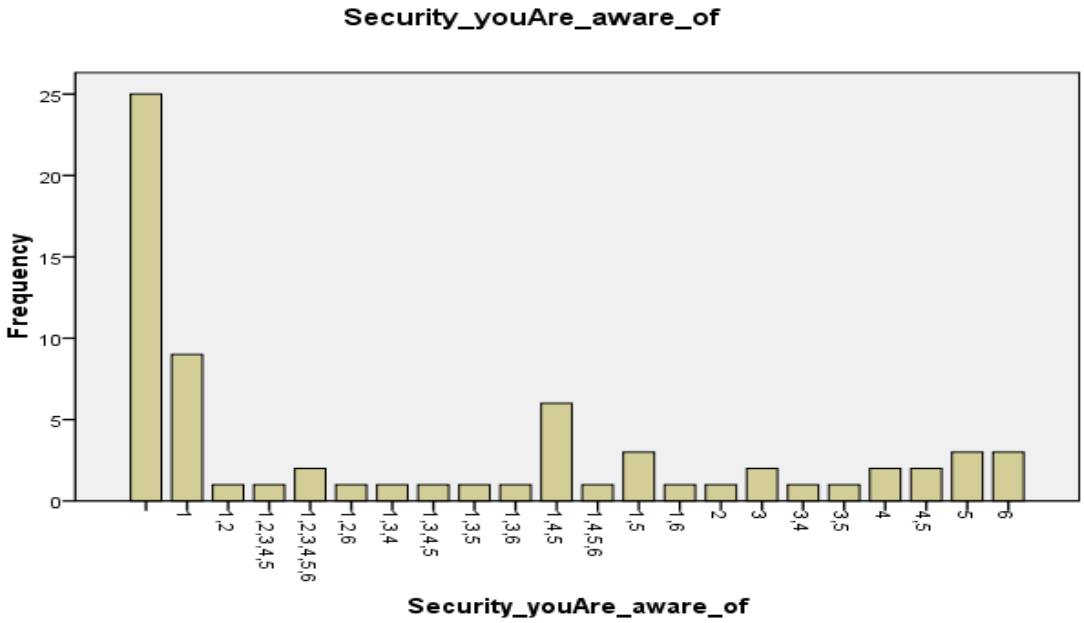


Figure 17: which of the following security are you aware of?

which of the following security are you aware of?	Value
1	29
2	6
3	11
4	17
5	21
6	9

Table 20: which of the following security are you aware of?

1. A closed padlock on the bottom right of your browser window

2. Your friends or colleagues in work have warned you about phishing

3. via an online search engine

4. The security certificate for the website matches the name of the website

5. The web address is prefixed with https in its address label

6. Other

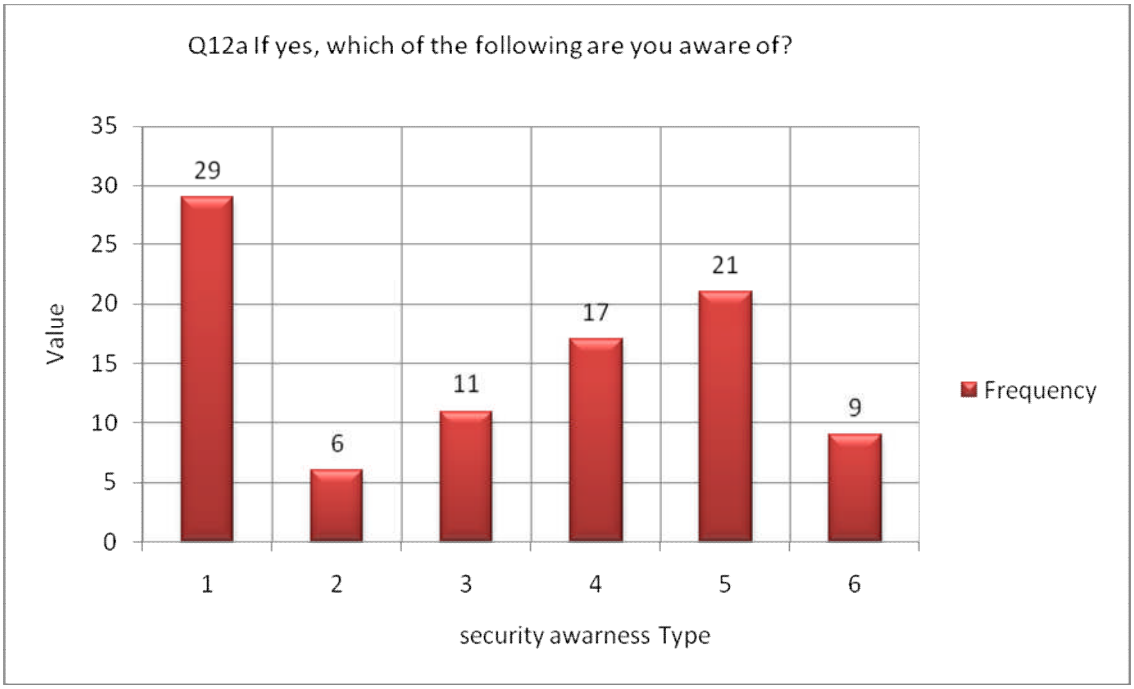


Figure 45: which of the following security are you aware of?

5.1.14 National wide Bank phishing E-mail:

When the users were shown the screenshot of the email they were asked to review it and then give their opinion whether they thought the email to be phishing or legitimate or they could not come to a conclusion. Of the data gathered in table 19, 68.1% of individuals straightaway picked up the fact that the email was a phishing scam where as 10.1% believed the email to be real.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		3	4.3	4.3	4.3
	Phishing	47	68.1	68.1	72.5
	Legitimate	7	10.1	10.1	82.6
	No Answer	12	17.4	17.4	100.0
	Total	69	100.0	100.0	

Table 21: Could you read the email above and answer this question: Do you think this e-mail is? (phishing or Legitimate NationalwideBank E-mail)

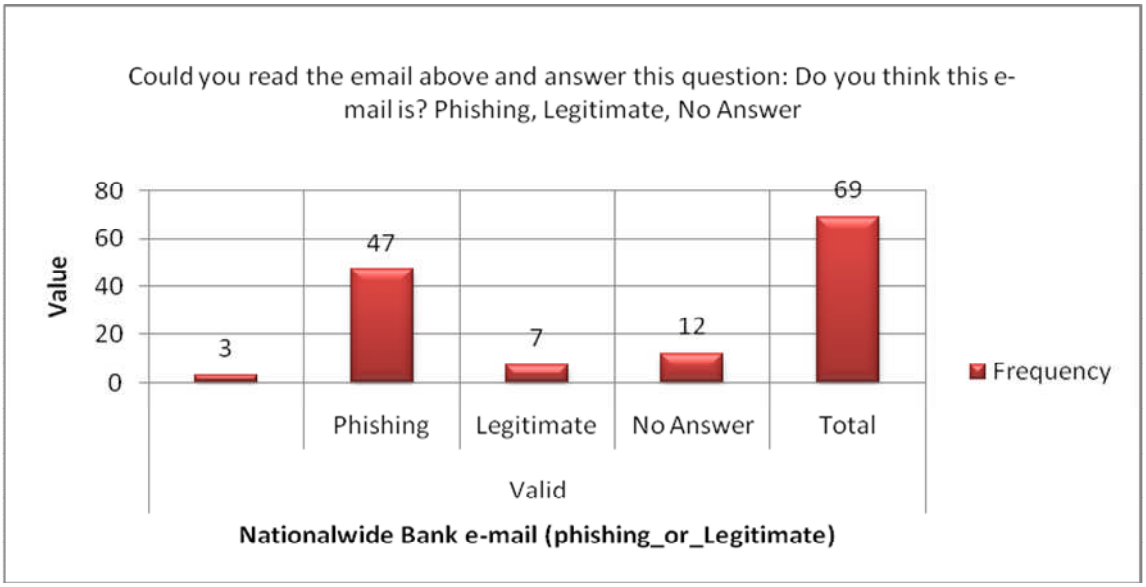


Figure 19: Could you read the email above and answer this question: Do you think this e-mail is? (phishing or Legitimate NationalwideBank E-mail)

According to the responses given by the individuals, when they were asked to clarify their answers they were interlinked but have been split into different categories.

Hyperlinks:

The link did not look genuine and when the mouse is hovered over the link it shows a web link to a different website rather than nationwide. Another individual interestingly noticed the fact that there was no https in the address diversion in the hyperlink and it was not addressed to the named person. Disguised links or forged URL addresses are another way of email spoofing (Drake, et al. 2004).

Information:

None of the banks would ever request such type of information online and banks would address the user with their name when contacting the user via email. Interestingly there was no logo included in the message which means that the message was not by nationwide themselves. No bank would request the user to change their password online and in this instance it encouraged the user to change their password. In reality, banks would not request users to update their information via emails. All such information is either changed in the back, over the

phone or when the user signs into their account, a message regarding it would be displayed to the user.

Overall the individuals detected most of the reasons which rightly contribute in suggested that the email is phishing rather than real as banks would never ask an individual to update their information online.

5.1.15 HSBC Bank E-mail:

When similar question was asked regarding the HSBC email the results did not change at all. 65.2% straightaway found out that the message being displayed was as a result of phishing where as only 8.7% thought that the message was legitimate. 20.3% avoided from answering so the analysis could only be carried out where an answer was obtained but graph produced took all the three options into consideration. The high numbers correctly identifying the email to be phishing shows the awareness that the people possess and that they would not fall for scams easier which means that the businesses cannot be blamed for any losses as a result of its customers being targeted by such phishing emails, yet the businesses need to keep their website security level up to the maximum and protect customer's data at all times.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		4	5.8	5.8	5.8
	Phishing	45	65.2	65.2	71.0
	Legitimate	6	8.7	8.7	79.7
	No Answer	14	20.3	20.3	100.0
	Total	69	100.0	100.0	

Table 22: Could you read the email above and answer this question: Do you think this e-mail is? (HSBC Bank phishing or Legitimate E-mail)?

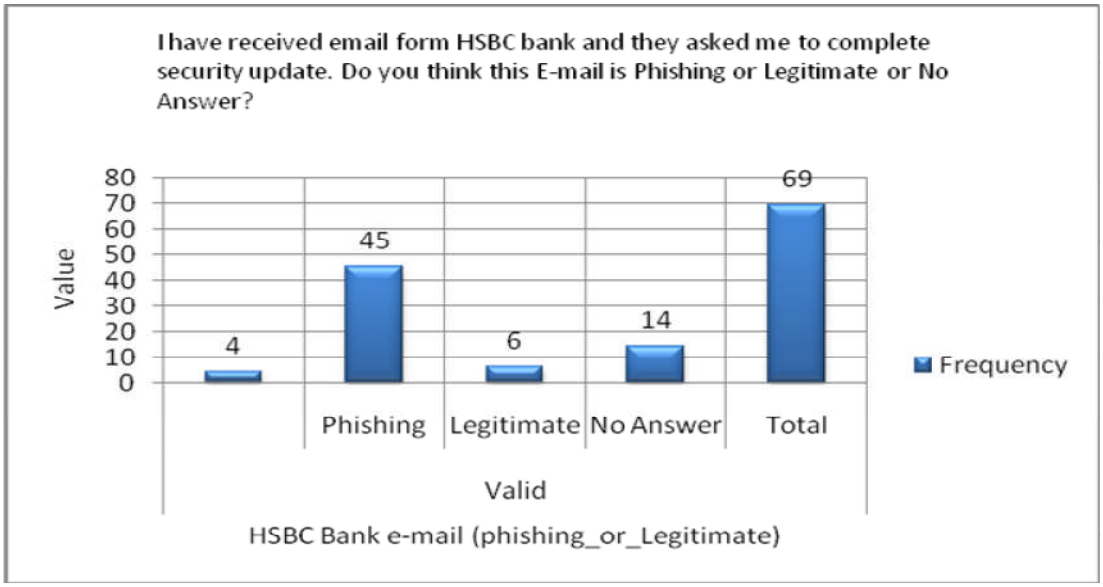


Figure 46: Could you read the email above and answer this question: Do you think this e-mail is? (HSBC Bank phishing or Legitimate E-mail)?

According to the user responses when asked to clarify their answers individuals replied that when banks would contact an individual they would address them with their name rather than "Dear Valued Customer" and the language used in the message is not what banks would use. Another point which individuals realized was that banks would never allow their customers to login through their emails and if a log in is required then it is via the hsbc website. Another response was the reason why the person was asked to update the account was not convincing and only if they required any information then they could easily gets in touch via post. All these type of responses show that individuals have become more aware now of how a phishing email would look like and with anything such as the logo, complete web address missing it could result in the uncertainty changing into 100% certainty.

5.2 Phishing case study:

5.2.1 Phishing email detail:

Date Reported: wed 21/4/2010

Visible Sender: GTbank

Return address: Guaranty Trust Bank (GeNS@gtbank.com)

E-mail format: HTML

URL of Web content:

http://guarantytrustbankplc.t35.com/www/gtbplc/guarantytrustbank/

Anchor text of URLs: HERE

Location: United States, California

Detailed server information:

http://gfx8.hotmail.com/mail/15.1.3059.0405/styles/base/hig.css

Comments:

- The email claims to be from a legitimate bank, in this case GTBank, and requests that the user follows link so that it (the bank) can verify the customer details so that it can activate a debit card.
- No legitimate company ask for confidential information such as requested when following the link given in the email.
- The link to this email no longer exists the web registrars and/or the APWG would have closed the site as soon as possible after it was verified as a phishing web site, differences of site occur daily and reported by users frequently but care still needs to taken as it could be days or even weeks before sites are dealt with sites have to be confirmed to be phishing or scamming web sites before action can be taken.

5.2.2 Phishing Email:

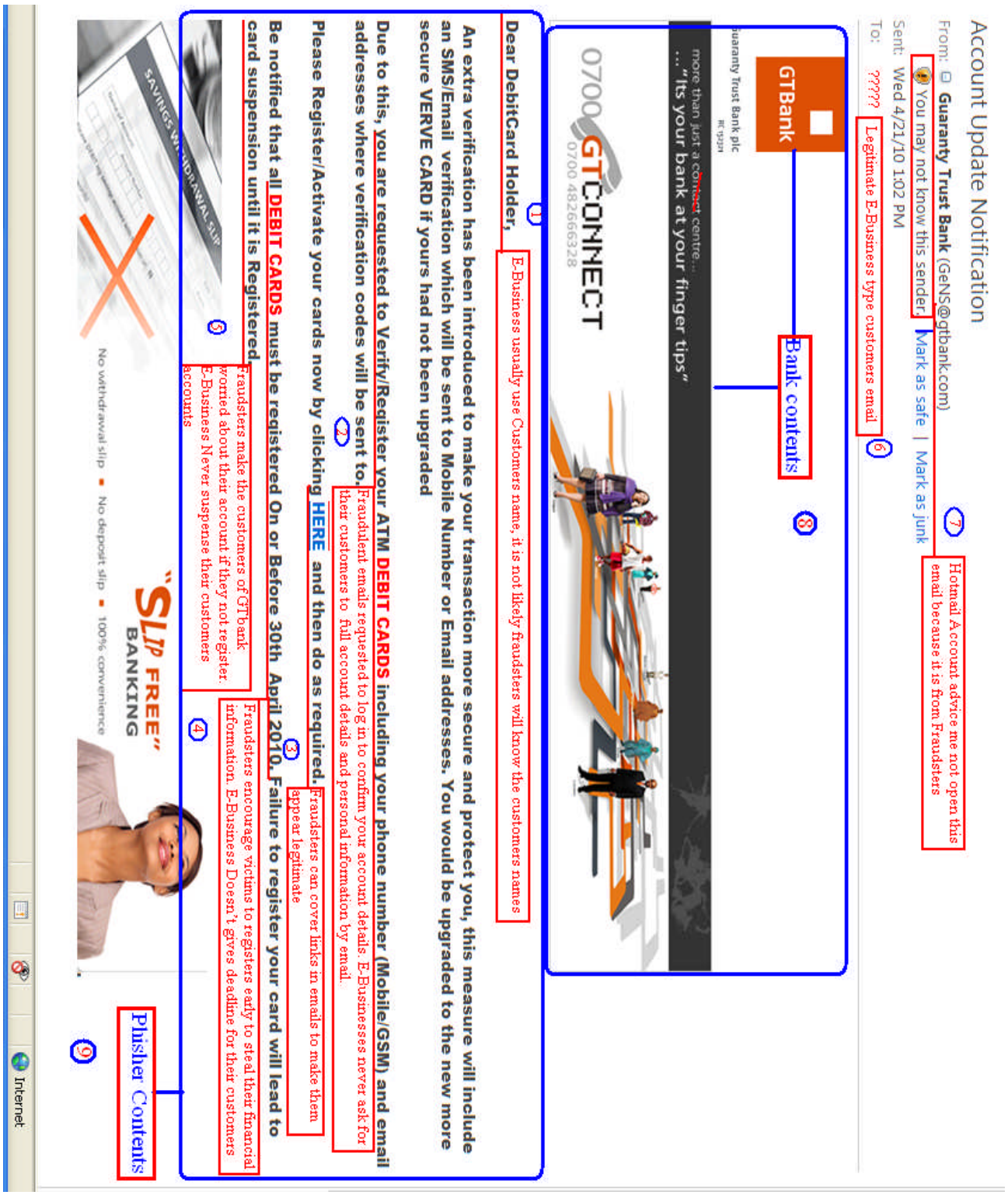


Figure 47:Phishing E-mail. Adopted from Hotmail Account(2010)

5.2.3 REASONS FOR SELECTING THIS CASE:

The purpose of selecting a case study in a research is to have a comprehensive understanding of the research object, an understanding that is as close to the practical world as possible. This case was selected due to the following reasons in this research.

- Selecting an example from a personal experience gives a more in-depth understanding of the situation. As the event or the situation happens to oneself, it is easier to draw conclusions from that occurrence. However, in such a case the subjectivity of that conclusion might be questionable, but usage of references can coagulate the evidence.
- It's "an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used" (Yin, 1984).
- The case uses two examples to put forward its argument. About such cases Yin (1984) said, "Validity, which comes first while doing research increases when multiple sources of evidence are used. This multi source case study approach increases not only the external but also the internal validity of research".

5.2.5 Phishing Email Explanation:

5.2.5.1 The "From:" Address

The "From:" address of an email cannot always be trusted as it can easily be faked by the criminals who send out the Phishing emails. In the case in hand it appears that the email has come from a "@gtbank.com email address", and while the Guaranty Trust Bank does use email addresses ending in "@gtbank.com", in this example the address has been faked as the link provided takes the user to a fake web site. How this is carried out is covered in chapter *3.11.2 - Forged Sender Addresses.*

5.2.5.2 The "To:" Address

It should be noted here that the "To:" address as most will not be personally addressed to a registered name. If it is not addressed that way then it may not be a legitimate message and therefore not from the organisation it claims to be. If the

"To:" address contains multiple addresses then this is a sign that the email may be a fake. The example does not carry any personal address information but is instead addressed to "*?????*" (Where the symbol????? represent a space with no personal or email information shown).

5.2.5.3 The Message "Subject:"

The subject of Phishing email may give signs to the fact that it is fake. In this case it is claiming to be from "Guaranty Trust Bank", if this were real then it would only be using the name "gtbank" and not "Guaranty Trust Bank ". Phishing emails will usually have urgent and exciting claims in the subject line or by the use of statements such as "Account Update Notification" or "confirm account information" (Kirby, 2004). Be careful of such emails as they are almost surely fake.

5.2.5.4 E-Business Logos

Phishing emails will always use real logo for the organisation they are trying to replicate. The logos are extremely easy for phishers to re-use so therefore exact logos of a company in an email cannot guarantee the legitimacy of that email. Many fraudulent websites in order to give legitimacy to the email use original company logos and images to deceive the users (Drake, et al. 2004). This is covered in chapter 3 and in the abstract section of this report.

5.2.5.5 Message Body of the Email

Phishing email messages will usually address their emails generically and almost certainly will not use a person's name as the message receiver. If they are claiming to be from a user's bank and they have addressed the email to "Dear Customer" or "Dear DebitCard Holder", caution must be observed as the email may be a fake. There are occasions at times when a company will send out a general email to all of its customers and in these circumstances it (the company) would never ask the receiver to give their personal and confidential information in order to verify their account legitimacy.

5.2.5.6 The Web Link

Supplying a fake web link is one way of how phishers attempts to get the user to their (phisher's) fake web site. Although the link may look genuine but when clicked would take the user to a fake or a disguised link (Drake, et.al. 2004), owned by the phisher. In this case when we click on the link in this phishing email we would be taken to a fake website at.

"http://guarantytrustbankplc.t35.com/www/gtbplc/guarantytrustbank/"
whereas the true website address is "http://www.gtbank.com/". To be sure that the site is genuine, one should never click on a link within an email but instead should use a reliable search engine to search for the genuine web address and then type the address that you know is correct into the web-browser address bar.

5.2.5.7 The Message Body

Spelling and grammar errors are common features together with a mix of UK English and American English. As many spammers are not English speakers they make errors which most English speakers would not. They may use "z" instead of an "s" or by mixing the two (organization (USA) & organisation (UK))in the same email. A message from a bank would be typed as "NatWest" and not typed "Natwest".these are different ways of creating visual deception to lure the users into committing a mistake (Hearst, et al. 2006).

The phisher hopes that a quick look at the senders address will be made whereas a more critical reading of the address, spelling, grammar etc is called for.

Phishers may also include some form of urgency (Kirby, 2004) in the email and request the users to respond quickly. There is a threefold reason for this:

- The phisher does not know how long his fake web site will remain active before it is discovered and closed down by the registrar or APWG.
- Giving the victim more time before he or she visits the bogus site increases the chances of the user being alerted by friends or colleagues to the phishing scam.
- The sooner the victim supplies the requested information the sooner can the phisher carry out whatever form of illegal activity it is they want to do.

5.2.6 Comparisons Between Legitimate and Phishing Emails[4]

Legitimate E-mail	indicators	Phishing E-mail
Customer name	Greetings	May have good greeting and not customer name
usually doesn't include spelling and grammar mistakes	Spelling	may include spelling and grammar mistakes
grants you period to think about their offer	Importance	uses disturbing or amazing short statements to immediately respond
No link including in the e-mail but might be phone number	Imbedded or Hidden Link or Phone number	Phone number and link appears in the body of e-mail
personal information and financial are not requested	Asking for private Information	They request personal information & financial to guide to a fake website.
e-mail address is reliable with the information of the sender e.g Identity, location	Sender	e-mail address may be faked with the identity, location of the sender
genuine institutions avoid asking personal and financial information by e-mail	Corporate E-mail Use	use of genuine institutions name and reputation to send a huge numbers of emails to customers and non customers and may request personal
Might be send clear and normal text	Text	may include disturbing or amazing text

Figure 48:Comparisons Between Legitimate and Phishing Emails. Adopted from: Personal Information and Scams Protection report (Royal Canadian Mounted Police , 2007)

There are several comparisons that may be drawn between genuine emails and phishing ones. These include:

- The victim may be greeted by his or her name though this is not the normal practice as phishing email usually is addressed to "Dear Sir" or Dear Customer", or may have no greetings included.
- Both may carry a statement of importance - completing the requested information by a certain date, immediate attention is required, please respond immediately for example. Legitimate emails may carry some form of time limited offer but a phishing email often carries a message that could be considered a threat or warning, such as closing a person's account unless they conform with the request immediately.
- Both legitimate and phishing emails may carry a phone number but where the genuine email will provide an office or call centre number, the phisher may

[4] http://www.rcmp-grc.gc.ca/scams-fraudes/student-etudiant-guide-eng.pdf accessed at 20.6.2010

provide a number which claims to be a genuine office number but may well as be a private address to take calls.

- Both may supply information such as sender, location, employees name etc but a phishing email will only have these to give a genuine look.
- Both legitimate and phishing emails will contain text but whereas the genuine email will be professional and polite without aiming to cause alarm or panic to the customer, the phisher may employee disturbing, hurrying or alarming tactics to get the desired information.

5.2.7 Guarantee Trust Bank Phishing website

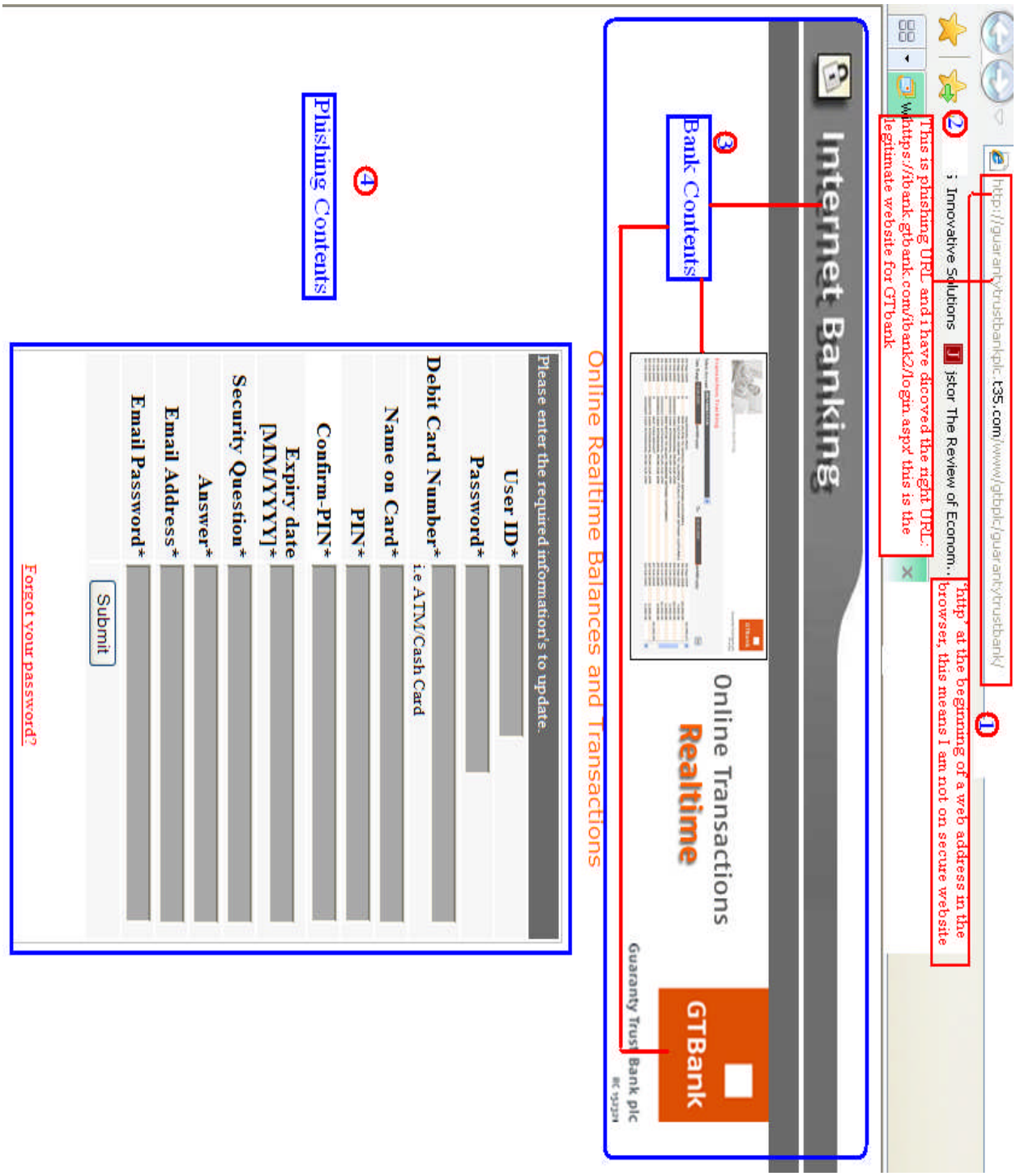


Figure 49:Guarantee Trust Bank Phishing website. Adopted from: Hotmail Account(2010)

5.2.8 Phishing Website Explanation:

5.2.8.1 The Address Type (HTTP vs. HTTPS)

All web addresses start with either HTTP or HTTPS. The "S" signifies that the website is using a secure connection. If no "HTTPS" is seen in the address bar and if a link is clicked that is declaring to be from a legitimate company or organisation then no details requested should be supplied. Legitimate websites never ask for confidential information on emails and even if a web site is genuine, but having a weak security system may lead to details being leaked to hacker through interception. The "secure" and "Truste" symbols on a web site can be easily faked.

5.2.8.2 The URL or Web Address

In this case the web address is:

http://guarantytrustbankplc.t35.com/www/gtbplc/guarantytrustbank/

It can be seen that this address has failed to use "HTTPS" and instead is using an unsecure address beginning with "HTTP" so any data sent will not be secure and secondly, while the web address seems to be legitimate,

http://guarantytrustbankplc.t35.com what follows www/gtbplc/guarantytrustbank" means that the user is not actually reading a page from the GTBank but from a fake site which is where personal information would be sent if it were entered. To an unaware user this address would not seem to be fake compared to an advanced user who would know that this address is faked.

5.2.8.3 GTbank Logos

As covered above, phishing emails will always use what appears to be a correct logo of organisations so therefore reliability of a company logo in an email cannot always be trusted.

5.2.8.4 Asking for your Cash Card Number

GTbank, or any other banking corporation, will never ask a customer to supply so much confidential information. There are times when a customer has to give his or

her card details and maybe even the security code on the back of the card (as in a financial transaction) but never would they (the customer) be asked for sensitive data.

5.2.9 Comparisons between Legitimate and Phishing Websites[5]

Legitimate Website	Indicators	Phishing Website
https:// padlock icon in the status bar and in browser address bar	Secure website signs	Fake security bar or not have any security sign
completely functional	Functionality	may not be completely functional or link to few the genuine website functionality
Personal information and financial are not requested. They have all the customer details	Asking for private Information	personal information and financial are requested
display the accurate domain name	Domain Name	status bar or address bar may be faked or include a similar domain name or not have a status bar at all
usually will not have error	Error in Browser Status Bar	may have errors while loading website page

Figure 50: Comparisons Between Legitimate and Phishing website. Adopted from: Personal Information and Scams Protection (Royal Canadian Mounted Police , 2007)

An "expert" phisher will try to make his phishing website look as legitimate as possible so as to lure many users as possible before the web site is suspended. The best way of gaining confidence from the user is to supply them with an email and subsequent web site that looks as genuine as possible. To this end there are several comparisons that can be drawn between legitimate and phishing web sites:

- While both may carry the https web address prefix only the legitimate web sites prefix is genuine and can be trusted. The phishing web site may fake the prefix so that it looks genuine, but is not.
- Some of the content e.g. logos may be used in both sites but as described in the abstract the phishing web site logos will be faked and trust cannot be built on logos alone.
- A legitimate web site may have few, if any, errors whereas the phisher site may be littered with poor grammar and spelling mistakes. But this cannot be taken into

[5] http://www.rcmp-grc.gc.ca/scams-fraudes/student-etudiant-guide-eng.pdf accessed at 20.6.2010

account at all times and cases because at times a phishing website may have no writing errors where as a genuine website may contain fair amount of errors, yet they are legitimate.

- A legitimate web site may require the input of screen name and password it will not ask for any other information from a user. A phishing web site may ask for this information also but will request a lot more personal information from the user such as debit card number, expiry date, security code, address, full name etc. The reason for this is that the more a phisher knows about a person the more likely he is of succeeding in the scam by changing passwords, withdrawing funds, ID theft etc.

- Some phishing web sites may appear to be functional e.g. entering of details, internal links, messages etc but these can be compared to a trial version of software or a virtual reality driving site; they may look functional but in reality, nothing works. A legitimate site will have all its contents fully functional with exceptionally throwing up an error message box that apologises for the failure of the active content at times when a fault is developed in the site or when the active link is “timed out. It is here that a phishing site can be compared to a genuine one in that it is easy for an error message box to be displayed every time a fake internal link is clicked.

5.2.10 Anti – Phishing Email Chart:

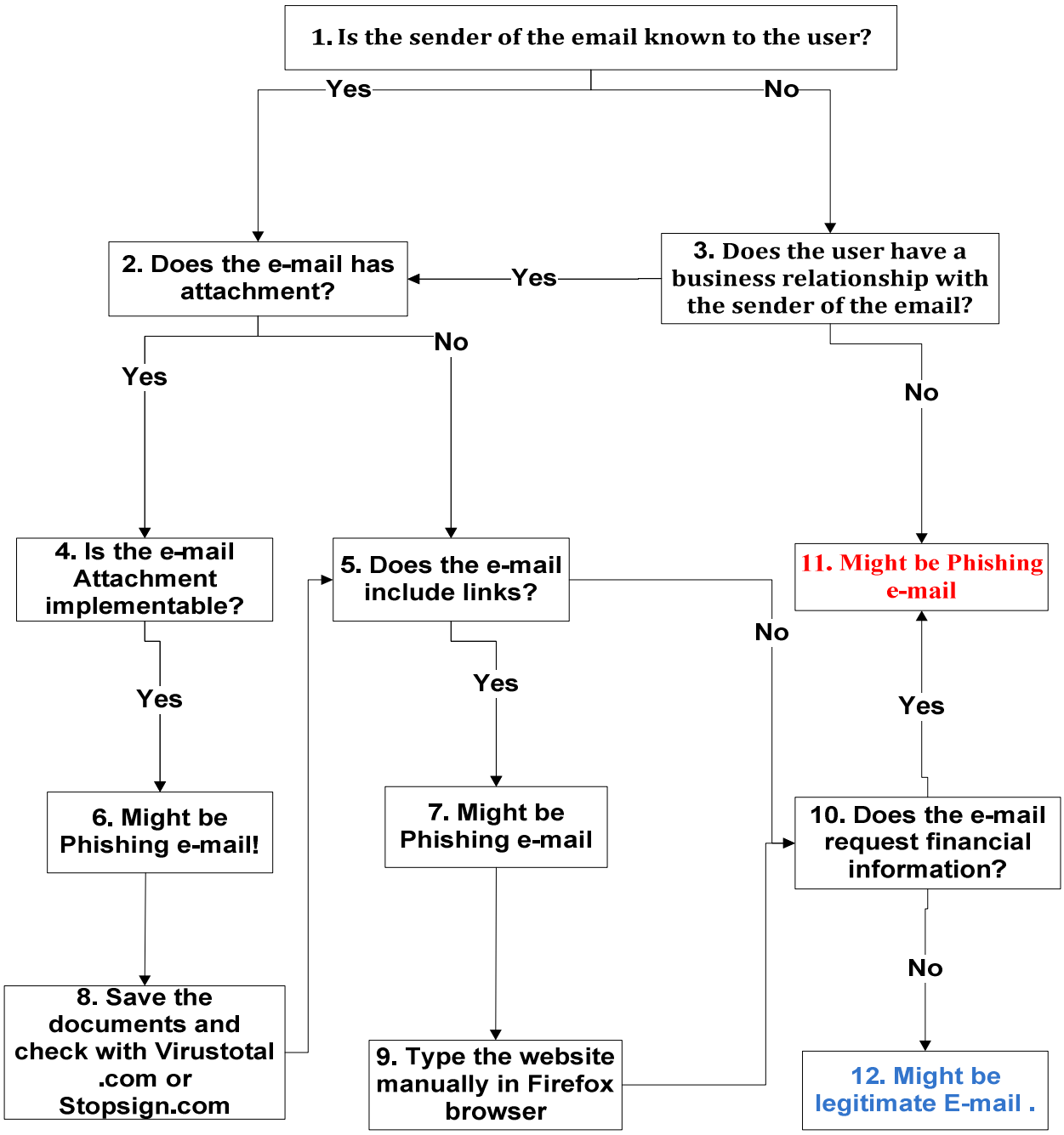


Figure 51:Anti – Phishing Email Chart

5.2.11 Genuine and Phishing Email Trail

1. Is the sender of the email known to the user? Phishers often use the disguise of genuine companies (banks, online shopping sites such as EBay, credit card companies etc) to try and convince the victim that the email is genuine and not fraud.

2. An attachment to an email may be easy method of a phisher but is generally not used by a genuine company which prefers to use links to their secure web site. Unfortunately this is also a common method of phishers as well. In either case, caution should be applied as it is still not yet known if the email is genuine, or phishing.

3. Does the user have a business relationship with the sender of the email? NatWest bank, for example, would not send an email to a non NatWest bank customer, neither would the USA based Wells Fargo bank or GTBank would send to a non investor or borrower. Any emails received from such companies should be dealt with care as it is almost certain that any such messages are phishing. The major players in the email business (Yahoo, Hotmail and Gmail etc) normally recognise these as scam emails and will post them to the "junk" folders of the user's email box. This is not always the case so it cannot be assumed that, "because Gmail did not recognise it as junk, it is safe" should not be taken with any great confidence.

4. Not all attachments contained within an email are active. A phishing email attachment could be a plan by the phisher to get the user to click on the attachment and, once selected, a malware might be downloaded to the user's computer and get activated directly.

5. A link provided in the email might be a true link to a legitimate site but, it could also be a link to a phishing site set up by a phisher so caution should be taken when clicking on them.

6. An active attachment should be treated with caution as it may not be as clean as it may appear and could cause the implementation of a piece of malware which, when automatically downloaded may install a threatening program such as a key logger or screen logger on the victim's computer.

7. A link to another web site should be subjected to caution if the sender of the email has no business dealing with the user as the link may be to a phishing web site set up by a phisher. To be sure that the link is a genuine site it is advised that the web address is typed into the address bar and not clicked on as the email requests. The link may look genuine but could well be phishing.

8. Any suspicious emails or web sites should be checked for validity and if needed, should be reported to the true owner of the site or to APWG etc.

9. Phishers often use varying font styles to help disguise the link and, unlike an address written on a letter and posted, an email or web address has to fit exactly the address which was registered. www.lloydstsb.co.uk may look genuine but the 2nd "l" has been replaced with the Greek letter "Iota".

10. If the email does not request any sensitive or confidential information then the email might be genuine. This is especially so if no forwarding link or attachment is provided for selection by the user. The main problem with these emails is that scammers often use emails to discover if an email is active or dead. The very action of opening this type of email alerts the scammer and informs him that the email address is still being used. While in itself, no harm is done, it can mean that the email address will be inundated with rogue emails for services, financial and other secret offerings, some of which could be phishing emails.

5.3 Phishing Countermeasures:

Jakobsson and Myers (2008), suggest the following countermeasures in order to avoid a phishing attack from happening or by taking steps in the absence of any crisis to improve the responsiveness and mitigate damages. Phishers generally have multiple techniques and methods at their hand in carrying out attacks and therefore there is no single measure that can counter all these attack vectors (Ollmann, 2004).

5.3.1 Detecting a likely attack:

A phisher generally sets up a domain to receive phishing data. Therefore one method of countering this can be the preemptive domain registrations that targets spoof domains which can help in reducing deceptively named domain. Jakobsson and Myers (2008), also suggest that phishers while creating phishing servers may save a copy of the legitimate website which is being copied. Analyzing these access patterns in weblogs can help in detecting phishers' downloading activities.

5.3.2 Preparing for a likely attack:

Preemptive actions can make companies' establish safeguards in countering any future attacks. These actions may include:

- Providing customers with a spoof reporting email address where feedbacks can be sent by the customers regarding such emails. Warnings of potential threats to customers can also be passed on.
- Monitoring of "bounced" emails can help in identification of a possible phishing attack being carried out as phishers often email bulk lists that may include addresses which are nonexistent.
- Monitoring customer calls relating to certain pattern of inquiries such as changed passwords, can indicate a possible phishing attack.
- Monitoring the usage of corporate logos and art work that phishers may copy to deceive customers.

5.3.3 Email Filtering:

Email filters are a good defensive technique in countering phishing emails. Anti phishing spam filters can be designed in a way to identify specific known phishing emails and then prevent them from reaching the customer. These spam filters can be installed at different installations such as ISP gateways, or as a software on a PC (Youl, 2004).

5.3.4 Email Authentication:

When phishers send emails to possible targets, they make it look as legitimate as possible and being received from a trusted site. They may use techniques such as:

- Faking a return address;
- Registering a cousin domain (e.g. Paypal-security.com to spoof a legitimate domain name Paypal.com).

Message authentication technique provides an assurance that the email was received from a legitimate source or sent from a party named as the sender. Once these authentication methods are deployed phishers are generally left with no options but to reveal a suspicious looking return address to escape detection.

Email authentication techniques such as Sender-ID, SPF (Sender Policy Framework), and DKIM (Domain Key Identified Mail), prevent return address forgery by checking and verifying cryptographic signatures through DNS records (Jakobsson and Myers, 2008).

5.3.5 Cousin Domain Rejection:

In these types of phishing attacks the phishers' obtain domain names similar to the targeted domain, such as "PayPel.com" instead of "PayPal.com". Users often fail to recognise these subtle differences and fall prey to such trap.

Analyzing the originating addresses of incoming mail messages and interfering with the delivery of messages originating from illicit domains can prevent cousin domains from harming and deceiving users. Similarly such techniques can be applied to other components of a URL, such as sub domains, which can be deceivingly similar to the legitimate domain name.

5.3.6 Secure Patching:

Security vulnerabilities are generally exploited by phishers using malware techniques. Users that run unpatched operating systems face the risk of getting infected with malware by even connecting to the internet. A fully patched computer behind a firewall is another way of defense against exploit-based malware installations.

5.3.7 Padlock and http:

Keeping a check on the padlocks on the status bar or http:// at the start of the URL, while submitting sensitive financial information can be a useful technique in preventing users from divulging information to phishing servers (Youl, 2004). Their presence may not guarantee any security but the absence of these indicates that the website is not secure.

5.3.8 Customer Education and Awareness:

If customers are not aware and educated well enough regarding internet frauds, than they remain vulnerable to the phishing attacks that are evolving at a rapid rate. These phishers use methods that are convincing and deceive an average user into passing of sensitive information. Consumers need to train themselves on the interned fraud, the changing trends and the continual development of deceptive techniques by phishers in luring the users into a trap (Youl, 2004).

5.4 Summary:

This chapter discusses the survey responses in light of the questionnaire created for collecting the phishing data in carrying out the research. Questions such as the awareness among respondents regarding online phishing were asked, and encouraging results were received as 84% of the survey respondents agreed to knowing about this fraud technique. The survey also suggested that 65% of the respondents use internet to shop online not more than 10 times in a month. This can suggest that although e-commerce technology has improved the shopping patterns but the security needs of the customers may remain questionable. The scope of the problem can also be judged by the fact that 48% of the respondents received 10 or less fraud emails in last 1 year, where as 13% of the respondents as per the survey results; have fallen victims to phishing emails suggesting that no

matter how many times users receive phishing emails, a certain percentage may fall victim to this hook every time.

The survey also suggests that 12% of the respondents may have lost between 100 to 1000 pounds due to phishing. The IC3, 2009 report also suggests that majority of losses users face lies between $100 and $1000 if seen from a dollar perspective. In terms of responding to such emails, 36% of the users suggested that reporting to police, password change, contacting the banks/company immediately etc may save them from getting in this lure. 24% of the victims continue to shop online as they may have become aware and educated and continue to practice this knowledge in keeping this threat away, where as 49% of the respondents seem satisfied to the complaints they made to their banks/company. The survey overall suggests that 56% of the survey respondents seem aware of the website security warnings and data protection symbols such as padlocks, security certificates, address labels etc.

CHAPTER 6

CONCLUSION

6. CONCLUSION

This chapter gives the concluding remarks of this study in light of its objectives. These objectives were to identify the impact that phishing has on an e-business and how such businesses as well as individual users can mitigate this threat with the help of certain tools, techniques combined with awareness of the problem. The phishing patterns in the study suggests the fact that such phishing scams are not easy to detect and phishers while enticing users into the trap make huge sums of money ranging from tens of thousands to millions of dollars in the process. Similarly businesses and consumers have been deeply impacted by this crime as significant short and long term financial losses have affected the overall financial health, stability, brand, and reputation of several products worldwide.

For the purpose of meeting the objectives of this study, a questionnaire and a case study were analysed. The questionnaire targeting online consumers was dispatched to a random sample of people from all walks of life to study the patters of online usage and vulnerability of users in getting attacked by such sophisticated phishing techniques. Nearly 84% of the respondents showed signs of awareness of the phishing threat looming around, but still this threat doesn't seem very serious to these users as they have never come across any damages as 20% of the total respondents received more than 50 phishing emails during a year, 13% of the respondents fell victims to such emails, and 24% of the respondents continue shopping online even after falling victims. But in this case it can also be suggested that these 24% of the victims who continue to shop online may have got better educated and use protection mechanisms in ensuring a safe transaction. Whereas 8% of the victims suggested that they don't shop online any more as their losses and victimisation may have caused a negative psychological effect on their usage behaviors. These negative psychological behaviors may have a direct or indirect link with the level of losses theses victims may have faced. The study in this regard also sheds light on the levels of losses and damages users faced as nearly 12% of the respondents who became victims to phishing emails lost between $100 and $1000.

The study also concludes this encouraging fact that nearly 37% of the respondents while responding to a phishing email may take actions involving reporting to police, changing the password settings, and contacting the business/bank regarding the email. 54% of the respondents suggested being provided by security software by their banks which surely supports users in mitigating this live threat and also facilitate in improving the awareness among customers. Businesses educating their customers through necessary actions such as providing free security software on their websites and also giving details as to how phishing emails look like and what are the likely indications in identifying a legitimate email with a fraud one may help a lot of users who remain aloof to this threat e.g. RBS offers phishing email examples to their customers on their website. 49% of the respondents as per the survey results have shown their satisfaction over the actions taken by their bank or business against phishing complaint as these businesses have gained insight regarding the phishing threats and are now more prepared to tackle this issue while also keeping their customers safe and satisfied.

Nearly 23% of the respondents felt that businesses should have a dedicated anti phishing department working round the clock in making sure such emails don't circulate and reach their customers, secondly the data encryption on the websites and transactions maybe more secure and equipped. And thirdly all these security features should be present on the website to make it a secure tool in carrying out transactions.

As phishers use techniques such as deceptive images, false links, and fake images of security indicators, businesses need to be aware of such creative fraud techniques and enforce tough steps in countering these threats by ensuring early threat detections, email authentication techniques, domain controlling and rejection techniques, secure patching and firewalls, dedicated SSL protected pages, and user awareness etc. It can also be said here that enforcement policies employed by businesses that react automatically when a particular policy gets violated may yield the best security results, but the security tools discussed above,

no one tool or technique can be branded as the beat and relied on exclusively and therefore a combination of tools should be put in place in countering such threats.

Online businesses and Government should fight this kind of online crime especially in developing countries like Nigeria. Law enforcement as well as government agencies should work more closely in combating phishing through consumer awareness; education; practice awareness; authentication techniques; law enforcement efforts; reviewing internet crime legislations; improving reporting mechanisms; and improving data security and integrity; usage of current security protection and protocols etc. There are some reasons why phishing is increasing in these regions and why online businesses suffer in term of law and fighting phishing:

1. International locations with no electronic fraud laws.
2. Locations with such fraud laws but not being strictly enforced.

At the end it is imperative to suggest that consumer education is the most significant of techniques in fighting phishing attacks. This education initiative can be spread with the support of government agencies, law enforcement authorities, financial institutes, ISP providers, software companies, banking industry, and all such businesses who share presence on the internet. Combating this menace requires businesses and consumers to adopt best practices

CHAPTER 7

LIMITATIONS & RECOMMENDATIONS FOR THE RESEARCH

7. LIMITATIONS AND RECOMMENDATIONS:

7.1 LIMITATIONS:

The limitation of my project has been discussed below like any other research:

7.1.1 Time restriction:

This project faced time limitation in my research and I couldn't finish my work early because of lengthy subject and having numerous points worthy enough to be discussed in more detail. Some of the limitations are explained below:

7.1.1.1 Interviews:

Interview gives more useful information and better analysis for the research questions and we could gather results from both survey and interviews to give us useful and in-depth information. Interviews were not selected as they are costly and take more time to arrange, collect, analyse, and becomes difficult to avoid any biasness in the results.

7.1.1.2 Targeted audience:

Due to shortage of time and resources the questionnaires sent may not have reached the desired audience and therefore floated to public at large for the online customer survey. For this research another questionnaire targeting the business users was also sent to 485 companies but unfortunately no responses were received to make the final results more valid and practical. A greater return may have led to better results being produced.

7.1.2 SAMPLE SIZE:

Approximately 400 internet users were sent one of the two types of online survey and of these only 69 replied to the survey. The results of the survey were interesting in that they showed how aware many users are of internet fraud and

phishing emails and also showed that even with well educated how easy it can be to fall victim to phishing emails and phishing web sites. However, this small survey response size cannot be said to be indicative of all internet users in that insufficient returns did not produce enough results to allow e-businesses to make decisions as to the awareness and possible victims of phishers for their online customers.

A larger questionnaire response size would have created more effective result for e-businesses and given a reflective image of the online users and phishing activities taking place on the internet at this time. The samples are not representative of all types of online users, as the main respondents to the survey were friends, students, and limited number of business users.

More than 480 online companies did not reply to the online business survey and this affected the research paper enough to distort any results and therefore to reach any real conclusions.

7.2 RECOMMENDATIONS:

7.2.1 Recommendations for Online business:

Recommendations of steps that can be taken to reduce phishing attacks include:

- Phishing sites do most of their damage and steal the majority of confidential information from their victims in the first hours of the phishing scam being launched and so it is vital that the domain is closed down as quickly as possible. Once the registrar is notified and confirmed the criminal activity connected with that domain it will be able to shut the site down but it is often dependent on businesses and individuals to notify them of sites.
- There are many sources that can provide information to identify malicious activity. The APWG provides a continually updated listing all of the phishing URLs identified by the APWG community and these can be used to check for phishing scams. Companies such as the SORBS Dynamic User and Host List can provide networks linked to dial-up, DSL, and cable networks that are more likely to be abused. The Composite Block List (XBL) may indicate fraud. (APWG. 2009)

- As soon as a phishing scam associated with a particular company has been showed the scam company should alert all its online customers and employees of the fake site or email so as to help minimise their staff or customer from fallen victim. As mentioned earlier in this report, many individuals fail to update the security settings or patches so it is even more necessary that all customers are aware.
- Draw up guidelines and rules concern the receiving and sending of emails to third party addresses, i.e. anyone not associated with the company and its business. Issue a security policy that states what sites an employee can and cannot visit and what can and cannot be downloaded from such sites.
- Train all employees on the risks and possible results of falling victim to a phisher and show them examples of phishing sites as compared to genuine sites from the same company. Regular coaching sessions should be carried out to show compliance with company policies and guidelines.
- Investing in software that can block all messages containing evidence or likelihood of phishing, infected attachments or links to infected websites, as well as all requests to visit websites infected with phishing malware that masquerade as legitimate websites or have been agreed as being unnecessary third party sites.

7.2.2 Recommendations for online Users:

By following a few simple guidelines individuals can help protect themselves from phishers, though it must be said that even following all safety precautions may not totally prevent confidential information from being stolen as expert phisher will always find a way to trick some users.

The following are some guidelines that individual users can follow to help secure their online data:

- Be suspicious of any email with requests for personal financial information especially when informed that the request is urgent or from an unknown source.
- Unless the email is digitally signed it cannot be trusted and that it wasn't forged or spoofed.
- Phishers usually include false disturbing or exciting messages in their emails. This is to get people to react immediately before the phishing web site is closed

down or before the user is informed of the phishing scam by the company being scammed.

- Virtually all phishing scams ask for information such as username, password, credit card numbers, date of birth, address, etc. Therefore such information should never be passed on through e-mails. If e-mail has been received from the users own bank, then they should call and confirm if such email was being delivered or not.
- Phisher emails are normally not personalised, but they can be; that is, they usually begin with, “Dear Sir or Madam”, instead of, “Dear Mr Smith”. Valid messages from a bank or e-commerce company generally are personalised. If in doubt it is always recommended that the bank etc is called to confirm the legitimacy of the email.
- Be wary of links in an email, instant message, or chat room to get to any web page if there is the slightest suspicion that the message might not be authentic. Check all email links etc to see if the address is from who it says. If in any doubt never follow the link because the very action of clicking a link can activate malware which can be downloaded to a computer. Even the best firewall can be bypassed this way as it is the user who has agreed to accept the address rather than a phisher trying to ‘force his way into a network’.
- Avoid filling out forms in email messages that ask for confidential information as this should only be filled out on a secure web site or on the telephone as phishers are able to 'spoof,' or forge both the "https://" normally seen on a secure Web server and a legitimate-looking address.
- Enter a banking or similar web address manually so as to be certain that the web site is genuine to that particular banking, shopping, auction, or financial transaction website and do not rely on displayed links as these may be bogus.
- Check that the yellow lock seen near the bottom of the screen on a secure site has not been forged. When double-clicked, the lock displays the security certificate for the site. Any warnings displayed that the address of the site displayed does NOT match the certificate is sure knowledge that the web site displayed is fake and the site should not be trusted.
- Always accept the latest security updates from Microsoft or other similar company as these often contain the latest security patches or software to help in

the fight against phishing and other scams. The latest version of web browser, IE8 for example, has a tool bar to help protect the user from known fraudulent websites. These toolbars match where you are going with lists of known phisher Web sites and will alert the user of possible bogus sites.

- Regularly check any online accounts held for suspicious transaction and any found should be reported to the institution concerned (credit card company, bank, EBay, PayPal etc).
- However all online businesses SHOULD provide free security software and another methods for their customers. For examples, online businesses SHOULD message their customers when the customer's account is login and message them when some money spends it from their account. If online businesses do so, they might avoid refund some money to their customers.

8. REFERENCES

Turban,K,M,M,L,V (2008) "Electronic Commerce. A Managerial Perspective" 2008 Ed, Pearson International Edition

Goueff, S (2000). "The draft cyber crime convention. Creating an international law enforcement standard". Vol.2, No.6. Camford Publishing Ltd.

Rayport, J.F., and Jaworski, B.J. (2003). "Inroduction to E-commerce", 2nd Ed. New York: McGraw Hill

Laudon, K.C., and Traver, C.G. (2009). "E-Commerce: Business, Technology, Society", 4th Ed, Prentice Hall

Damanpour, F. (2001). "E-business E-commerce Evolution: Perspective and strategy". Department of finance and business law, James Madison University, Virginia, Vol.27, No.1.

Emarketer (2010). "Retail E-Commerce in Western Europe". [Online: web] Viewed: 22nd June 2010. <http://www.emarketer.com/Reports/All/Emarketer_2000679.aspx>.

Schneider, G.P. (2002). "E-Commerce", Boston: Course Technology, Thompson Learning.

Varian, H.R. (2000). "When commerce moves online, competition can work in strange ways", New York Times, New York, N.Y, Published: August, 2000. [Online: Web] <http://people.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-08-24.html>.

Tedeschi, B. (2007). "Web Videos Let Car Buyers Survey Their Many Choices". New York Times, N.Y, Published: May, 2007. [Online: Web] Viewed: 4 June 2010. <http://www.nytimes.com/2007/05/14/technology/14ecom.html>.

Rudman, R.J. (2009). "Incremental risks in web 2.0 applications". The electronic library, Vol. 28, No.2, pp. 210-230. Emerald Insight Ltd.

Burton, J. (2008). ""UK public libraries and social networking services", Library Hi Tech News, Vol. 25 No. 4, pp. 5-7. Emerald Insight Ltd.

Hamid, S. (2007). "Web 1.0 vs Web 2.0". [Online: web] published: August 2007, Viewed: 5 June 2010.<http://www.sizlopedia.com/2007/08/18/web-10-vs-web-20-the-visual-difference>

Kawamoto, D. (2009). "internet users worldwide surpass 1 billion". Published: January, 2009, Viewed: 7th June, 2010. < http://news.cnet.com/8301-1023_3-10149534-93.html>

McKinsey Quarterly. (2007). "*How businesses are using Web 2.0: A McKinsey Global Survey*". Published: January, 2009, Viewed: 10th June, 2010.<https://www.mckinseyquarterly.com/Marketing/Digital_Marketing/How_businesses_are_using_Web_20_A_McKinsey_Global_Survey_1913?pagenum=3#sidebar1up >

Andam, Z.R. (2003). “e-Commerce and e-Business”. e-ASEAN Task force, UNDP Asia Pacific Development Information Program (APDIP). [online: web] Viewed: 10june 2010 http://www.apdip.net/publications/iespprimers/eprimer-ecom.pdf

Lord, D. (2001). “B2B E-commerce: From EDI to eMarketplaces”. Technology reports, Business Insights. [Online: Web] Viewed: 15June 2010. http://www.globalbusinessinsights.com/content/rbtc0047m.pdf

U.S Census Bureau. (2010). “E-Stats – Ecommerce 2008”, [Online: web] Viewed: 15June 2010. <http://www.census.gov/econ/estats/2008/2008reportfinal.pdf>

Stambor, Zak. (2010). “M-Commerce sales to hit $2.42billion this year – and 1.53% of e-commerce”. Internet Retailer.com, published: April 2010. [online: web] viewed: 10 June 2010 <http://www.internetretailer.com/2010/04/16/m-commerce-sales-to-hit-2-42-billion-this-year-and-1-53-of-e>.

Coda Research Consultancy. (2010). “U.S mobile advertising and mobile commerce revenues, with forecasts to 2015”. Report released: April, 2010. [online: web] viewed: 12 June 2010. http://www.codaresearch.co.uk/usmobilerevenues/growth.Bmp

Internet Retailer. (2010a). “Trends and Data: Online retain sales growth”. [Online: web] Viewed: 16June 2010. < http://www.internetretailer.com/trends/>

Internet Retailer. (2010b). “Trends and Data: Broadband access in the U.S”. [Online: web] Viewed: 16June 2010. < http://www.internetretailer.com/trends/internet/>

Al-Slamy, N.M.A. (2008). “E-Commerce Security”, IJCSNS International Journal of Computer Science and Network 340 Security, VOL.8 No.5, pp 340-344.

Clifton, C. et.al. (2002). “Directions for Web and E-Commerce Applications Security”, Working paper 4259-02, MIT Sloan School of Management. [online: web] viewed: 13June 2010. http://dspace.mit.edu/bitstream/handle/1721.1/1853/4259-02.pdf?sequence=1

Grazioli, S. (2004). “Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet”, Group Decision and Negotiation Vol. 13, pp: 149–172. Springerlink Ltd.

Chou, D.C. et.al, (1999). “Cyberspace security management”. Industrial management & data systems. Vol.99, No.8. pp. 353-361. Emerald Insight Ltd.

CyberSource, (2010). “Online payment, fraud trends, merchant practices and benchmarks”, Online Fraud Report, 11th Annual Edition, 2010. [Online: web] viewed: 14 June 2010. <http://img.en25.com/Web/CyberSource/CSC118_FR2010f_012110.pdf>

IC3, (2009). “Internet Crime Report 2009”. [Online: web] viewed: 14June, 2010. <<http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf>

Barik, M.S., et.al, (2005). “E-commerce security – A life cycle approach”. Sadhana, Vol. 30, Part: 2 & 3, pp.119-140. [Online: web] viewed: 10 June 2010. http://www.ias.ac.in/sadhana/Pdf2005AprJun/Pe1335.pdf

VeriSign, Inc. (2004). "Industry Update: Internet security intelligence briefing", Vol. 2, No. 2. [online: web]viewed: 12 June 2010 http://www.verisign.com/static/017574.pdf

Tront, J.G. and Marchany, R.C. (2002). "E-Commerce security issues", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

Khusial, D., and McKegney, R. (2005). E-Commerce security: Attacks and preventive strategies", [online: web] viewed: 12 June 2010. http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html

OECD, (2008). "OECD policy guidance on online identity theft", Ministerial meeting on the future of Internet Economy. [online: web]viewed 10June 2010. http://www.oecd.org/dataoecd/49/39/40879136.pdf

Barker, K.J., et.al (2008). "Credit card fraud: awareness and prevention", Journal of Financial Crime, Vol.15, No.4, pp. 398-410. Emerald Group Publishing Limited.

Statistical Bulletin, (2008). "E-commerce and information and communication technology (ICT) activity, 2008", Office for National Statistics, UK. [Online: web] Viewed: 12 June 2010. http://www.statistics.gov.uk/pdfdir/ecom1109.pdf

Granova, A., and Eloff, J.H. (2005). "A legal overview of phishing", Computer Fraud and Security, July 2005.

Price, S. (2008). "Phishing Warfare Against Armed Forces", IAnewsletter, vol.11, No.4, pp. 5-31.

Eimgh, A. (2005). "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", ITTC Report on Online Identity Theft Technology and Countermeasures.

Tippingpoint. (2005). "Phishing Protection Data Sheet", [Online: web] viewed: 19June 2010. http://www.tippingpoint.com/pdf/resources/datasheets/400951-001_Phishing.pdf

Youl, T.(2004). "Phishing Scams: Understanding the latest trends". A white paper presented by Fraud Watch International, June 2004.

Anti Phishing Working Group, (2009). "Phishing Activity Trends Report – 4th Quarter 2009". [online: web] viewed: 22June 2010. <http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf>

Fitzgerald, T. (2008). "The Ocean is Full of Phish", Information Security Management Handbook, 6th ed. Vol. 2, Boca Raton, FL: Auerbach.

Jakobbson, M, and Myers, S. (2008). "Phishing and Countermeasures: Understanding the increasing problem of electronic Identity theft", Wiley Interscience, Hoboken, New Jersey: John Wiley & Sons, Inc.

Rachael, L, and Russel,D,V. (2005)."Phishing Cutting the Identity Theft Line", Wiley Publishing, Inc.

Wheelock, P. (2005). “Phishing Hook, Line and Sinker”, Security tip of the month, Microsoft Security TechNet. [online: web] Viewed: 21st June 2010. < http://technet.microsoft.com/en-us/library/cc512621.aspx>

Pacchiano, R. (2010). “Phishing: Falling Hook, Line and Sinker - Tips for Quickly Spotting and Avoiding Phishing Scams”. Software Reviews, Win Planet. [Online: web] Viewed: 24th June 2010. < http://cws.internet.com/article/3038-.htm>

Montalbano, E. (2007). “Phishing Scams Hook Few”, Consumer Advice – PC World, October 2007. [Online- web] Viewed: 22nd June 2010. < http://www.pcworld.com/article/138150/phishing_scams_hook_few.html>

Harley, D., and Lee, A. (2007). “Phish Phodder: Is User Education Helping or Hindering?” Paper presented at 17th Virus Bulletin International Conference, Vienna, 2007. [Online: web] Viewed: 23rd June, 2010. < http://www.eset.com/resources/white-papers/Phish_Phodder.pdf>

Peel, M. (2006). “Nigeria-related financial crime and its links with Britain”, A Chatham House Report, November, 2006. [Online: web] Viewed: 17th June, 2010. http://www.chathamhouse.org.uk/pdf/research/africa/Nigeria1106.pdf.

Hearst, M., et al. (2006). “Why Phishing Works”, [Online: web] Viewed: 19th June, 2010. < http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf>

Wiles, G. (2008). “White Hat Hackers in Demand”, Technology News – Computer Security, Posted: July 2008, USATODAY. [online: web] viewed: 24th June, 2010. http://www.usatoday.com/tech/news/computersecurity/hacking/2008-01-07-good-hackers_N.htm

IBM, Developer Works. (2010). “Security for Web-based mail: A case study (Types of hackers sidebar)”, Technical Library. [Online: web] Viewed: 21st June, 2010. http://www.ibm.com/developerworks/lotus/library/ls-mail_security_case_study/side1.html

Linden, E.V. (2007). “Focus on terrorism”, Vol. 9, NY: Nova Science Publishers, Inc.

Moore, T. (2007). “Phishing and the economies of e-crime”, Info Security, September, 2007. [Online: web] viewed: 22nd June, 2010. http://people.seas.harvard.edu/~tmoore/infosec-phishing.pdf

Abad, C. (2006). “The Economy of Phishing: A survey of the operations of the phishing market”, Cloudmark, Inc. [Online: web] Viewed 25th June, 2010. http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf

Symantec. (2009). “Symantec Global Internet Security Threat Report – Trends for 2009”. Volume XV, Published April 2010. [Online: web] Viewed: 24th June, 2010. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

Krebs, B. (2009). “Payment Processor Breach may Be Largest Ever”, Security Fix, The Washington Post. Published: Jan 2009. [Online: web] viewed: 19th June, 2010. http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html

Microsoft. (2010). "How to recognize phishing e-mails or links", Microsoft Online Safety. Microsoft, 2010. [Online: web]viewed: 24th June, 2010. < http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx>

Rao, H.R., et al. (2007). "Managing Information Assurance in Financial Services", Hershey, New York: IGI Publishing (an imprint of IGI Global).

Lin, M. (2005). "An Overview of Session Hijacking at the Network and Application Levels", SANS Institute – INFOSEC Reading Room. [Online: web] viewed: 23rd June, 2010. < http://www.sans.org/reading_room/whitepapers/ecommerce/overview-session-hijacking-network-application-levels_1565>

Rogers, B. (2005). "Dealing with Hosts File Poisoning". [online: web] viewed: 22nd June, 2010. < http://www.2000trainers.com/windows-xp/hosts-file-poisoning/>

Kerner, S.M. (2005). "DNS-Based Phishing Attacks on The Rise", All Security Trends – eSecurity Planet. [Online: web] viewed: 23rd June, 2010. < http://www.esecurityplanet.com/trends/article.php/3488216/DNS-Based-Phishing-Attacks-on-The-Rise.htm>

McAfee. (2006). "Phishing and Pharming: Understanding Phishing and Pharming", White Paper – January 2006. [Online: web]Viewed: 24th June, 2010. < http://www.mcafee.com/us/local_content/white_papers/wp_phishing_pharming.pdf>

Frost and Sullivan. (2009). "Key Challenges in fighting Phishing and Pharming". A Frost and Sullivan White Paper. [Online: web]viewed: 23rd June, 2010. < http://www.easysol.net/newweb/images/stories/downloads/Frost_Sullivan-Phishing_wp_dec09.pdf>

Ollmann, G. (2004). "The Phishing Guide – Understanding and Preventing Phishing Attacks", The Phishing Guide, NGS Software Insight Security Research. [Online: web] Viewed: 22nd June, 2010. < http://www.ngssoftware.com/papers/nisr-wp-phishing.pdf>

Drake, C.E., et al. (2004). "Anatomy of a Phishing Email", White Paper – Mail Frontier Inc. [Online: web]Viewed: 24th June, 2010. http://www.mailfrontier.com/docs/MF_Phish_Anatomy.pdf

Leyden, J. (2004). "Fear of Phishing Hits E-Commerce" *The Register*. Published: 5th May, 2004.[Online: web]viewed: 12th June, 2010. http://www.theregister.co.uk/2004/05/05/phishing_fears_survey

Kirby, C. (2004). "New Scam Threat at eBay: Hackers Obtained Information on Some Customers." SFGate.com.[Online:web] viewed: 15th June, 2010. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/03/16/BUG5T5LCM31.DTL&type=business

Munro, J. (2004). "Security Watch Letter: Adware, Phishing Plague IE Users" *PC Magazine*. Published:14th June, 2004. [Online: web]Viewed: 21st June 2010. http://www.pcmag.com/article2/0,1759,1612119,00.asp

Miller, M. (2008). “Is It Safe?: Protecting Your Computer, Your Business, and Yourself Online”, Indianapolis, Indiana: QUE Pubishing.

Trend Micro. (2006). “Phishing: Botnet, Threats and Solutions – Best Practices Series”, A Trend Micro White Paper. [Online: web]Viewed: 12th June, 2010. http://www.antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf

Kanellis, P. (2006). “Digital Crime and Forensic Science in Cyberspace”, Hershey, PA: Idea Group Publishing.

Biggam. J,(2008) Succeeding with you Master's Dissertation: A Step-by-Step Handbook: A Step-by-step Guide, open university press

Maxwell, J.(1996). Qualitative research design: An interactive approach.Thousand Oaks, CA. Sage.

Bernard, H.R. (1995). Research Methods in Anthropology, Second Edition. London, Sage Publication.

Bidgoli, H. (2004) The Internet Encyclopedia, Volume one. Canada, Wiley Publication,

Lakshman, M. (2000). “Quantitative Vs Qualitative Research Methods” Indian Journal of Pediatrics, springerlink Ltd. [Online: web] Viewed: 19th July 2010.< http://www.springerlink.com/content/t618471656140755/fulltext.pdf>

Batanov, D.N. (2008). “Research Methodology Frederick institute of technolog” [Online: web] Viewed: 15th July2010. <http://staff.fit.ac.cy/com.bd/Research%20Methodology-FUC.pdf>

GEORGE,(2001) “Data Collection Techniques, Colorado State Universit”, . [Online: web] Viewed: 17th July 2010. <http://www.cas.appstate.edu/~kms/classes/psy3100/Documents/DataCollection.pdf>

Insite,(2007).”Tips on Qualitative and Quantitative Data Collection Methods” . [Online: web] Viewed: 17th July 2010. <http://www.insites.org/CLIP_v1_site/downloads/PDFs/TipsQualQuanMthds.4B.8-07.pdf>

Appendix:

Appendix:

Online Users Survey:

THE UNIVERSITY OF WARWICK

Phishing Survey

Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal customer□s personal identity data and financial details.
Phishing is the act of sending false emails, or spam, written to appear as if they have been sent by banks or other trusted organisation in an attempt to fool the user into disclosing sensitive information such as username and password, account details etc

Online Individual

Q1 On average, how often each month do you use an online shopping or banking web site?
- *1 - 10* ○
- *11 - 25* ○
- *26 - 50* ○
- *>51* ○

Q2 Have you heard of online phishing? (Phishing is an online attempt to acquire sensitive and/or personal information about an individual for illegal purposes)
- *Yes* ○
- *No* ○

Q3 How many times in the last year have you received phishing email?
- *1 - 10* ○
- *11 - 25* ○
- *26 - 50* ○
- *>51* ○

Q4 Have you ever been fallen victim to a phishing email?
- *Yes* ○
- *No* ○

Q5 How much did you lose?

- *£100 - £1000*
- *£1001 -£10000*
- *£10001 - £10000*
- *>£100000*
- *Prefer not to say*

Q6 Which of the following actions should you take if you have responded to phishing e-mail?

- *Report it to police*
- *Change your passwords*
- *Contact your bank account immediately*
- *Report it to the online trader involved (bank, credit card company etc)*
- *All of the above*

Q7 After falling victim to phishing have you continued shopping online

- *Yes*
- *No*
- *N/A*

Q8 Are you satisfied with the action taken by the business/bank against the phishing if you responded to it?

- *Yes*
- *No*

Q8a If not, why not

Q9 What precautions do you think businesses should take in order to prevent phishing related incidents?

- *Anti-phishing department*
- *Better encryption of personal data*
- *Developing a more secure website*

Q9a What other precautions do you think businesses should take in order to prevent phishing related incidents?

Q10 Does your bank provide free software to help prevent phishing?

- Yes
- No
- Don't Know

Q10a If yes, have you downloaded anti-phishing software from your bank website?

- Yes
- No

Q10b If not, why not?

Q11 Do you think it is safe to fill personal information into pop-up windows?

- Yes
- No

Q12 Do you know whether a web site offers security to protect your confidential data?

- Yes
- No

Q12a If yes, which of the following are you aware of?

- A closed padlock on the bottom right of your browser window
- Your friends or colleagues in work have warned you about phishing
- Via an online search engine
- The security certificate for the website matches the name of the website
- The web address is prefixed with https in its address label
- Other

Q13

Nationwide proud to be different

Dear Customer,

Nationwide's Internet Banking, is here by announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service,against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below.

http://www.nationwide.co.uk/update_asp?ID=3b89db2a6001ec93328d21e59a011b0a 25a

http://www.drinkrezepte.de/shakes/index.html

Regards
Rafiq Miah
Customer Advisor
Nationwide Direct

Nationwide Building Society

Could you read the email above and answer this question: Do you think this e-mail is?

- *Phishing*
- *Legitimate*
- *No Answer*

Q14a Could you clarify your answer above?

Q15 HSBC Security Update - Alert

Dear Valued Customer,
A scheduled security maintenance has just been completed on the HSBC Internet Banking system. In order to ensure your account with us has not been affected by this maintenance, you will be required to complete our Security Update. Kindly click on the "Login to HSBC" link stated below to proceed:
Login to HSBC
Failure to complete the security update will lead to account suspension. We apologize for any inconveniences caused as your security is our major priority.
Security Department,
HSBC Bank plc.

I have receive email form HSBC bank and they asked me to complete security update. Do you think this e-mail is

- *Phishing?*
- *Legitimate?*
- *No Answer*

Q15a Could you clarify your answer above?

Thank you for taking the time to complete this survey. If you are willing for me to contact you directly for further information regarding phishing attacks please supply a contact name and telephone number.

Q17 Name

Q18 Position

Q19 Contact number

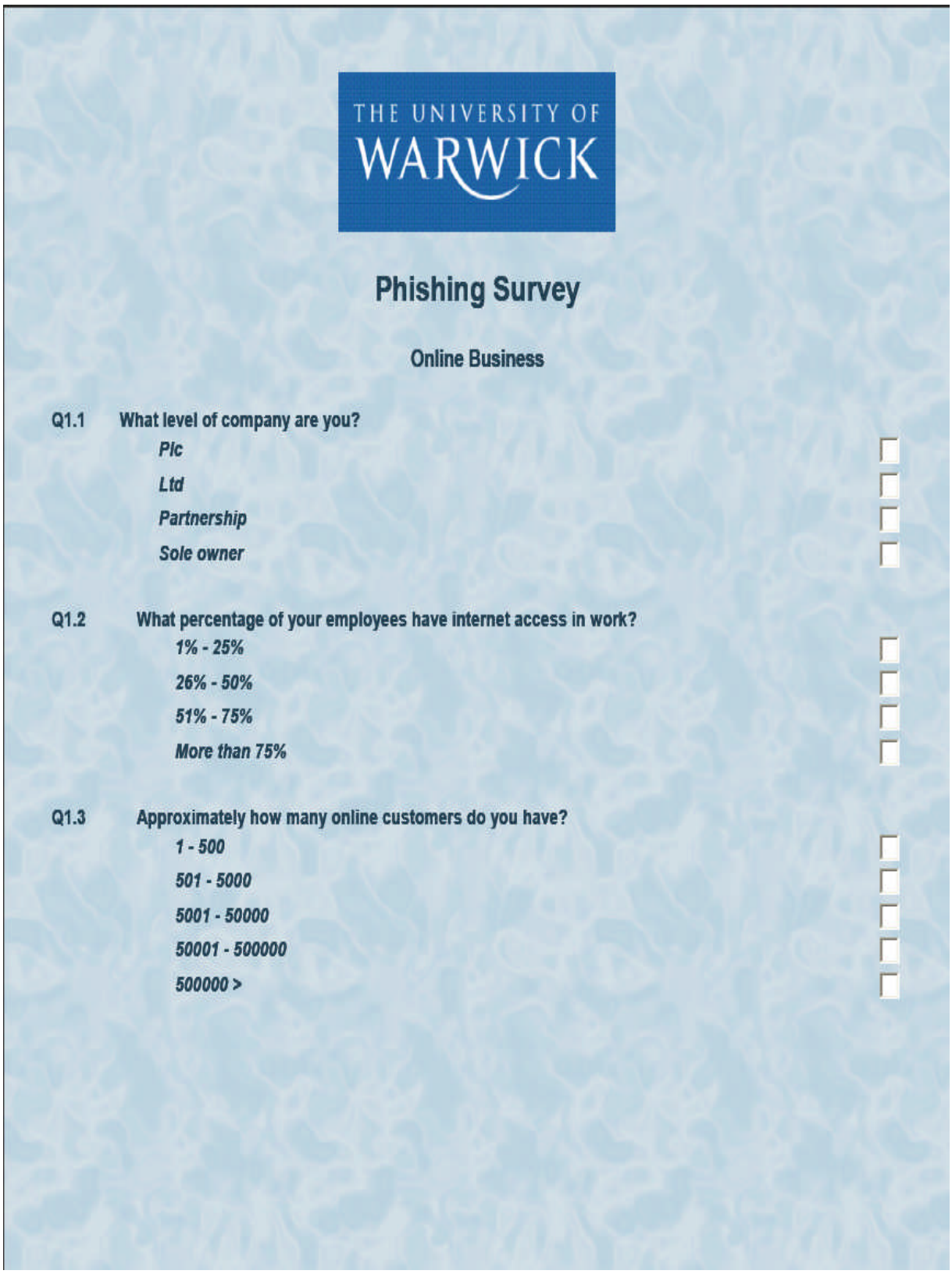
Q20 E-mail Address

All answers given in this survey will be treated with the utmost confidentiality and only the overall results may be made public with no release whatsoever of any personal or business details.

Thank you.

Powered by snap Reset Submit

Online Businesses Survey:



THE UNIVERSITY OF WARWICK

Phishing Survey

Online Business

Q1.1 What level of company are you?

- *Plc* ☐
- *Ltd* ☐
- *Partnership* ☐
- *Sole owner* ☐

Q1.2 What percentage of your employees have internet access in work?

- *1% - 25%* ☐
- *26% - 50%* ☐
- *51% - 75%* ☐
- *More than 75%* ☐

Q1.3 Approximately how many online customers do you have?

- *1 - 500* ☐
- *501 - 5000* ☐
- *5001 - 50000* ☐
- *50001 - 500000* ☐
- *500000 >* ☐

Q1.4 Do you offer your customers guidance to be more aware of phishing? If so, say briefly, what guidance you offer

Q1.5 Has your business ever fallen victim to a phishing attack?

- *Yes*
- *No*

Q1.6 If yes, how many times?

- *1 - 50*
- *51 - 100*
- *101 - 500*
- *500 >*

Q1.7 How did your business resolve the phishing attack incident?

Q1.8 What is your estimated business loss owing to Phishing?

- *£100 - £1000*
- *£1001 -£10000*
- *£10001 - £100000*
- *£100001 - £1000000*
- *£1000001>*
- *Prefer not to say*

Q1.9 Do you keep records on the type of phishing attacks on your company?

- *Yes*
- *No*

Q1.10 If so, what type of attacks are they? For example - EBay, banking, lottery, credit cards.

Q1.11 What actions should you take if you have been a victim by phishing?

- *Report it to police*
- *Change your passwords*
- *Contact your bank account immediately*
- *Report it to your dealer*
- *All of the above*

Q1.12 Have any of your customers reported a phishing attack to you?

- *Yes*
- *NO*

Q1.13 If yes, how many?

- *1 - 10* ☐
- *11 - 50* ☐
- *51 - 100* ☐
- *101 - 500* ☐
- *>501* ☐
- *Prefer not to say* ☐

Q1.14 What is the estimated loss to customers owing to phishing?

- *£100 - £1000* ☐
- *£1001 -£10000* ☐
- *£10001 - £100000* ☐
- *£100001 - £100000* ☐
- *£100000 >* ☐
- *Prefer not to say* ☐

Q1.15 Do you believe that you have lost online business customers owing to phishing?

- *Yes* ○
- *NO* ○

Q1.16 If yes, please say why

Q1.17 Do you keep records on the type of phishing attacks on your customers that have been reported to you? If so, what type of attacks are they? For example - EBay, banking, lottery, credit cards.

Q1.18 Are you aware of any national or international initiatives to reduce phishing? If so are you part of them?

- *Yes*
- *NO*

Q1.19 If so are you part of them?

Q1.20 Do you see the occurrences of phishing increasing or decreasing in the next 12 months?

- *Increasing*
- *Decreasing*

Q1.21 Have you been involved in a successful prosecution of a third party for phishing?

- *Yes*
- *No*

Q1.22 Have you been involved in a unsuccessful prosecution of a third party for phishing?

- *yes*
- *No*

Q1.23 Do you have an automated system to detect or prevent phishing activities of your customers' accounts?

Yes ○

No ○

Thank you for taking the time to complete this survey. If you are willing for me to contact you directly for further information regarding phishing attacks please supply a contact name and telephone number.

Name:

Position

Contact Number

All answers given in this survey will be treated with the utmost confidentiality and only the overall results may be made public with no release whatsoever of any personal or business details.

Thank you.

Online Businesses E-mails List:

1. "phishing@santander.co.uk "
2. "suspiciousemails@alliance-leicester.co.uk"
3. "alert@aib.ie"
4. "security@hbosplc.com"
5. "internetsecurity@barclays.co.uk "
6. "emailscams@lloydstsb.co.uk"
7. "spoof@egg.com"
8. "24hours@firstdirect.com"
9. " 24hours@mail.firstdirect.com"
10. "littleblackbook@mail.firstdirect.com"
11. "newsletter@mail.firstdirect.com "
12. "security@hbosplc.com "
13. "onlinesecurity@if.com"
14. "DPO@moneysupermarket.com "
15. "phishing@natwest.com."
16. "nationwide@nationwidebuildingsociety-email.co.uk"
17. "phishing@rbs.co.uk."
18. "support@trusteer.com"
19. "ive_seen_a_scam@smile.co.uk"
20. "privacy@abebooks.co.uk"
21. "stop-spoofing@amazon.com"
22. "bbcshop@bbc.co.uk"
23. "mail.ox@blackwell.co.uk"
24. "bob.online@blackwell.co.uk"
25. "privacypolicy@bca.co.uk."
26. "departmentdma@bca.co.uk"
27. "customerservices@foyles.co.uk "
28. "orders@foyles.co.uk"
29. "website.service@hmv.co.uk"
30. "digitalservice@hmv.co.uk"
31. "pureservice@hmv.co.uk"
153. "sa-info@ironport.com"
154. "kr-info@ironport.com"
155. "tw-info@ironport.com"
156. "sa-info@ironport.com"
157. "africa-info@ironport.com"
158. "de-info@ironport.com"
159. "benelux-info@ironport.com"
160. "nordic-info@ironport.com"
161. "ee-info@ironport.com"
162. "nordic-info@ironport.com"
163. "fr-info@ironport.com"
164. "de-info@ironport.com"
165. "ireland-info@ironport.com"
166. "it-info@ironport.com"
167. "benelux-info@ironport.com"
168. "privacy@webex.com"
169. "privacy@demon.net "
170. "dpa@demon.net "
171. "customerservice@demon.net "
172. "media.enquiries@thus.net"
173. "mail.eddie@thus.net"
174. "mail.mike@thus.net"
175. "mail.simon@thus.net"
176. "mail.dan@thus.net"
177. "mail.stewart@thus.net"
178. "information@thus.net"
179. "customerservicea@asterisk.com"
180. "privacy@symantec.com"
181. "Tracy_Ross@mcafee.com"
182. "Joris_Evers@mcafee.com"
183. "Francie_Coulter@mcafee.com"
184. "Kim_Eichorn@mcafee.com"
185. "Sal_Viveros@mcafee.com"
186. "Erica_Coleman@mcafee.com"
187. "Ally_Zwahlen@mcafee.com"
320. "info@bmoinvestorline.com"
321. "contact@bmonb.com"
322. "online.fraud@bmo.com"
323. "inquiries@dundeewealth.com"
324. "quality@laurentianbank.ca"
325. "ombudsman@obsi.ca"
326. "ombudsman@laurentianbank.ca"
327. "info@the-cma.org"
328. "inside.sales@equifax.com"
329. "commercial.solutions@equifax.com"
330. "tdsource@td.com"
331. "awardentries@the-cma.org"
332. "awardtickets@the-cma.org"
333. "events@the-cma.org"
334. "info@the-cma.org"
335. "regulatory@the-cma.org"
336. "join@the-cma.org"
337. "lookforthelogo@the-cma.org"
338. "contactcouncils@the-cma.org"
339. "careers.help@the-cma.org"
340. "mediacontact@the-cma.org"
341. "login@the-cma.org"
342. "investorrelations@sabb.com"
343. "sabb@sabb.com"
344. "CustomerCare@samba.com"
345. "info@alinma.com"
346. "contactus@alahli.com"
347. "complaints@alahli.com"
348. "aliqtisad.alislami@dib.ae"
349. "salhajailan@emiratesbank.com.sa"
350. Hanir@emiratesbank.com.sa
351. "SaudG@emiratesbank.com.sa"
352. "Aliaza@emiratesbank.com.sa"
353. "ebirtreasury@emiratesbank.com.sa"
354. "info@eisksa.com"

32. "dataman@hmb.co.uk."
33. "customer.relations@hmb.co.uk"
34. "info@pickabook.co.uk"
35. "care@pickabook.co.uk"
36. "privacy@play.com"
37. "enquiries@affiliatefuture.co.uk "
38. "care@thehut.com"
39. "customer.relations@whsmith.co.uk"
40. "customer.relations@whsmith.co.uk"
41. "whsmith-ebooks@overdrive.com"
42. "whs@mapmarketing.com"
43. "info@penwizard.co.uk"
44. "customer.services@ccagroup.co.uk"
45. "info@whs-newsrecreated.co.uk"
46. "help@moonpig.com"
47. "info@penwizard.co.uk"
48. "themagazinegroup@dovetailservices.com"
49. "info@aqu3.com"
50. "info@historic-newspapers.co.uk"
51. "whsphoto@cewecolour.co.uk"
52. "onlinestore@gbposters.com"
53. "dataprotection@next.co.uk"
54. "newsletter@kelkoo.co.uk"
55. "legal@kelkoo.co.uk"
56. "qeries@shopdirect.com"
57. "equests@allposters.com"
58. "3P@figleaves.com"
59. "ceo@figleaves.com"
60. "robin@walktall.co.uk"
61. "enquiries@affiliatefuture.co.uk"
62. sales@shore.co.uk
63. "simon@shore.co.uk"
188. "cvar@mxlogic.com"
189. "Catherine_helzerman@mcafee.com"
190. "Richard_Cohn@mcafee.com"
191. "info@approvedindex.co.uk"
192. "personalinfo@approvedindex.co.uk"
193. "feedback@approvedindex.co.uk"
194. "sales@eibs.co.uk"
195. "admin@eibs.co.uk"
196. "support@eibs.co.uk"
197. "support@commitcrm.com"
198. "sales@commitcrm.com"
199. "info@commitcrm.com"
200. "info@impirius.co.uk"
201. "info@nixonwilliams.com"
202. "sales@books2taxes.com"
203. "kevin@books2taxes.com"
204. "sales@1300bpo.com"
205. "inquiries@variman.com"
206. "sales@primestyle.com"
207. "customersupport@cashmygold.co.uk"
208. "queries@shopdirect.com"
209. "sales@diamond-heaven.co.uk"
210. "info@tamba.co.uk"
211. "queries@vertbaudet.co.uk"
212. "Eve.Lacey@ideasnetwork.co.uk"
213. "website.service@hmv.co.uk"
214. "digital download - digitalservice@hmv.co.uk "
215. "pureservice@hmv.co.uk"
216. "sales.national@newlifecleaning.com"
217. "enq@pinnaclecleaning.co.uk"
218. "info@energistuk.co.uk"
219. "support@mySupermarket.co.uk"
220. "enquiries@mySupermarket.co.uk"
221. "affiliates@mySupermarket.co.uk"
222. "manufacturers@mySupermarket.co.uk"
355. "IBHRS@emiratesislamicbank.ae"
356. "info@eifb.ae"
357. "enquiries@emiratesmoney.ae"
358. "merchants@network.ae"
359. "NIBDU@network.ae"
360. "merchant@network.ae"
361. "HeadOffice.GOD@bankofindia.co.in"
362. "barodaconnect@bankofbaroda.com"
363. "nakuru@abcthebank.com"
364. "librahouse@abcthebank.com "
365. "eldoret@abcthebank.com "
366. "meru@abcthebank.com "
367. "industrial.area@abcthebank.com"
368. "headoffice@abcthebank.com"
369. "westlands@abcthebank.com"
370. "koinange@abcthebank.com"
371. "mombasa@abcthebank.com"
372. "COSMonitor@aol.com"
373. "advertising.aol.co.uk"
374. "advertising.aol.co.uk"
375. ukdisupport@aviva.co.uk
376. "info@hm.com"
377. "customersupport@theAA.com"
378. "contactus@skype.net"
379. "ukdisupport@aviva.co.uk "
380. "helpdesk@aviva.co.uk "
381. "sponsorship@aviva.co.uk"
382. "askhr@aviva.co.uk"
383. "hrpay@aviva.co.uk"
384. hrref@aviva.co.uk
385. "webmaster@axa.co.uk"
386. "internetsecurity@barclays.co.uk"
387. "consulthelp@bupa.com"
388. "customerservices@belmontthornton.co.uk"
389. "info@claimsregulation.gov.uk"
390. "press.office@debenhams.com"

64. "help@gocompare.com"
65. "feedback@gocompare.com"
66. "ibis@co-operativebank.co.uk. "
67. "feedback@swiftcover.com"
68. "marketing@comparethemarket.com"
69. "commercial@comparethemarket.com"
70. "feedback@comparethemarket.com"
71. "ukdisupport@aviva.co.uk"
72. "helpdesk@aviva.co.uk"
73. "askhr@aviva.co.uk"
74. "enquiry@castlecover.co.uk"
75. "dpo@castlecover.co.uk"
76. "subs.enquiries@saga.co.uk"
77. "enquiries@landg.com"
78. "customercare@rowlandspharmacy.co.uk"
79. "will@brianmaclaurin.com"
80. "pharmacist@chemistdirect.co.uk"
81. "superintendent@chemistdirect.co.uk"
82. "marketing@chemistdirect.co.uk "
83. "director@chemistdirect.co.uk"
84. "sales@chemistdirect.co.uk"
85. "customer-services@lloydspharmacy.co.uk "
86. "webappquestions@rbsworldpay.com"
87. "delivery@royalmail.com"
88. "datasales@royalmail.com"
89. "parcelforce@parcelforce.co.uk"
90. "webcollections@parcelforce.co.uk."
91. "info@parcel2ship.co.uk."
92. "webmaster@ups.com"
93. "support@sage.com"
94. "customer.care@sage.com."
223. "advertising@mySupermarket.co.uk"
224. "press@mySupermarket.co.uk"
225. "customerservice@mothercare.com"
226. "privacy@cafepress.com"
227. "info@perfectsmilethailand.com"
228. "info@medontic.com"
229. "sale@anle.cn"
230. "service@medontic.com"
231. "sales@medontic.com"
232. "info@mtidental.com"
233. "interact@port.ac.uk info.centre@port.ac.uk"
234. "hktdc@hktdc.org"
235. "tdc.databank@tdc.org.hk"
236. "esupport@tso.co.uk"
237. "lisa.price@tso.co.uk"
238. "queries@happyprice.co.uk "
239. "susie@jgmdesign.com"
240. "info@ker-chingmedia.com"
241. "islam@sunion.warwick.ac.uk"
242. "Nurafiah.Muhammad@warwick.ac.uk"
243. "compforservices@googlemail.com"
244. "syscon@accessbankplc.com"
245. "VirtualBanking&EFT@accessbankplc.com"
246. "cardservices@accessbankplc.com"
247. "contactcenter@accessbankplc.com"
248. "contactcenter@accessbankplc.com"
249. "PHBLink@bankphb.com"
250. "mncg@ecobank.com"
251. "wamz.tb@ecobank.com"
252. "nigeria.tb@ecobank.com"
253. "uemoa.tb@ecobank.com"
254. "ceeac.tb@ecobank.com"
255. "esa.tb@ecobank.com"
256. "regionaltrade@ecobank.com"
257. "tfi@ecobank.com"
391. enquiries@gotravelinsurance.co.uk
392. "feedback@gotravelinsurance.co.uk"
393. "info@helpucover.co.uk"
394. "security@ingdirect.co.uk"
395. "investments@landg.com"
396. "enquiries@landg.com "
397. "direct.investments@landg.com"
398. "graham.baldock@landg.com
399. "mattmorris@lifesearch.co.uk
400. "enquiries@nationalfriendly.co.uk"
401. "compliance@nationalfriendly.co.uk"
402. "complaint.info@financial-ombudsman.org.uk "
403. "motor.insurance@saga.co.uk"
404. "customerservice@primaryinsurance.co.uk"
405. "provisionalmarmalade@3xd.co.uk"
406. "onlineinvestigations@sainsburysbank.co.uk"
407. "contactus@pentax.co.uk"
408. "ukonlinemarketing@samsung.com"
409. "privacy@eu.sony.com"
410. "info@toshiba.co.uk"
411. "nocontact@travelodge.co.uk"
412. "customer.services@travelodge.co.uk"
413. "e_opt_out@hilton.com"
414. "customer_privacy@hilton.com"
415. "privacy@marriott.com"
416. "sales.buenosaires@lhw-offices.com"
417. "london@lhw-offices.com"
418. "info@lhw.com"
419. "feedback@gocompare.com"
420. "help@gocompare.com"
421. "business-development@gocompare.com"
422. "marketing@gocompare.com"
423. "feedback@comparethemarket.com"
424. "commercial@comparethemarket.com"
425. "marketing@comparethemarket.com"

95. "newbusinessadvice@sage.com."
96. "privacy@sage.com"
97. "Jay.moore@hp.com"
98. "jos.baltes@hp.com"
99. "omegaline@dhl.com"
100. "hdn@hdnl.co.uk
101. "phishing@visa.com"
102. " customersupport@visa.com "
103. "enquiries.europe@visa.com"
104. "cpo@ftc.gov"
105. "spam@uce.gov"
106. "webmaster@fedex.com"
107. "solutions@fedexscs.emea.fedex.com"
108. "abuse@fedex.com"
109. "privacy-officer@adobe.com"
110. "comments@dominos.co.uk"
111. "richardwperkins@perfectpizza.co.uk"
112. "paulyoungman@perfectpizza.co.uk"
113. "website@perfectpizza.co.uk"
114. "feedback@pizzaexpress.com"
115. "amurdoch@pizzamarzano.com"
116. "pmusto@verisign.com"
117. "ir@verisign.com supplychain@verisign.com"
118. "enterprise_security@verisign.com"
119. "phishing@oucs.ox.ac.uk"
120. "security@slc.co.uk"
121. "webmaster@ucs.cam.ac.uk"
122. "cert@cam.ac.uk"
123. "webmaster@securityfocus.com"
124. "editor@securityfocus.com"
125. "spam@warwick.ac.uk"
126. "webteam@contacts.bham.ac.uk"
258. "tfi@ecobank.com"
259. "capitalmarkets@ecobank.com
260. "capitalmarkets@ecobank.com"
261. "investmentbanking@ecobank.com"
262. "firstcontact@firstbanknigeria.com"
263. "complaints@gtbank.com"
264. "corpaff@gtbank.com "
265. "enquiries@gtbank.com"
266. "customercare@oceanicbank.com"
267. "ebusiness@oceanicbank.com"
268. "isupport@oceanicbank.com"
269. "info@afribank.com"
270. "ebusiness@zenithbank.com"
271. "enquiry@zenithbank.com"
272. "customerservice@zenithbank.com"
273. "cardservices@zenithbank.com"
274. "info@zenithinsurancecoy.com"
275. "CIC@ubagroup.com"
276. "abuse@unionbank.com"
277. "webmaster@standardbank.co.za"
278. "InvestorRelations@cwbank.com"
279. "MediaEnquiries@cwbank.com"
280. "comments@cwbank.com"
281. "tracey.ball@cwbank.com"
282. "rmanning@shawbiz.ca"
283. "info@phonebusters.com"
284. "security@citizensbank.ca"
285. "remarque@bmo.com"
286. "bmomastercard@bmo.com"
287. "feedback@bmo.com"
288. "mutualfunds@bmo.com"
289. "advice@banksafeonline.org.uk"
290. "weddingplan@tpsltd.com"
291. "info@virginmoney.com"
292. "complaint.info@financial-ombudsman.org.uk"
426. "travel@support.expedia.co.uk"
427. "ecommerce@coop.co.uk"
428. "webcustomerservices@co-operative.coop.co.uk"
429. "pretravelservices@firstchoice.co.uk"
430. "aftertravel@firstchoice.co.uk"
431. "hhype.customerservices@holidayhypermarket.co.uk"
432. "info@wavex.co.uk"
433. "support@wavex.co.uk"
434. "helpdesk@flightcore.net"
435. "info@tribeca-it.com"
436. "sales@clearstreamtechnology.co.uk"
437. "support@clearstreamtechnology.co.uk"
438. "provisioning@clearstreamtechnology.co.uk"
439. "finance@clearstreamtechnology.co.uk"
440. "resourcing@clearstreamtechnology.co.uk"
441. "research@clearstreamtechnology.co.uk"
442. "development@clearstreamtechnology.co.uk"
443. "enquiries@rmaltd.co.uk"
444. "privacy@cisco.com"
445. "web.queries@computershare.com"
446. "sales@linksys.com"
447. "security@linksys.com"
448. "publicrelations@linksys.com"
449. "privacy@Linksys.com"
450. "uk-info@ironport.com"
451. "info@ironport.com"
452. "nordic-info@ironport.com
453. "ru-info@ironport.com"
454. "sp-info@ironport.com"
455. "nordic-info@ironport.com"
456. "sw-info@ironport.com"
457. "la-info@ironport.com
458. "anz-info@ironport.com"
459. "ch-info@ironport.com"

127. "info@itwales.com"	293. "customerservices@simplyhealth.co.uk"	460. "ch-info@ironport.com"
128. "iatcommercial@swansea.ac.uk"	294. "international@overstock.com"	461. "in-info@ironport.com"
129. "in2events@swansea.ac.uk"	295. "enquiries@harpersphoto.co.uk "	462. "sa-info@ironport.com"
130. "B.M.Guess@swansea.ac.uk"	296. "sales@richardfrankfurt.co.uk"	463. jp-info@ironport.com
131. "ecdladmin@swansea.ac.uk"	297. "leasing@bhphoto.com"	464. "sa-info@ironport.com"
132. "insrvConnect@cf.ac.uk"	298. "requests@allposters.com"	465. "ch-info@ironport.com"
133. "helpline@ncl.ac.uk"	299. "customercare@net-a-porter.com"	466. "anz-info@ironport.com"
134. "webmaster@sonicwall.com"	300. "fashionadvisor@net-a-porter.com"	467. "businessexpress@flybe.com"
135. "irt@gla.ac.uk"	301. "feedback@net-a-porter.com"	468. "pressoffice@flybe.com"
136. "webeditor@it.gla.ac.uk"	302. "press@net-a-porter.com"	469. "customeraccounts@flybe.com"
137. "webmaster@st-andrews.ac.uk"	303. "designers@net-a-porter.com"	470. "phishing@email.ba.com"
138. "dataprot@st-andrews.ac.uk"	304. "editors@net-a-porter.com"	471. "msnmoney@live.co.uk"
139. "student-it-helpline@nottingham.ac.uk"	305. "katew@asos.com "	472. "msnhomepage@live.co.uk"
140. "security@nottingham.ac.uk"	306. "marketing@asos.com"	473. "msnshopping@live.co.uk"
141. "web-team@nottingham.ac.uk"	307. kate@katesclothing.com	474. "dataremoval@comet.co.uk"
142. "its-help@reading.ac.uk"	308. "info@citygoddess.co.uk"	475. "privacy@Currys.co.uk"
143. "webmaster@reading.ac.uk"	309. "sales@glittermonster.co.uk"	476. "privacy@dell.com"
144. "enquiries@opodo.com"	310. "UrbanEuropeCS@urbanout.com"	477. "rivacy@play.com"
145. "pressenquires@cheapflights.co.uk"	311. "andrea.merloni@indesit.com"	478. "play@hillandknowlton.com"
146. "corporate-pr@cheapflights.com"	312. "corporate.affairs@indesit.com"	479. "operations@v12finance.com"
147. "easyjet@mailnj.custhelp.com"	313. "sales@humaxdirect.co.uk	480. "privacy@jvc.co.uk"
148. "press.office@easyjet.com"	314. "uksupport@humax-digital.co.uk"	481. "mydetails@jvc.co.uk"
149. "bmitravelinsurance@chartisinsurance.com"	315. "customerservices@humaxdirect.co.uk"	482. "comitato.privacy@indesit.com"
150. "businessdevelopment@flybmi.com"	316. " customer.service@topshop.com"	483. "orders@all4sourcing.com"
151. "data.protection@flybe.com"	317. "info@clothing2u.com"	484. "londonstorecustomerservices@liberty.co.uk"
152. anthony.com"	318. " sales@netclothing.net"	485. "info@citygoddess.co.uk"
	319. " isis@imrg.org"	" customerservice@john-