ISAP – AN INFORMATION SECURITY AWARENESS PORTAL

by

ANNETTE TOLNAI

Dissertation
Submitted in fulfilment of the requirements for the degree

MAGISTER SCIENTIAE

in

INFORMATION TECHNOLOGY

in the

FACULTY OF SCIENCE

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF S.H. VON SOLMS

OCTOBER 2008
ACKNOWLEDGEMENTS

A special thank you to Prof von Solms for all his patience, input and hard work. Your ongoing support throughout the year will never be forgotten.

Thank you to G. Buncombe for proof reading this manuscript.
ABSTRACT

The exponential growth of the Internet contributes to risks and threats which materialize without our knowledge. The more computer and Internet use becomes a part of our daily lives, the more we expose ourselves and our personal information on the World Wide Web and hence, the more opportunities arise for fraudsters to get hold of this information.

Internet use can be associated with Internet banking, online shopping, online transactions, Internet Relay Chat, newsgroups, search engines, online blogs and e-mail. The source behind online activities carried on over the Internet may be different from what we are led to believe. Communication lines may be intercepted, compromising sensitive information of the user. It is a risk to make digital payments and reveal sensitive information about ourselves to an unknown source. If the risk materializes, it may result in undesired circumstances.

Using the Internet securely should be a prerequisite to every user before conducting online transactions and activities over the World Wide Web. Owing to the versatility and ease of the electronic medium, electronic databases and vast amounts of sensitive information are readily accumulated. This is cause for concern regarding the main issues, namely privacy, identity theft and monetary fraud. Major countermeasures to mitigate the main forms of security and Internet-related issues are awareness of these risks and how they may materialize as well as relevant protection mechanisms.

A discussion about why the Internet is a popular medium for criminal behaviour, what risks are involved, what can be done about them and some technical as well as non-technical preventative measures are covered in this dissertation.

The purpose of this dissertation is to create an overall awareness of Internet banking and the process of Internet transactions. The end result is the development of an information security awareness portal (ISAP) aimed at the general public and potential Internet users who may be subject to identity and credit fraud. The aim of the ISAP is to sensitize users and minimize the growing numbers of individuals who are victimized through online crimes. Individuals using the Internet need to be aware of privacy concerns governing the Internet and how searchers are able to find out almost anything about them.

The false sense of security and anonymity we as users think we have when innocently connecting to the World Wide Web outlines threats lurking in the background where we would never imagine. By the time you are finished reading this dissertation, it may put you off transacting and revealing sensitive information about yourself online ever again.
Why a Dissertation on Internet Banking Awareness?

Based on the number of victims caught in a web of mistrust owing to online crimes, Internet banking has become one of the main targets of crime. Clearly, there is a need for a portal or manual to guide the average user on a need-to-know basis about using the Internet securely.
Motivation for Writing Style

The writing style presented in this dissertation will use personal pronouns to denote oneself and another or others. Use of this notation in the direct sense implicitly and particularly denotes the conditions directly to the user, namely oneself, another or others. The use of direct language allows for ease of reading, indicating that the context and effects of online fraud and identity theft apply directly to all of us - no exception. The masculine pronoun will also be deemed to include the feminine gender where applicable.

Motivation for the Use of Cartoon Strips and Cartoon Characters

People normally draw their own conclusions when it comes to understanding risk and security awareness. This is based mainly on the view of telling people what to do and what not to do, what should and should not be done, as well as giving warnings about threats. The security gap appears where users are not given good reasons why they should change certain behaviours. A security gap also appears because there is a lack of explanation as to what happens if security measures are not followed and these reasons are not described.

The consequences of online fraud result from the security decisions users make based on limited knowledge of risk, such as whether to install a series of programs or to click on a link to fill in sensitive data such as passwords. Education material should be based on actual user behaviour and understanding this behaviour. This will minimize the result of degraded security awareness.

Because the dissertation is focused mainly on user awareness, cartoon strips are used because these have proven to be the most effective method as an awareness strategy for users to understand the seriousness of cybercrime. Since these cartoon strips are successful in this education process, they too will feature in the ISAP.

“About what our readers say:

We are grateful for the overwhelmingly positive feedback we are receiving from people who think we are addressing an important problem in a meaningful way. We hear from individuals, from representatives of educational institutions, governments, financial institutions, and companies of various sizes. People write to praise, make requests for new material, and ask how they can use our material. Some write with requests to translate our cartoons, others ask us to help them redesign their client education.” [Srikwan, S. Jakobsson, M. 2007]

For more information visit http://www.securitycartoon.com - Using Cartoons to Teach Internet Security - by Sukamol Srikwan and Markus Jakobsson for a more detailed analysis.
The words used in this document such as perpetrator, scammer, violator, offender, predator, intruder, fraudster, thief, hacker, attacker and con artist all have the same meaning to identify a typical criminal within different contexts.
CONTENTS

Part I
Dissertation Outline ............................................................................................................. 1

Chapter 1
Introduction and Background ............................................................................................ 2

1.0. Overview .................................................................................................................. 2
1.1. Introduction ............................................................................................................. 3
1.2. Problem Statement ................................................................................................. 3
1.3. Objectives .............................................................................................................. 4
1.4. Deliverables ........................................................................................................... 5
    1.4.1. Dissertation ................................................................................................. 5
    1.4.2. Information Security Awareness Portal (ISAP) ...................................... 6
1.5. Research and Approach ......................................................................................... 7
    1.5.1. Literature ..................................................................................................... 7
    1.5.2. Development ............................................................................................... 8
    1.5.3. Proposed End Result ................................................................................... 9
1.6. Overview and Structure ....................................................................................... 10
    1.6.1. Overview .................................................................................................... 10
    1.6.2. Structure .................................................................................................... 10
1.7. Roadmap Overview ............................................................................................. 13
    1.7.1. Atom ......................................................................................................... 13
    1.7.2. Roadmap Functionality ........................................................................... 14
1.8. Awareness Citation Overview .............................................................................. 14
1.9. Summary ............................................................................................................... 15

Part II
Prologue to the Internet and Internet Transactions ..................................................... 16

Chapter 2
Computers and the Internet ............................................................................................ 19

2.0. Overview .............................................................................................................. 19
2.1. Internet Pre-history .............................................................................................. 20
2.2. How the Internet Works ...................................................................................... 22
    2.2.1. Connecting to Cyberspace ....................................................................... 23
    2.2.2. Hardware, Software and Firmware ......................................................... 23
    2.2.3. The Internet Router ................................................................................. 24
    2.2.4. Internet Protocol (IP) Address ................................................................. 24
    2.2.5. Domain Name System (DNS) Servers ..................................................... 25
    2.2.6. The WWW and Internet Web Browsers .................................................. 26
    2.2.7. Duplication in the World Wide Web....................................................... 38
2.3 Summary .............................................................................................................. 38
Chapter 3

Internet Transactions ................................................................................................................. 31

3.0. Overview............................................................................................................................. 31
3.1. Introduction to Internet Transactions – Our Data Trail ........................................................... 32
  3.1.1. Our Data Trail .................................................................................................................. 32
  3.1.2. Buying Online .................................................................................................................. 32
  3.1.3. Process of a Typical E-commerce Transaction ................................................................. 32
  3.1.4. Processing the Order ....................................................................................................... 33
  3.1.5. Us for Sale ....................................................................................................................... 33
  3.1.6. Our Data Trail Summary .................................................................................................. 46
3.2. Benefits of E-commerce ....................................................................................................... 35
  3.2.1. Benefits of E-commerce to the User ................................................................................. 46
  3.2.2. Benefits of E-commerce to the Business ........................................................................ 46
3.3. Concerns and Challenges about E-commerce ..................................................................... 36
  3.3.1. Preferences regarding Conventional Methods ................................................................. 47
  3.3.2. Trust Issues associated with Scams or Unethical Businesses ........................................ 47
3.4. Are Secure Internet Transactions Really Secured? .............................................................. 37
  3.4.1. What is a Digital Certificate? .......................................................................................... 48
  3.4.2. What are Certificates used for? ....................................................................................... 49
3.5. Other Types of Online Transactions .................................................................................... 49
  3.5.1. PayPal, Auction and Shopping ....................................................................................... 49
  3.5.2. Social Networking .......................................................................................................... 50
3.6. Summary............................................................................................................................ 39

Part III

Compromise of Sensitive Information ......................................................................................... 40

Chapter 4

Introduction to Online Fraud and Finding Personal Information ............................................... 43

4.0. Overview............................................................................................................................. 43
4.1. Privacy Issues and Personal Identifiable Information Online ................................................. 44
4.2. Effects and Results of Identity Theft ................................................................................... 44
  4.2.1. Credit Card Fraud .......................................................................................................... 56
  4.2.2. Phone or Utilities Fraud ................................................................................................ 56
  4.2.3. Bank/finance Fraud ....................................................................................................... 56
  4.2.4. Government Documents Fraud .................................................................................... 56
  4.2.5. Pretexting ..................................................................................................................... 57
  4.2.6. Other Fraud .................................................................................................................. 57
4.3. Top Hacker SecretsExposed ............................................................................................... 46
  4.3.1. The Typical Hacker ........................................................................................................ 46
  4.3.2. Industrial Espionage ....................................................................................................... 47
  4.3.3. Gaining Unlimited Access ............................................................................................ 58
  4.3.4. What do Attackers Want? ............................................................................................. 58
4.4. Summary............................................................................................................................ 59
Chapter 5

Modus Operandi (MO) Techniques for Committing Online Fraud

5.0. Overview

5.1. Category 1: Banking
5.1.1. Credit Card Fraud
5.1.2. The SIM Swap Scam
5.1.3. Payment Confirmation
5.1.4. Counterfeit Cashier's Cheque

5.2. Category 2: Solicitation
5.2.1. Phishing
5.2.2. Spoofing
5.2.3. Social Engineering
5.2.4. Social Networks

5.3. Category 3: Malicious Software
5.3.1. Spyware and Malware (Malicious Software)
5.3.2. Key Loggers
5.3.3. Wireless Attacks
5.3.4. Risk of File-sharing (P2P Networks)
5.3.5. Botnets
5.3.6. Browser Hijacking
5.3.7. Anti-spyware Scams

5.4. Category 4: Fraud Schemes
5.4.1. Advance Fee Fraud/Nigerian 419 Scams
5.4.2. Debt Elimination
5.4.3. Escrow Services Fraud
5.4.4. Investment Fraud
5.4.5. Auction Fraud

5.5. Category 5: Extortion
5.5.1. Information Brokers
5.5.2. Internet Extortion

5.6. Category 6: Illegal Activities
5.6.1. Identity Theft
5.6.2. Online Gambling
5.6.3. Conventional Fraud Modus Operandi

5.7 Summary of MO and Respective Categories

Chapter 6

Preventing MO Subterfuge

6.0. Overview

6.1. Category 1: Banking
6.1.1. Preventative Measures: Credit Card Fraud
6.1.2. Preventative Measures: The SIM Swap Scam
6.1.3. Preventative Measures: Payment Confirmation
6.1.4. Preventative Measures: Counterfeit Cashier's Cheque

6.2. Category 2: Solicitation
6.2.1. Preventative Measures: Phishing
6.2.2. Preventative Measures: Spoofing
6.2.3. Preventative Measures: Social Engineering
Part IV

General Preventative Measures ............................................................ 115

Chapter 7

Non-technical and Technical Preventative Measures ............................. 118

7.0. Overview .................................................................................... 118
7.1. Non-technical Preventative Measures .......................................... 119
   7.1.1. Passwords ........................................................................ 119
   7.1.2. Preventative Measures: Guidelines to Securing Unattended User Equipment ............................................................................... 132
7.2. Technical Preventative Measures ................................................ 121
   7.2.1. Anti-virus Software Packages ........................................... 121
   7.2.2. Anti-spyware Software Packages ....................................... 124
   7.2.3. Firewall Software Packages .............................................. 126
   7.2.4. Protect Our Identity ........................................................ 128
   7.2.5. Secure and Recommended Internet Browsers ....................... 131
   7.2.6. Secure E-mail Clients .................................................... 132
   7.2.7. Updates and Patches ....................................................... 144
   7.2.8. Encryption Mechanisms ................................................ 144
   7.2.9. Other Encryption Mechanisms and Techniques .................... 146
7.3. Summary .................................................................................. 147
Part V
ISAP Discussion and Conclusion ................................................................. 137

Chapter 8
ISAP Overview .......................................................................................... 140
8.0. Overview ......................................................................................... 140
8.1. Software Requirements to View the ISAP ........................................ 141
8.2. Overview of ISAP Functionality ...................................................... 141
   8.2.1. The 3D Carousel .......................................................................... 142
   8.2.2. The Link Bar ................................................................................ 143
   8.2.3. The Home Page Contents .......................................................... 143
   8.2.4. The ISAP Web Page Contents .................................................... 143
8.3. Technologies used to Develop the ISAP .......................................... 144
8.4. Summary ......................................................................................... 146

Chapter 9
Conclusion .................................................................................................. 147
9.0. Overview .......................................................................................... 150
9.1. Research and Development Opportunities ....................................... 151

References ................................................................................................. 152

Further Reading ......................................................................................... 161

APPENDIX

Appendix 1 ............................................................................................... 1
Appendix 2 ............................................................................................... 11
Appendix 3 ............................................................................................... 25
Appendix 4 ............................................................................................... 31
Appendix 5 ............................................................................................... 54
Appendix 6 ............................................................................................... 74

LIST OF FIGURES

FIGURE 1. Roadmap overview .................................................................. 14
FIGURE 2. Internet Pre-history time line .................................................. 21
FIGURE 3. Interconnected networks ......................................................... 22
FIGURE 4. Connecting to an ISP ............................................................... 23
FIGURE 5. Packets following a path across different routers .................... 24
FIGURE 6. Requesting a Web page ........................................................... 26
FIGURE 7. Our data trail ........................................................................... 34
FIGURE 8. Information gathered by Web sites without our knowledge or consent .......................... 129
LIST OF TABLES

TABLE 1. List of categories and their respective modi operandi ........................................... 53
TABLE 2. Preview of banking category (category 1) and its MO ............................................. 54
TABLE 3. Preview of solicitation category (category 2) ......................................................... 56
TABLE 4. Preview of malicious software category (category 3) ........................................... 62
TABLE 5. Preview of fraud schemes category (category 4) ................................................... 71
TABLE 6. Preview of extortion category (category 5) .......................................................... 74
TABLE 7. Preview of illegal activities category (category 6) .................................................. 75
TABLE 8. Summary of MO and respective categories ......................................................... 78
TABLE 9. Preventative measures: List of categories and respective MO ......................... 84
TABLE 10. Preview of banking category and its MO .......................................................... 85
TABLE 11. Preview of solicitation category (category 2) ..................................................... 89
TABLE 12. Preview of malicious software category (category 3) ....................................... 95
TABLE 13. Preview of fraud schemes category (category 4) ............................................... 101
TABLE 14. Preview of extortion category (category 5) ....................................................... 105
TABLE 15. Preview of illegal activities category (category 6) ............................................ 106
TABLE 16. Summary of categories and their MO preventative measures ..................... 112
TABLE 17. Review of reviews – results - sorted by category .......................................... 122
TABLE 18. Consensus report ............................................................................................ 123
Part I

Dissertation Outline

Chapter 1
Introduction and Background
Chapter 1
Introduction and Background

1.0. Overview

Web server hosting companies and many such organizations have established themselves to keep up to date with the latest technological trends. These organizations manage vast amounts of information, including personal records, within enormous databases. Searching through personal records has become a lot easier and more productive than when personal records existed only on paper. Computerized records are easily stored, recorded, duplicated, retrieved, compared and manipulated beyond mere convenience and are accessible to any searcher that wants to obtain information. The user needs to be aware of these developing technologies and acquire knowledge of the relevant protection mechanisms.

Education regarding security awareness has proven to be a failure in several observations. Some people argue that the relevant protection mechanisms involve technology alone and that security education, or security awareness, is hopeless. Others underestimate the normal Internet user’s perspective in making meaningful security decisions. Communicating important advice is possible, but not necessarily easy. The aspects discussed in this dissertation regarding security-related issues may also apply to your average e-commerce and auction trading Web sites.

In this chapter the introduction will provide an overview of some of the many elements that will be addressed in the dissertation, followed by the problem statement, objectives, deliverables, research and approach, overview and structure, as well as an overview of the roadmap and awareness citations.
1.1. Introduction

Information security is becoming a serious matter in terms of the possible risks the electronic medium may enforce upon us. Because the electronic medium is so volatile and diverse, the Web is easily manipulated to the intruder’s advantage.

The fabrication of official-looking documents, Web pages, e-mails and other media are all used by fraudsters. We are living in an information age where the compromise of confidential information can take place easily. Convenience and cost-effectiveness allow rapidly evolving and developing technologies, intelligent software and new forms of pervasive computing to introduce new challenges.

“A key assumption is that computer-mediated communication, such as over the Internet, will undermine trust because it eliminates face-to-face interaction” [Mansell, R. Collins, B.S. 2005: 210].

Uncertainty plays a major role when conducting confidential online transactions. We cannot see whom we are dealing with and therefore cannot take the Internet purely at face value. The reasons why the Internet cannot be trusted will be covered throughout this dissertation. The modus operandi (MO) techniques are discussed in detail in Chapter 5. Solutions and countermeasures to the risks which may materialize on the Internet are discussed in Chapters 6 and 7.

Additionally, the information security awareness portal (ISAP) will provide online instant access to anyone who would like to know more about the security issues and the risks involved when using the Internet. The most important aspects to using the Internet securely will also be provided in the portal. More detail about the ISAP is discussed in Chapter 1, 1.4.

Information security issues introducing risks have been discussed briefly. The problem statement is discussed in the next paragraph, which introduces what the principal security problem is on the Internet concerning us and our safety. This is followed by the objectives.

1.2. Problem Statement

The continuing technological development of cyberspace raises matters directly related to our privacy, safety and security. We are casually granted online access to online banking accounts without any prior knowledge of the risks involved and what consequences could arise. Similarly, online transactions such as e-commerce Web sites are also a cause for concern. Because online institutions neglect to educate the average user, we tend to become a risk to ourselves.
The question is how risk, identification and trustworthiness can be transferred into cyberspace effectively. Not knowing how the World Wide Web (WWW) operates in cyberspace causes issues which need to be clarified and addressed. It is therefore important for us to understand and perceive the underlying mechanisms of a typical Internet transaction.

Uncertainty is the main cause of risk. These risks may materialize in threats, and may affect us directly or indirectly should we fall victim to such a situation. Victims in this regard are escalating in number as more online services are accessible - and more users become susceptible to online fraud.

Although fraudulent activities are due mostly to unethical behaviour, this topic will not be discussed in this dissertation. Jurisdiction and ethical morals are not enough to direct and control misconduct in cyberspace. It is therefore important for us to take responsibility and protect our valuable assets.

Summary of Problem Statement

The foremost risks in using the Internet today, is a lack of awareness of the relevant information security risks, together with a lack of knowledge of the correct information security and preventative measure to mediate these risks.

Because the Internet is an intangible medium, it causes risks to whoever enters it, and more so to the users who are unaware of such risks. The objectives of the dissertation are discussed next, which will address user awareness and the lack thereof.

1.3. Objectives

More can be done to prevent online security risks if the average user is aware of the consequences and how the compromise of information can be avoided. It is important to create awareness around us in order to enforce protection mechanisms against online fraudulent activities. We must be able to distinguish a fraudulent Web site or e-mail from a legitimate one. We must be aware of certain procedures, such as implementing and performing routine tasks on anti-virus software, as well as technical and non-technical measures, such as protecting passwords, which can be done to avoid becoming a victim of online crimes. The overall aim of this dissertation is to contribute to the battle and prevention of online crimes in terms of literature and an information security awareness portal (ISAP).
The intended research, including the dissertation, is to create an information security awareness portal which will serve the following principles. This is not an exhaustive list.

- Provide a platform to develop and enhance current security awareness strategies of each individual.
- Provide links for further reading material.
- Provide opportunity for downloading relevant security software.
- Provide easy and instant access to security resources such as a list of definitions and existing risks.
- Provide updated information of evolving security threats (must be maintained).
- Provide the ability to communicate relevant messages to the users and to educate the user as efficiently as possible.

Secondary objectives of the dissertation include the following:

- To easily understand the risks.
- To serve educational purposes.
- To be able to apply our knowledge gained from this dissertation.
- To execute preventative measures against online fraudulent activities.
- To be able to understand what must be done and when to prevent or to mitigate risks should they materialize.
- To communicate relevant messages to the user and to educate the user as efficiently as possible.

Overall, the goal is to provide the user with knowledge on how risks and issues materialize and what to do about them. The deliverables in the next section include the dissertation and the ISAP.

1.4. Deliverables

The information provided to enhance the knowledge and awareness of the average user is contained in two formats: The dissertation and the ISAP.

1.4.1. Dissertation

The dissertation is the conventional paper version and provides some of the detailed content relevant to security in cyberspace as well as online transactions. The structure and the topics covered in this dissertation will be discussed in 1.6: Overview and Structure.
1.4.2. Information Security Awareness Portal (ISAP)

The ISAP consists of a Web site which is made publicly available online at [http://www.securityportal.co.za](http://www.securityportal.co.za). The online portal version highlights all the relevant topics necessary for us to become aware of our surroundings regarding our own safety in the WWW.

The portal is simply designed to allow us to navigate easily through the relevant topics. The topics and their contents were carefully selected to illustrate the most important concepts. Selected areas which are covered within the portal are as follows:

- **Home:** provides an overview of the problem statement and why it is important to gain an understanding of the content portrayed in the portal.

- **The Internet:** provides a short history of the Internet for the interest of the reader and an overview of how the Internet works.

- **Online transactions:** this section shows how Internet transactions work to enable us to gain a better understanding of what happens during a typical online transaction. The main question is how secure are secure online transactions.

- **Risks and modus operandi (MO):** covers what risks exist and how each of the risks materializes.

- **Countermeasures:** this section provides the general rules for information security, the technical as well as the non-technical preventative measures.

- **Downloads:** this section provides relevant links to free software downloads (and trial versions) which will aid us to enable better protection mechanisms.

The contents featuring in the ISAP are extracted from the dissertation itself, including other content such as cartoon strips.

The main parts contained in the portal will enable us to kick-start our awareness of security on the Internet. The average user is and remains a target for online criminal activities and therefore remains the main objective in the research and approach, which are discussed next.
1.5. Research and Approach

Each individual must be able to enforce protective and preventative measures to ensure safety and security before being exposed to the potential and unknown threats of the online world. The research approach targets mainly user awareness, given that the materialization of risks and criminal activities on the Internet is due mostly to lack of user awareness.

Lack of awareness on the Internet must be addressed, by shedding light on the topic and promoting awareness of the risks lurking in cyberspace as well as relevant preventative measures for each risk. The communication of relevant security measures is important as the exposure of sensitive information, willingly or not, remains our own responsibility.

The ISAP therefore plays a vital part in communicating the security risks and preventative measures to the user and to ensure the maximum benefit and exposure of valuable information to reach a vast majority of people. The research approach is therefore divided into two main parts: literature and development.

1.5.1. Literature

The literature overall is composed of a dissertation, which will serve as the complete, offline and detailed extensive awareness manual.

1.5.1.1. Literature Study

The literature study involves research based on the consequences arising from lack of awareness. Awareness elements also filter into organizations, compromising sensitive data vital to the lifeline of the business, such as personal records. The results of lack of awareness are analyzed and a detailed explanation is given of how predators operate, what risks exist, why they exist as well as how or when risks can materialize (this is discussed in detail in Chapter 5). Alerting users to the risks of compromised sensitive and credential information as well as their relevant preventative measures will feature by means of detailed explanations throughout the literature.
1.5.1.2. Creation of Dissertation

The dissertation is divided into a total of six parts with a total of nine chapters. Certain chapters focus on the types of risks which can materialize in the WWW, while others are dedicated to how materialization of these risks can be avoided, prevented and mitigated.

The contents of the dissertation feature directly in the ISAP. Most of the factors discussed in the dissertation, including the appendices, will accordingly be restructured in the online version.

The dissertation also provides an explanation of the ISAP, how it is set up and how it works (see Chapter 1, 1.6. for a more detailed analysis).

1.5.2. Development

The development will involve the creation of the ISAP designed to educate and alert the user to online risks.

1.5.2.1. Creation of ISAP

Traditional resources, such as print volumes, have the innate inability to keep up to date with the evolution of new technologies as links to sites change and disappear. The challenge is to keep abreast of technologies, and to provide an updated resource for staying secure on the WWW. Keeping the relevant information up to date through a dynamic resource will be made possible through the ISAP, which can be updated accordingly.

The ISAP will provide us with the efficient knowledge to protect this information in the future. It will provide each individual with the summary and most important parts of this dissertation and the relevant defence mechanisms needed in order to prevent and minimize risks from materializing. The portal will be accessible on the Web by those who were or are victims and by those who want to expand their awareness. The purpose will be to serve the public, and guide the individual in the correct procedures of what should be done and how it should be done - should a user become a victim of criminal fraud. However, guidance on what should be done and how is not enough. Therefore, cartoon strips will feature as a resource to portray why a certain procedure is important (see Notes to the Reader for a detailed explanation).
Downloads will also be made available relating to the security risks as preventative measures. Parts of this literature will be accessible in the portal for easy use and understandability to the general public.

### 1.5.2.2. Visual and Informative Aspects that must feature in the ISAP

- The look and feel of the portal must be simple, yet impressive.
- The design must allow users to easily navigate and understand the Web site.
- Links and their contents must be easy to understand and navigate.
- The medium in which ISAP is developed must be compatible with most, if not all, operating systems and platforms.
- The portal must therefore be easily understood by a large audience and community of people, from the average person in the street to the highly educated business person.
- Additionally, the ISAP must be able to provide some value to each person reading the contents of the portal from the most basic level to a more detailed level.
- Key links to be included:
  - Home
  - The Internet
  - Online transactions
  - Risks and MO
  - Countermeasures
  - Downloads

The structure of the portal must be able to address a wide audience. Two different levels will be integrated within the ISAP to allow for simplicity as well as further and more detailed reading:

- **Level 1:** The background to different aspects covered in this dissertation will be enclosed in the portal on this level.
- **Level 2:** More details of each aspect can be accessed through hyperlinks and will be covered with regard to its respective appendix.

### 1.5.3. Proposed End Result

The formatting of the different levels both in the ISAP and the literature is designed to address a wide audience. From the most basic level (Level 1) to the more detailed level (Level 2), everybody will be able to obtain some value from it.
In addition to raising awareness and the current prospects discussed in this part, such as the challenges arising from evolving technologies, the literature and portal may serve as a base and/or guideline to any future developments and research that may take place.

In this part, Research and Approach, the literature and development prospects have been discussed where the dissertation features as the written version, while the portal features as the online, more accessible, version. The Overview and Structure of the dissertation provides a more comprehensive analysis of what is contained within the literature study.

1.6. Overview and Structure

The structure explains the different parts of the dissertation and its relevant chapters. An overview of the topics featured in the literature is given next.

1.6.1. Overview

The basic structure of the dissertation begins with an introduction to the history of computers and the Internet.

The history is followed by an introduction to how the Internet operates, and then Internet transactions and their security are analyzed. The types of risks and threats are presented, followed by how these risks can materialize and their various solutions, techniques and countermeasures to mitigate each of the risks.

The dissertation ends with a conclusion, describing the aspects of the document that were discussed and the further research opportunities in the field.

1.6.2. Structure

This dissertation is organised into five main parts. A brief introduction to each chapter within each part is included in this subdivision:

1.6.2.1. Part I: Dissertation Outline

The advent of computerized records has created virtual access to electronic documents containing sensitive and personal information. Although technology has
introduced convenience, time-saving benefits and almost instant calculations, it has also brought with it a number of security risks.

In Part I, Chapter 1, Dissertation Outline, an introduction and background provided to the problem are given. Part I also provides an objective and overview pertaining to the direction to where we are heading in this study.

1.6.2.2. Part II: Prologue to the Internet and Internet Transactions

The development of the Internet would not have been possible without the advent of computers. Data in the electronic medium is not tangible, which causes privacy issues and compromise of data. This data is vital in today's Information Age, as information forms the basis of survival in the global economy. This is why it is important to understand how the Internet and cyberspace work, and how information is transmitted through cyberspace.

In Part II, Chapter 2, a history of how the Internet developed is presented as background.

Chapter 3, Internet Transactions and the Internet, discusses how the Internet and Internet transactions work. This part of the dissertation will answer the burning question of the security levels behind secure online transactions.

1.6.2.3. Part III: Compromise of Sensitive Information

There is normally a good motive for the determined criminal to get to our personal information and banking details. Compromising privacy and identity theft can materialize in more than one way – and sometimes using blended threats, which is a combination of more than one methodology or attack method. Obtaining personal information is as good as gold for a potential thief. A variety of methods may be used by skilled identity thieves to get hold of our information, and our credential subterfuge may materialize from a variety of modus operandi. Modus operandi (MO) involves the use of various Internet crime schemes used by perpetrators as a method for operating to achieve their motive. By using the various MO, victims risk losing their identity, resulting in financial and credibility loss.
In Part III, Chapter 4, Introduction to Online Fraud and Finding Personal Information, an introduction to identity theft, hacker secrets and finding personal information about people is provided.

Chapter 5, Modus Operandi (MO) Techniques for Committing Online Fraud, introduces various techniques that can be utilized by fraudsters. This chapter also illustrates how we expose ourselves to cyberspace and its potential risks. The various crime schemes and MO are introduced, one by one, in Chapter 5.

Chapter 6, Preventing MO Subterfuge: In this chapter, the corresponding precautions and preventative measures to each MO introduced in Chapter 5 will be further discussed in Chapter 6, following the same approach.

1.6.2.4. Part IV: General Preventative Measures

Chapter 7, entitled Non-technical and Technical Preventative Measures, is dedicated to general and technical security measures to ensure secure transactions and online Internet banking.

The most common and important security mechanisms are discussed in this chapter, where multiple security mechanisms and programs can be used for added protection to provide a barrier between our important information and the intruder.

1.6.2.5. Part V: ISAP Discussion and Conclusion

An overview of the development of the ISAP, including a conclusion to the dissertation, will be provided in the final part.

Part V, Chapter 8, ISAP Overview, presents the downloads, various aspects discussed in this dissertation, and easy-to-access links to the corresponding Web sites.

Chapter 9, Conclusion, depicts the outline of what has been discussed. After reading and gaining explicit information from the dissertation, we will have a good basic understanding of the risks involved. This part will also discuss any future prospects for future research opportunities.
1.6.2.6. Appendices

The appendices serve as an addendum to the content in this dissertation. More details will be provided in the appendices on each relevant chapter and topic, which will be indicated accordingly within the content. The purpose of this structure is to provide a background to and deeper understanding of the relevant topics in the dissertation itself. The more technical details are available in the appendix indicated to those who wish to read further.

Appendices 1-6 provide the relevant details corresponding to each part presented in the dissertation.

1.6.2.7. References

This part gives an overview and list of the references and information sources used to compile the dissertation. Sources referred to in the appendices are also listed in the references provided in the main dissertation.

The relevant parts and the chapters featuring within each part have been discussed briefly with a brief introduction. However, to keep the reader in context, a roadmap had been included within the reading material, and this element is discussed next.

1.7. Roadmap Overview

The roadmap is a graphical representation of the contents presented in the dissertation. The illustration features just after each heading displayed on a single page introducing each chapter.

1.7.1. Atom

The roadmap is a gigantic atom with circular rings. Smaller particles orbit around the main particle, which is depicted as the world. The illustration of the world portrays that Internet security awareness is a global issue that can affect users from all parts of the world – no exceptions. The orbiting circular rings and smaller particles show that there is no escape from Internet security issues, and that each part outlined around this particular atom is interrelated.
1.7.2. Roadmap Functionality

Each time a particular chapter is introduced, the roadmap features as part of the introduction. This concept is designed to be a placeholder within the context of the dissertation.

The particles circulating the world are coloured in red, while the world encloses a red reflection. The colour red was chosen to depict alertness related to the Internet security awareness issues. Furthermore, the part number and chapter number corresponding to each chapter will be highlighted in red (see Figure 1).

An explanation of the roadmap and its functionality was provided in this section. Because the dissertation and ISAP are dedicated to user awareness, another concept related to creating an impact follows in the next section.
1.8. **Awareness Citation Overview**

The awareness citations feature on the page following the roadmap introduction. The purpose of the awareness citation is to send a security message to the reader and user. The differently sized letters and emphasis placed on the important words add impact to the seriousness of the Internet security issue at hand.

1.9. **Summary**

In this chapter an overview of the features that will be presented throughout the dissertation, such as the awareness citation and roadmap, were presented. An overview of the dissertation, such as the overview and structure, research and approach, deliverables, objectives and problem statement, was given.

Records which once only existed on paper are now easily accessed electronically and are easily stored, recorded, duplicated, retrieved, compared and manipulated beyond mere convenience. This causes security risks to valuable information that can be misused, creating the need for user awareness in this regard. To prevent the compromise of sensitive information, the communication of important advice is necessary, but not necessarily easy.

The next few chapters will introduce some aspects of the Internet to provide background and prepare us to better understand how security risks on the Internet materialize and how to prevent them. The next part and chapters focus on the Internet pre-history in Chapter 2 and how Internet transactions work in Chapter 3.
Part II

Prologue to the Internet and Internet Transactions

Chapter 2
Computers and the Internet
Security incidents are getting worse.

"YOU CAN’T PREDICT when AND where THINGS WILL HAPPEN, SO YOU’LL HAVE TO UNDERSTAND THE how.”

John Chambers
Chairman and CEO Cisco Systems
Chapter 2
Computers and the Internet

2.0. Overview

A simple name and address opens the doorway to personal information such as a user’s profession, how much tax he pays, what car he drives, the names and ages of his children and spouse, the demographics of his neighbourhood as well as the value of his house. From the above information an estimated guess of an income can be concluded. All this information can be known about anyone just by sitting behind a keyboard [Lane, C.A. 2002: 3].

Protecting our privacy is becoming an increasingly important issue in cyberspace. Little privacy remains and is dissipating at a rapid rate [Lane, C.A. 2002: 3].

To later understand how it is all possible, it is first important to understand how the Internet and cyberspace work, and how information is transmitted through cyberspace. Data in the electronic medium cannot be seen tangibly and therefore cannot be distinguished clearly.

The invention of computers contributed greatly to the electronic medium and the development of the Internet. Before I explain how the Internet works, a small but brief history of the development of the computer and the Internet is provided as background.
2.1. Internet Pre-history

The Internet itself was created based on computers and telecommunications models. For the purposes of this dissertation, the history discussed will be based on computers as opposed to the telecommunications market. However, a full background regarding the Internet pre-history is not necessarily vital to understanding the underlying mechanisms of the risks of the Internet and Internet banking. Nevertheless, a brief Internet history is provided in a timeline format, listed in chronological order beginning from some 5 000 years ago through to 1994 (see Figure 2). The events are listed in chronological order by date, and more information is provided in Appendix 1 on each date and its corresponding event.

The next section introduces how the Internet works, how it contributed to globalization and why regulation of the Internet is a constant challenge.
Figure 2. Internet pre-history time line. By A. Tolnai.
2.2. How the Internet Works [Tyson, J. 1998-2008] [English online. 1998]

The name of the Internet comes from the idea of interconnected networks (see Figure 3). A network is more than one computer connected together either by telephone cable, wireless technology or by other means to enable all the computers to communicate with one another. Hence, the Internet comprises a global collection of networks both big and small. The Internet has grown immensely to tens of millions from just four host computer systems since 1969.

When a piece of data such as a Web page or e-mail is transferred over the Internet [English online. 1998]:

1. **The data is broken up into packets**, which may consist of many same-sized pieces.

2. A **header is added to each packet**, which informs potential destinations of where it came from, where it should be positioned in relation to other receiving packets and its destination.

3. The **packet travels through routers (see 2.2.3.), from computer to computer** until it reaches its destination. The packets may take different routes, depending on the accessibility of the deciding computer along the route.

4. All the **packets are examined at the destination computer**. A message may be sent back to the sending computer asking to resend any missing or damaged packets, until all packets are received in their correct form.

5. Once each packet is received without error, the **packets are reassembled** into their original form.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is responsible for sending, receiving and checking packets flawlessly between each computer positioned within the Internet. To allow computers to communicate with one another, the connecting computer first needs to establish a connection to a larger framework of underlying connectivity.
2.2.1. Connecting to Cyberspace [Tyson, J. 1998-2008]

The computer uses a modem or router to establish a connection to the Internet. Our computer then becomes a part of the Internet service provider’s (ISP) network (see Figure 4):

1. The signals transmitted from the computer to the ISP are converted to travel over the telephone line or dedicated subscriber line.
2. The ISP has a point of presence (POP) in each region to allow local users to connect to it. The ISP may connect to a larger network and become a part of that larger network.
3. There are several high-level networks connecting to one another through network access points (NAPs).
4. Various regions are connected through dedicated backbones, which are owned by most large communications companies.

There is no controlling body with authority over all the networks. The basic underlying structure of the Internet is based on computers and those computers are further connected to other networks. To make it all possible, the process is driven through hardware, software and firmware capabilities.

2.2.2. Hardware, Software and Firmware
Hardware consists of mechanical devices and electronic components that make up a computer system, such as a keyboard. Software enables us to use this hardware through the use of programs, such as a word editor. Firmware is similar to software, only it is stored permanently within the hardware component. The router is defined below.

2.2.3. The Internet Router [Tyson, J. 1998-2008]

A router is a piece of hardware that uses firmware in order to direct data traffic on a network and allows for communication between various networks and computers using different protocols. A protocol is used to enable different types of computers to communicate flawlessly.

![Packets following a path across different routers](image)

The router’s basic function is to ensure that the information we send from our computer reaches its correct destination. Information may be sent across many different routers across the globe to reach another computer on the other side of the world. The information that we send from our computer is placed inside packets. These packets can be broken up into smaller segments if the information being sent is too large. The packets are then reconstructed at the receiving end based on the information contained within the packets (see Figure 5).

For example, a typical packet would contain the type of protocol used, packet numbers, the data which we are sending, and the data to show the end of the packet as well as the sender’s and receiver’s IP addresses.

2.2.4. Internet Protocol (IP) Address [Tyson, J. 1998-2008]
An IP address is a unique identifying number for each computer connecting to a network. A typical IP address is depicted in decimal form, as a dotted decimal number such as 168.78.12.110. The IP is used as a language which allows computers to communicate on the Internet.

In the early days of the Internet, an IP address would be used to find the Web page a user wanted to retrieve. This became unmanageable when the Internet grew from just a few host systems. The Network Information Center (NIC) managed a simple text file to map domain names to IP addresses but this became too large to manage. This changed in 1983, when the University of Wisconsin created the Domain Name System.

### 2.2.5. Domain Name System (DNS) Servers [Brain, M. 1998-2008]

DNS servers are used to convert human-readable domain names into the machine level IP addresses. DNS servers perform two functions [Brain, M. 1998-2008]:

1. Accepting requests from programs to convert a domain name into an IP address.
2. Accepting requests from other name servers to convert a domain name into an IP address.

A DNS server will ultimately do one of four things with the request it receives from a machine [Brain, M. 1998-2008]:

1. If the DNS server already knows the IP address to the requested domain, it can respond adequately to that request.
2. The DNS server may contact other name servers to complete the request for a specific domain and find the corresponding IP address. The DNS server may contact multiple other name servers.
3. The DNS server may refer the client computer to the IP address for another name server that may know more, and may find the request for the specified domain.
4. If the requested domain is invalid or does not exist, the DNS server may return an error message.

When a universal resource locator (URL) is typed in a browser to request a Web page, that request is sent to another computer and the desired Web page is displayed in the requesting browser.

A server is a computer receiving a request from the client computer. The computer which is requesting a service is called a client. The request is processed by the server and sends the result back to the client computer. Therefore, the server computer provides a service to the client computer.
The Internet is composed of servers and clients and would not be possible without them. A server’s IP address does not change very often. On the other hand, the ISP may or may not assign a new IP address every time a local user connects to the Internet, making it unique to the current session.

The server locates the files and downloads them to the client computer via the WWW and displays the contents in a Web browser (see Figure 6).

![Figure 6. Requesting a Web page](image)

2.2.6. The WWW and Internet Web Browsers [Joshi, C.V. 2005]

The World Wide Web was developed by Tim Berners-Lee and was designed to make navigation of the Internet easier (see Appendix 1 (1.18.) of the Internet pre-history).

The World Wide Web (also known as W3, WWW or simply the Web) is a system of Internet servers that support specially formatted documents.

A concept called hypermedia or hypertext appears in the Internet browser (now also adopted in Windows help files) as underlined text and allows virtual retrieval of one Web page after another. Once the requested Web page has been retrieved, the connection to the responding server is broken, saving on overhead costs while we read the document.

A Web browser assembles the content on the screen through the use of an Internet Web browser such as Internet Explorer, Mozilla Firefox or Safari, amongst others (Web browser security is discussed in more detail in Chapter 7). Most documents are formatted using Hyper Text Markup Language, more commonly known as HTML. HTML consists of a variety of elements such as graphics, audio, tables, text, colours and other media.
The World Wide Web Consortium (W3C) is an organization which maintains the standards that enable us to use the WWW. More information on W3C can be found at http://www.w3.org/

2.2.7. Duplication in the World Wide Web

Computers and the Internet world work through duplication. Every time a Web page is retrieved, a copy of that Web page and all its contents are loaded onto the requesting computer. The original copy is kept on the server for other client computers to view.

Most security risks originate from this concept of flawless duplication. A precise and exact duplicate may be created from the information that is created, stored, retrieved and transferred without our knowledge.

2.3. Summary

A brief history of the invention of computers and the Internet was given, as well as a brief introduction to how the Internet works. A typical Internet transaction is dependent on the operations of computers and the Internet, and many types of Internet and e-commerce Web sites have developed from this concept. The benefits, concerns and challenges of e-commerce are discussed in the next chapter.
Part II

Prologue to the Internet and Internet Transactions

Chapter 3
Internet Transactions
Part I
Dissertation Outline
Chapter 1: Introduction and Background

Part II
Chapter 2: Computers and the Internet Transactions
Prologue to the Internet and Internet Transactions

Part III
Chapter 4: Introduction to Online Fraud and Finding Personal Information
Chapter 5: Modus Operandi (MO) Techniques for Committing Online Fraud
Chapter 6: Preventing MO Subterfuge

Part IV
Chapter 7: Non-Technical and Technical Preventative Measures

Part V
ISAP Discussion and Conclusion
Chapter 8: ISAP Overview
Chapter 9: Conclusion

INTERNET SECURITY AWARENESS
... Hackers are bent on taking over servers, extracting information and using it to their benefit.

As e-commerce continues to grow, the more aware we should all be of the dangers it brings to our finances.

—Claidissa Holm Helium
Chapter 3
Internet Transactions

3.0. Overview

Owing to the development of Internet transactions, writing out cheques, swiping credit cards and handling paper money are now turning into a thing of the past. Convenience is challenged by the risks of compromising sensitive personal information, which may occur during any Internet transaction that leaves a personal data trail in and around the Internet. The data left after every transaction gets snooped up by predators.

The compromise of sensitive and personal information may lead to identity theft, an onslaught of spam and even monetary fraud. A brief introduction to this concept illustrates the process of how sensitive personal information may be compromised. The aspects of a secure transaction not only by the merchant but by us, too, may mitigate the risks of compromising personal data. Although the growth of e-commerce and Internet transactions has been an unhurried one, e-commerce continues to develop. The reasons and reluctance to employ e-commerce are discussed in the sections on benefits, challenges and concerns of e-commerce.
3.1. Introduction to Internet Transactions – Our Data Trail

When our personal data goes online, just about everyone wants a piece of us. This is illustrated in Figure 7, which illustrates how we go up for sale.

3.1.1. Our Data Trail

Figure 7 illustrates how we compromise sensitive and personal information about ourselves when we complete a typical Internet transaction. Marketers, data aggregators and credit report agencies all want to use our information for personal gain, including online thieves. The diagram presents how identity theft and monetary fraud occur simply by purchasing online. The data trail begins in the centre of the diagram illustrating us (the user) connecting to our ISP and surrendering our information to merchants’ servers. Each step is numbered in chronological order from 1 to 8. Each entity additionally includes an explanation describing what is happening between each data trail.

3.1.2. Buying Online [Krebs, B. 2006]

We are responsible for the first step of completing a secure online transaction. This means that we must ensure that our computer is free from spyware and viruses, we do not respond to phishing attacks and that the Web site we are purchasing from is a secure site (more on ensuring that the site is secure in 3.4. Also see non-technical and technical preventative measures to ensure secure transactions in Chapter 7).

1. Merchant’s secure server: our ISP connects our computer – and personal data - to online stores’ servers (see Figure 7) where our shipping address, purchase and account details are gathered by the online server.


When we find an item we want to buy, the item is added to a list called a shopping cart or shopping basket. The process is as follows:
• We add all the items we want to purchase to a virtual shopping basket. In some cases, we may wish to add our chosen items to a wish list, which may be purchased at a later stage if we so desire.

• When we are finished adding items to the shopping basket, a checkout button is clicked where all the items are totalled with VAT and shipping costs.

• We (the customer) are required to fill in an online form with our personal information such as name, contact numbers, address and credit card information (the three types of electronic payments are discussed in Appendix 2 (1.1.)). Credit card information is encrypted using Secure Sockets Layer (SSL) technology (more information on SSL is provided in Appendix 2 (2.6.)) and sent to the merchant. Our personal information is stored on the merchant’s Web server.

• A confirmation message is displayed in the Web browser and a confirmation statement along with a confirmation message is sent to our e-mail address.

The problem with this process is that no network is able to guarantee security, meaning that no network is hack proof.

3.1.4. Processing the Order [Krebs, B. 2006]

Once the merchant servers have our billing information, the purchase process is almost the same as completing a purchase order with a credit card in a normal store (see Figure 7).

2. Merchant account provider (MAP): the credit card is processed by a MAP. The largest online stores are able to run their own MAP internally.

3. Credit card processors: credit card processing companies acquire the account information and purchase cost from the MAP, where the transaction is run through a fraud prevention system.

4. Credit issuing bank: the amount of credit available is checked by the credit card’s issuing bank and if the total cost is under the credit limit, approval is sent back up the stream.

5. Merchant’s bank: the merchant’s bank is credited electronically.

3.1.5. Us for Sale [Krebs, B. 2006]

6. Marketers, data aggregators, credit report agencies: Our data is collected by data-mining firms, marketing firms and credit-reporting bureaus as much as possible (see Figure 7).
7. **Selling of information to and from marketers, data aggregators, credit report agencies:**
   Online stores sell our data to marketing firms.

8. **You’ve got mail:**
   Our mailbox is then packed with junk mail. This means that information security is only as good as the laziest database employee.

**FIGURE 7.** Our data trail
[adapted from Krebs, B. 2006]
3.1.6. Our Data Trail Summary

As illustrated in Figure 7, our ISP plays a vital role in connecting us to the Internet. Without it, we cannot complete our transactions. How our sensitive information is filtered through the Internet to marketers, data aggregators, credit report agencies and even online thieves was discussed. However, there are also benefits to using e-commerce.


The key purpose of e-commerce is convenience. Many e-commerce sites provide facilities where we can browse and search through online catalogues for specific items. The convenience of e-commerce may come with certain benefits. These benefits can be for the user as well as the business.

3.2.1. Benefits of E-commerce to the User

- Usually we only need to enter our personal information once.
- When we want to purchase again we log in with our username and password.
- Registering personal information with the merchant means we only have to confirm our purchase.
- Completing the transaction in the future is as easy as clicking our mouse.
- The purchase is conveniently delivered to our physical address either by post or to our computer, depending on the type of purchase made.
- If we purchased software or an e-book, it may be bought and immediately downloaded onto the computer.
- Additionally, we can gain access to the online shop at any time we wish.

3.2.2. Benefits of E-commerce to the Business

- We as customers are more likely to return to an e-commerce site where our information is preserved, and do not have to re-enter all our personal data again.
- The more payments processed electronically, the less is spent on paper and postage and hence, the lower the business overhead costs.
Chapter 3 – Internet Transactions

- A typical business’s customers may access their online shop at any time around the clock and place their orders.
- The business is able to increase revenues by being able to accept and process more orders at no extra cost.
- For a company to own their own online shop means global exposure. More people from all over the world can purchase from them if they so wish.

On the other hand, the global exposure of online businesses and e-commerce comes with greater risks and responsibilities, which is cause for concern about the use and developments of e-commerce.


The delayed growth of e-commerce transactions on the Internet is mainly due to privacy issues, the possibility of identity theft and the subsequent identity crime. Privacy and identity theft concerns are presented in Chapter 4. Preference relating to familiarity with conventional methods and trust issues associated with scams or unethical businesses may be the main cause hindering the developments of e-commerce.

3.3.1. Preferences regarding Conventional Methods

- Privacy concerns aside, some of us prefer the conventional methods of handling paper money and writing out paper cheques.
- The idea of transacting online may be a task too tedious, time-consuming and risky.
- Usernames and passwords may be difficult to remember and easily compromised.

Besides the daunting task online payments may create for us and the questions asked about trust and uncertainty issues, e-commerce will continue to gain in popularity.

3.3.2. Trust Issues associated with Scams or Unethical Businesses

- Finding a trusted e-commerce company to do business with can prove to be a challenging task.
• Some e-commerce companies are scams out to steal our money, while others act as information brokers to sell our personal information.

This is why companies and merchants strive to have a strong online presence and to build a good reputation. One way to maintain a strong online presence is through securing online transactions.


Trust and uncertainty issues presented by the WWW also present high risks when revealing sensitive information to merchants during the completion of an online transaction. E-commerce is not necessarily secure. It is the merchant’s responsibility to ensure that sensitive customer information is handled securely. Some companies may choose to take some shortcuts in order to save on extra costs securing connections. From a user point of view, this is why it is important to look for the correct clues before continuing with any online Internet transaction. An explanation of certificates is discussed as an example of a security measure we may take to ensure that the third party we are dealing with is secure.


A digital certificate is a certificate in electronic form which contains a name, a serial number, expiration dates, the digital signature of the certificate-issuing authority and a copy of the certificate holder’s public key to be able to verify that a certificate is valid. (Public keys are used for encrypting messages and digital signatures. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signor of a document.) Digital certificates are used to verify the credentials when doing business or other transactions on the Internet with other third parties. They are issued by a Certification Authority (CA), such as VeriSign, which authenticates that the third party’s name is the one associated with the public key in the document and digitally signs the certificate. A public key infrastructure is a collective name for the system of public keys, certificates and certificate authorities.

Authentication warnings should be issued by the browser and there are several things our browser checks to determine if the certificate is legitimate:

• Whether the domain name in the address bar matches the domain name in the certificate.
• The date on the certificate and whether it has expired.
• Whether or not the certificate has been signed by a trusted CA.
• Whether or not the signing authority certificate is valid.

3.4.2. What are Certificates used for?

Authentication ensures that the Web site we are visiting is legitimate. Without authentication, any scam artist may act as if he is our bank. The problem is that SSL (see Appendix 2 (2.6.)) only secures the information from our browser to the Web server and not on the Web server itself. Protection of sensitive information may be lacking on the Web server, and on systems such as third-party Web-hosting companies. Detailed information on certificates is provided in Appendix 2 (2.1. – 2.5.) and covers the following elements:

• What an SSL certificate does not do.
• What an SSL certificate does do.
• Who do we trust?
• How to check a certificate in Mozilla Firefox Web Browser.
• How reliable is the system?

For the reader’s interest a section on how to set up secure e-commerce payments for your business is provided in Appendix 2 (section 3). The benefits of e-commerce were pointed out above and Internet transactions introduced. However, there are other types of online Internet transactions developing in other facets of electronic networking, such as Facebook, which are discussed in the next section.

3.5. Other Types of Online Transactions

Other types of online transactions not discussed in detail in this chapter are mentioned briefly in the next section.

3.5.1. PayPal, Auction and Shopping

PayPal can be used to make donations, pay for online auctions and purchase online goods and services by transferring funds electronically. Funds can also be sent to someone’s e-mail address, from where the receiver can sign up for his own account thereafter. Other types of popular online transactions apart from PayPal may also include auction sites such as eBay and shopping sites such as Amazon.com. A
detailed discussion on PayPal and how PayPal works, its advantages and disadvantages is provided in Appendix 2 (4.1.).

### 3.5.2. Social Networking

Online networks such as Facebook have opportunities for development in the advertising and marketing segments, and are slowly becoming a self-supporting ecosystem. More information on the evolution of e-commerce using Facebook and Facebook as a new form of advertising is provided in Appendix 2 (4.2.).

### 3.6. Summary

Online transactions such as auctions on eBay and Facebook were mentioned briefly. How sensitive personal information is compromised in the hands of predators by leaving a personal data trail was discussed and an example given on how to better secure this information. Based on the discussion provided in this chapter, it can be seen that our data trail encourages predators to commit identity theft by distributing and selling our personal information. The next chapter provides an introduction to identity theft, hacker secrets and privacy issues.
Part III

Compromise of Sensitive Information

Chapter 4
Introduction to Online Fraud and Finding Personal Information
The action of gathering and manipulating personal information for CRIMINAL purposes is a disturbing trend which is growing in South Africa.

4.0. Overview

Violations of our security lead to compromising the integrity of data and our privacy. Personal information can be found about us online and in formal documents (see Appendix 3 (1.1.)). Anyone can conduct a search and successfully investigate anyone else.

Different types of fraud can be used by thieves who misuse our information to their advantage and ruin our good name, as well as our credit ratings. An overview of the effects and results of identity fraud and top hacker secrets is provided in this chapter. It is important to know who typical hackers are, as well as how hackers gain unlimited access to our valuable systems.

Personal identifiable information (PII) about us can be found online by anyone. This type of information includes information we provided on sites such as Facebook, MySpace or Flickr, and can easily be traced. PII is sensitive and personal information about ourselves, which can be used to uniquely identify us, or to locate a specific individual. This includes personal information such as our name, address, telephone numbers, credit card numbers and even an e-mail address. Even if we provided only bits of information in various locations on the Web, the information can still be compiled to form a complete profile. Although most personal information cannot (usually) be found online, data such as birth certificates, marriage and divorce information, obituaries and licences can be found online in public records. There are sites that are free, some claim to be free, but those that charge for their services are not providing us with anything that we cannot find ourselves. Paying for such a service depends on how desperate we are to find information about a particular person.

Many of us think and mistakenly believe that our PII is kept private. Privacy is becoming more limited by the day owing to data-mining organizations and the advent of social networking. If we are able to guess someone’s e-mail address, we may find a great deal about a person’s trail of online activities.

Appendix 3 (1.2. - 1.4.) provides a step-by-step process concerning:

- How anyone can find and investigate anyone online.
- More on potential search sites.
- Tips and warnings.

Understanding how complete profiles are compiled about us may help us to better protect our identity. To enable us to further protect our identity, the effects and results of identity theft are described next.

4.2. Effects and Results of Identity Theft [Federal Trade Commission. 2008a] [PLM. 2008]

When our information had been used for personal gain, we may not know that our identity has been stolen. We may only find out once reviewing bank statements or contacted by a debt collector. Financial loss is not the only form of loss. There are greater consequences to a compromised identity.
Some victims of identity theft may lose out on job opportunities, or be denied loans for housing, education or vehicles owing to the bad reputation claimed on our credit reports. In rare cases, we may be arrested for crimes we did not commit. Clearing our name can be a challenging issue once previous actions have been placed on record in black and white. In South Africa many people have found that their stolen identity documents were used fraudulently to enter into marriages. However, fraudsters are still able to make great use of stolen identities in many ways:

4.2.1. Credit Card Fraud

Perpetrators may open new credit card accounts in our name. When they use the cards and don't pay the bills, the delinquent accounts appear on our credit report. They may change the billing address on our credit card so that we no longer receive bills, and then run up charges on our account. Because our bills are now sent to a different address, it may be some time before we realize that there is a problem.

4.2.2. Phone or Utilities Fraud

Thieves may open a new phone or cell phone account in our name, or run up charges on our existing account. They may also use our name to get utility services like electricity, heating, or satellite TV.

4.2.3. Bank/finance Fraud

Fraudsters may create counterfeit cheques using our name or account number, open bank accounts in our name and write bad cheques. Our ATM or debit card may have been duplicated and electronic withdrawals are then made using our name, draining our accounts. They may also take out a loan in our name.

4.2.4. Government Documents Fraud

Criminals may get a driver's licence or official ID document or passport issued in our name but with their picture. They may use our name and identity number to get government benefits. They may file a fraudulent tax return using our information.
4.2.5.  Pretexting

Perpetrators use false pretences to obtain our personal information from financial institutions, telephone companies and other sources to get what they want.

4.2.6.  Other Fraud

Thieves may get a job using our identity number. They may rent a house or get medical services using our name. They may give our personal information to police during an arrest. If they don't show up for their court date, a warrant of arrest is issued in our name.

The effects and results of identity theft have been discussed briefly. It may be useful to provide some insight into who is behind identity theft and other online crimes.

4.3.  Top Hacker Secrets Exposed [Macleod, C. 2007]

The public often have misconceptions of what a true hacker is, or imagine a hacker to be. Generally speaking, the hacker stereotype is often portrayed as a nerd, operating from a dark room, with enough technical knowledge to create viruses that bring down networks and hack into computers to get a kick out of the challenge. This image and perception could not be more wrong. A more realistic approach to the ideal image of a hacker performing online crimes is discussed throughout this section.

4.3.1.  The Typical Hacker

According to the FBI [Macleod, C. 2007], a typical hacker is probably the “guy-next-door” – the one who works and sits in the cubicle next to us, the employee who is always punctual, pleasant, tells funny stories at lunch and is helpful. Curiosity is the main driving factor to gaining unauthorized access to password-protected and confidential files as well as workstations. Another reason could be a disgruntled employee who has been given reason for revenge. The employee will be the one to spend time on networks trying to get unauthorized access into confidential files. “According to the FBI, 70% of all security breaches are due to internal hacker attacks” [Macleod, C. 2007].

46
4.3.2. Industrial Espionage

Industrial espionage is another common reason for gaining unauthorized access to systems. Performing in-depth background checks on every temporary IT consultant is a time-consuming process, especially when this form of help is recruited when time is of the essence. The outcome is unauthorized people gaining access to sensitive data and confidential systems. When targeting a specific user or system, different methodologies may be used to gain access to password information. Even if the intent is not to target a specific individual or system, methodologies such as malicious software and social engineering (see Chapter 5) can be used to carry out certain activities.

4.3.3. Gaining Unlimited Access [Internet Guide. 2002]

Once the hacker has gained access to the system with his own system administrator privilege rights (also known as backdoor access codes), he may do anything he wishes and gain access to any workstation his heart desires. He may even act upon malicious intentions and corrupt legitimate data which is valuable to the user or organization. If this is the case, the hacker may not be prosecuted if all malicious intent was under an anonymous account – the administrator. Manually changing these backdoor access codes by the user or organization can be time-consuming and these backdoors are left open to anyone who attempts to target these systems.


Most, if not all, attackers want the same thing and pursue the same goals. These goals may vary slightly, depending on motive and intent, but mostly follow the general guidelines below:

- Attackers generally want to execute malicious programs on our computer to gain access to confidential information without our permission.
- They want to modify, alter and even corrupt sensitive information kept on our computers and maybe even reformat our hard drives.
- Attackers not only want to modify data stored on our systems, but also modify the operating system to create new security holes, leave new traps or even cause the operating system to crash.
- If any home banking and finance systems reside on our computer (such as Quicken, available from http://quicken.intuit.com/personal-finance/ and MS
Money) attackers may utilize this application to transfer money out of our accounts into another account.

4.4. Summary

The concepts of online attackers, identity theft and privacy were explained. The next chapter is dedicated to the different methodologies through which fraudsters are able to execute their plans.
Part III

Compromise of Sensitive Information

Chapter 5
Modus Operandi (MO) Techniques for Committing Online Fraud
Spam... continues to degrade the INTEGRITY OF EMAIL.

Some 55 percent of email users say they have lost trust in email because of spam.

—The Pew Internet and American life Project
Chapter 5
Modus Operandi (MO) Techniques for Committing Online Fraud

5.0. Overview

Compromising privacy and identity theft can materialize in more than one way through blended threats, which are a combination of more than one methodology or attack method. There is normally a good motive for the determined criminal to get into our personal information and banking details.

Obtaining personal information and banking details is as good as gold for a potential thief. A variety of methods may be used by skilled identity thieves to snoop up our information. The theft of our credentials, such as our name, address, telephone numbers, banking details and credit card information, may materialize from a variety of modi operandi. “Modus Operandi (MO) is a Latin term that means, ‘a method of operating.’ It refers to the behaviours that are committed by an offender for the purpose of successfully completing an offense. An offender’s modus operandi reflects how an offender committed their crimes” [Casey, E. 2004: 670]. Through various MO, victims risk losing their identity, resulting in financial and credibility loss.

The various and most common methodologies used by perpetrators to commit crimes and gain access to credential information are described in this chapter and organized into relevant categories. There are six categories in total and each MO is sorted into its applicable category (see Table 1). This chapter also contains cartoon strips to better explain certain fraud methodologies and to create a better understanding and awareness of them.
## CATeGory

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 1 BANKING | 1.1. Credit card fraud  
|          | 1.2. SIM swap scam  
|          | 1.3. Payment confirmation  
|          | 1.4. Counterfeit cashier’s cheque  |
| 2 SOLICITATION | 2.1. Phishing  
|               | 2.2. Spoofing  
|               | 2.3. Social engineering  
|               | 2.4. Social networks  |
| 3 MALICIOUS SOFTWARE | 3.1. Spyware and malware  
|                      | 3.2. Key loggers  
|                      | 3.3. Wireless attacks  
|                      | 3.4. Peer-to-peer file-sharing  
|                      | 3.5. Botnets  
|                      | 3.6. Browser hijacking  
|                      | 3.7. Anti-spyware scams  |
| 4 FRAUD SCHEMES | 4.1. Nigerian 419 scams/advance fee fraud  
|                 | 4.2. Debt elimination  
|                 | 4.3. Escrow services fraud  
|                 | 4.4. Investment fraud  
|                 | 4.5. Auction fraud  |
| 5 EXTORTION | 5.1. Information brokers  
|             | 5.2. Internet extortion  |
| 6 ILLEGAL ACTIVITIES | 6.1. Identity theft  
|                     | 6.2. Online gambling  
|                     | 6.3. Conventional fraud MO  |
5.1. Category 1: Banking

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANKING</td>
<td></td>
</tr>
<tr>
<td>1.1.</td>
<td>Credit card fraud</td>
</tr>
<tr>
<td>1.2.</td>
<td>SIM swap scam</td>
</tr>
<tr>
<td>1.3.</td>
<td>Payment confirmation</td>
</tr>
<tr>
<td>1.4.</td>
<td>Counterfeit cashier’s cheque</td>
</tr>
</tbody>
</table>

5.1.1. Credit Card Fraud [Internet Crime Complaint Center (IC3), 2008a]

Credit or debit card numbers can be stolen from unsecured Web sites or through an identity theft scheme. Fraudulently acquiring money or property through the use of an unauthorized credit card, debit card or credit card number is considered credit card fraud.

One common methodology to fraudulently acquire credit card information is skimming. Skimming is discussed in detail in Appendix 4 (1.1.).

Another common methodology to grasping a victim’s finances is commonly known as the SIM swap scam.

5.1.2. The SIM Swap Scam

“...police estimate that at least R2-million has been stolen in more than 30 cases reported so far, but the banks will not disclose details” [Independent Online, 2008].

One security measure which is designed to enhance security in online banking is the SMS authorization utility. Criminals are constantly searching for security vulnerabilities through which they can break the system. Further details on how SMS authorization and the SIM swap scam works are provided in Appendix 4 (1.2. – 1.3.).

Money can also be scammed from its owner by altering payment confirmations received from the bank after every completed online transaction.
5.1.3. Payment Confirmation

By altering a faxed or e-mailed proof of payment a thief is able to defraud us (the victim). The thief will tell us that he will be depositing money into our account. An electronic payment is then made into our account and the proof of payment is altered and faxed/sent to us by e-mail. Sometimes the thief will claim that an overpayment was made and request a reimbursement. Always check that the money is in the account.

Similarly, this methodology also applies to cheques.

5.1.4. Counterfeit Cashier’s Cheque [Internet Crime Complaint Center (IC3), 2008a]

Individuals that sell classified advertisements on the Internet are targeted by interested buyers. The buyer tells the seller that a cheque will be sent to the seller as he has an associate in the US who owes him money. The money owed is significantly higher than the price of the merchandise (by thousands of dollars), and the seller is instructed to pay back the excess to the buyer or associate in locations such as Nigeria (West Africa).

Because the cheque is a cash cheque the funds are transferred almost immediately and the seller reimburses the buyer as instructed. Shortly thereafter the seller is notified that the cheque is fraudulent and he is held responsible by the bank for the full amount of the cheque.

In some cases the victim is conned into sending the remainder of the money when the buyer cancels the order as a result of some forthcoming circumstances.

In this category, the counterfeit cashier’s cheque, payment confirmation, the SIM swap scam and credit card fraud were highlighted. The next category, solicitation, deals with means used by criminals to solicit confidential information from a user. The first common solicitation scheme discussed is phishing (refer to Table 3).

5.2. Category 2: Solicitation
5.2.1. Phishing [Beal, V. 2006]

Phishing is one of the most common forms of stealing a user’s personal identity data and financial account credentials. These types of phishing attacks can use a variety of blended threats such as social engineering and technical subterfuge. “Some of today’s phishing attacks are so convincing that they can fool even the ultra-vigilant” [Krebs, B. 2006: 29].

Phishing has reached epidemic proportions, and the FBI has called phishing the “hottest, and most troubling, new scam on the Internet” [Computer Crime Research Center. 2005]. Many users receive phishing e-mails weekly or even daily.

Phishing is the analogy derived from the word “fishing” in the sense that thieves use e-mail scams or other electronic communications to lure their prey by fishing for passwords and other financial information out of the sea of Internet users. Phishing is a criminal attempt to capture financial and personal data from users by masquerading as a trustworthy business. Con artists may send millions of these e-mail messages. Data captured is used for identity theft, credit card fraud and other crimes. Hackers have been using the term “phishing” since 1996 and luring passwords from unsuspecting AOL users. To see how phishing can affect us, refer to the cartoon strip.
Details on who is behind the phishes, the concept of Web crawlers, spear phishing and vishing are given in Appendix 4 (2.1. – 2.4.).

Similar to the phishing concept and its variants described in this section is spoofing. What spoofing is and the types of spoofing as well as spoofing mechanisms are discussed in the next section.

5.2.2. Spoofing [Internet Crime Complaint Center (IC3), 2008a]

“When someone clicks on a compromised page, the attack checks for five different [Microsoft] vulnerabilities on the user's PC, and if it finds one, redirects them to a malicious Web site that can install identity-stealing malware” [Sherstobitoff in Miller, C. 2008].

The term “spoofing” refers to the fabrication of electronic documents claiming to be a legitimate or trusted business. This practice includes falsified e-mails and Web pages.
Vast amounts of information and billions of Web pages are contained within the WWW. It is easy for potential fraudsters to reinvent themselves and duplicate the entire Web because it is accessible to anyone and the Web constantly changes. As mentioned earlier in this document, the Internet operates by creating flawless copies of data from one machine to another.

What spoofing is, the types of spoofing, spoofing mechanisms and the people who are behind the spoofed e-mail to distribute spam are discussed next.

**What is Spoofing? [Simon, I.M. 2008]**

Spoofing means to fool. A spoofing attack in networking terms describes a situation where one computer is able to masquerade as a different computer or program. Spoofing generally refers to an unknown or fraudulent source masquerading as the actual source to gain an unfair advantage. An unfair advantage may be gained by tricking us to surrender sensitive information such as passwords, credit card and personal information. This is achieved by a common technique known to redirect our Web browsers to falsified Web sites.

Directing us away from the original Web site and to the fraudulent Web site or proxy server takes places through a technique known as pharming crime ware, also known as DNS cache hijacking or DNS cache poisoning (see cartoon strip below). Hackers attack the servers that host legitimate sites and once the sensitive details such as passwords have been entered, the victim is then redirected back to the original site. The Web site therefore was set up to steal information and is not genuine. Chapter 6 explains how to spot a spoofing scam.

See Appendix 4 (3.1. - 3.3.) for details on the:

- Different types of spoofing
- Spoofing mechanisms such as:
  - The man-in-the-middle attack
  - Spoofed Web sites residing in the cache
  - Why we must beware of filling in online forms
  - Bookmarking Web pages
- Masterminds behind spoofing and why
Chapter 5 - Modus Operandi (MO) Techniques for Committing Online Fraud

“WHAT HAPPENS WHEN YOU ENTER A WEB ADDRESS...”
WWW.MYBANK.COM

“THIS IS WHY SOME PEOPLE REFER TO THEIR COMPUTER AS SHE.”
ANYWHERE.COM, WHERE IS THAT?
WWW.MYBANK.COM

“NOT THERE, ROUTER, ANY IDEA?”
WWW.MYBANK.COM

“HEY THERE, ROUTER, ANY IDEA?”
WWW.MYBANK.COM

“HEY BUDDY, DO YOU KNOW MYBANK.COM?”
WWW.MYBANK.COM

“WHY... YES! IT IS 192.168.1.1.

“WHAT HAPPENS IF YOUR HOME ROUTER HAS BEEN PHARMED...”
WWW.MYBANK.COM

“MIP... EH... WAIT!!! I AM CORRUPTED. Bedroom, B + & #89.”
WWW.MYBANK.COM

“WHAT TO WATCH OUT IF YOU JUST TYPED THE CORRECT ADDRESS ...”
WWW.MYBANK.COM

“YOU WILL BE TAKEN TO THE WRONG PLACE...”
WWW.MYBANK.COM

“THANKS! THE ADDRESS IS 192.168.1.1.”
WWW.MYBANK.COM

“SO WHAT EXACTLY IS PHARMING, AND HOW DO YOU AVOID IT?”
WWW.MYBANK.COM

“To be continued...

PHARMINING IS LIKE...
OUT FOR A WALK WITH YOUR COMPUTER.

“EXCUSE ME! SIR, WHERE IS WWW.MYBANK.COM?”
WWW.MYBANK.COM

“MYBANK.COM, MY DEAR, JUST TURN LEFT, THEN THE THIRD ENTRANCE ON THE RIGHT...”
WWW.MYBANK.COM

“THANK YOU SO MUCH HAVE A NICE DAY.”
WWW.MYBANK.COM

“BEHIND THE BLUE DOOR!!”
WWW.MYBANK.COM

“NOW, JUST HAND OVER ALL YOUR CASH, OH! AND GIVE ME THAT PASSWORD TOO!”
WWW.MYBANK.COM

Reproduced with permission. Please visit www.SecurityCartoon.com for more material. Cartoons © 2007 By Sukamol Srikwan & Markus Jakobsson
Spoofing is not the only way in which we can become a victim to unwillingly surrendering personal data. A common technique called social engineering can also be used to solicit personal and sensitive credential information.

5.2.3. Social Engineering

Social engineering occurs when confidential and financial information is lured from the victim. This concept is similar to that of phishing, pretexting, spoofing and stealing information through malicious software (malicious software is covered in category 3). A common form of social engineering is the parcel courier e-mail scheme, as well as spam. The parcel courier e-mail scheme is discussed in Appendix 4 (section 4).

5.2.3.1. SPAM [Internet Crime Complaint Center (IC3). 2008a]

Spam is known as unsolicited bulk e-mail, used for social engineering purposes to extract information from users, such as sensitive personal and credential information. With improved technology and worldwide Internet access, bulk e-mail is sent simultaneously through numerous identical messages.

Spam is widely known as unsolicited e-mail because we on the receiving end did not opt to receive such e-mails. The US Controlling the Assault of Non-solicited Pornography and Marketing (CAN SPAM) Act, Title 18, U.S.C., Section 1037, is violated by those who send spam.

The result of unauthorized virus and Botnet infections on remote computers and servers can also be due to Spam, which may carry such malicious intent.

5.2.3.2. Masterminds behind SPAM

The perpetrators behind the spam often provide hosting services and sell open proxy information, credit card information and e-mail lists illegally.
In addition to spam and social engineering, the information which we willingly provide about ourselves on social networks can evidently also be used by fraudsters to gain personal information.

5.2.4. Social Networks

The personal information from social networks, such as Facebook and MySpace, can be used to the perpetrator’s advantage.

The cartoon strip presented below illustrates how people owning accounts on social networking Web sites are at greater risk of getting phished. Once we surrender our username and password we use to log in to the social networking Web site, the perpetrator may try to reuse our username and password for other Web sites we use to do Internet banking with. Once the perpetrator gains access to our social networking account, the personal information we provide about ourselves may be used to the perpetrator’s advantage and before we know it, we are victims of identity theft, credential and monetary fraud.

Reproduced with permission. Please visit www.SecurityCartoon.com for more material. Cartoons © 2007 By Sukamol Srikwan & Markus Jakobsson
In this category the methods of solicitation were presented. Information can also be solicited without our knowledge through the use of malicious software mechanisms (refer to Table 4).

**5.3. Category 3: Malicious Software**

**TABLE 4. Preview of malicious software category (category 3)**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 3 MALICIOUS SOFTWARE | 3.1. Spyware and malware  
3.2. Key loggers  
3.3. Wireless attacks  
3.4. Peer-to-peer file-sharing  
3.5. Botnets  
3.6. Browser hijacking  
3.7. Anti-spyware scams |
5.3.1. Spyware and Malware (Malicious Software) [msalsbury, 2006]

“Casey explains that spyware is software that covertly monitors activity on a computer and gathers information to be sent back via an Internet connection to whoever planted it” [ICTWorld. 2007].

About 92% of all computers are infected with risks that cannot be identified by most security programs. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using viruses and spyware such as key loggers. Malicious software can consist of various forms of spyware and adware, viruses, worms, rootkits and Trojans.

A spyware and/or virus program on any computer can cause multiple unwanted effects and potentially affect our productivity when using that particular machine. A computer can be slowed down by activities such as:

- Degradation of system performance
- Unwanted CPU activity
- Unwanted disk usage
- Unwanted network traffic, which may also cause difficulties connecting to the Internet
- Stability issues, such as application or system-wide crashes

In some cases users will assume that poor performance is a result of a virus, may be hardware-related or a Windows fault.

Since spyware monitors all users’ browsing activities, spyware software also records passwords, PIN code and credit card numbers that we key in. All this information can be used for identity theft purposes and even to access a user’s online banking account to make counterfeit transactions at the victim’s expense. Viruses may be instructed by their creator to achieve the same results.

5.3.1.1. What is Spyware? [msalsbury, 2006]

Spyware is computer software installed secretly on a user’s computer to supervise his actions without his knowledge or consent. This type of computer software records certain behaviours that take place and poses risks and threats such as the theft of personal information including credit card numbers. This is achieved by intercepting our communications transmitted over the Internet, routing URL requests to advertising sites, taking full or partial control over our interaction with
the computer, changing configuration settings and generally causing slight to severe forms of malfunction.

Appendix 4 (5.1. – 5.7.) provides further details on:

- The installation of unwanted software/spyware
- Adware in the spyware community
- Spyware used for commercial gain
- A user’s opt-in approach to spyware
- An introduction to anti-spyware packages
- Spyware and cookies
- How spyware is a security issue

5.3.1.2. Examples of Spyware [City of Gulfport.
2006] [Free Computer Technical Support.
2008]

A few examples of common spyware are given in this section to provide samples of the different behaviours found in some spyware applications.

- **CoolWebSearch:** a group of programs which direct traffic to advertisements of Web sites including coolWebsearch.com. The programs install themselves by exploiting Internet Explorer vulnerabilities. They also rewrite search engine results, modify the hosts file and display pop-up advertisements.

- **Internet Optimizer:** when entering a broken link or erroneous URL Internet Explorer is redirected to advertising pages. Internet Optimizer also makes it impossible for us to access password-protected Web sites since both use the same mechanism (HTTP basic authentication) as HTTP errors.

- **180 Solutions:** detailed information is transmitted to advertisers about the Web sites which users visit. HTTP requests are altered for affiliate advertisements linked from a Web site, so that the advertisements make unearned profit for the 180 Solutions Company. Pop-up ads are presented that cover the Web sites of competing companies.

- **HuntBar:** distributed by TrafficSyndicate, this is installed by ActiveX drive-by downloads where spyware installs more spyware. This form of spyware can be downloaded from partner Web sites, or advertisements displayed by other spyware programs. Another name for HuntBar is WinTools or Adware Websearch. Additionally, toolbars are installed onto
Internet Explorer to track Web browsing behaviour, redirect affiliate references and display advertisements.

Examples of spyware were mentioned and spyware and adware were discussed in this section. Viruses and spyware are interlinked and both approaches may achieve the same purpose.

5.3.1.3. Malware (Viruses and Trojans)

Malware, which is short for malicious software, may cause harm to a user’s computer or may even be created to achieve a certain purpose. Malware is used to steal PII, send spam and commit fraud. Convincing stories, appealing Web sites and attractive download offers are designed as bait to download malware through its links. Computers which do not use adequate security measures are at greater risk of infections and compromise of the security of data.

A common form of malware, namely Remote Access Trojans (RATs), is discussed in Appendix 4 (5.8.).

5.3.1.4. Virus Examples [AVG. 2008]

A few virus examples are presented here, to give a brief overview of their different functions:

- **I-Worm:** variants of this virus exist where a link in IP format contained in spam e-mail leads us to infected Web sites, or alternatively prompts us to download worm files such as funny.exe, foolsday.exe, kickme.exe, valentine.exe, withlove.exe. Web sites and worm sites have the capability to change every few minutes.

- **Stration Downloader:** spreads through e-mail messages with randomly generated subject and body. The e-mails come with two attachments: a pdf and an .exe extension and the virus may download itself.

The cartoon below illustrates what different malware fraudsters use to gain valuable information. Screen shots of the screen elements are captured each time the mouse is clicked, instead of the recorded keystrokes. This is called a screen scraper. The other methodology captures the keystrokes and is known as a key logger. The data stealer sends stored information to the fraudster from the hard drive.
Spyware and malware and examples of each were discussed in particular, to give a bit of background how a computer system can become infected and accessed remotely. Spyware and viruses can be used interchangeably as both may be forms of malicious software used to achieve the same malignant purpose. Another key concept, which is also directly related to remotely acquiring sensitive information, is the key logger.

5.3.2. Key Loggers

Like spyware and interception mechanisms, identity theft and various other potential risks and threats may materialize through the use of key logging procedures. This is a common methodology to gain access to our accounts. We could be providing our personal and sensitive information when innocently using the Internet.
5.3.2.1. What is Keystroke Logging?

Key loggers may be hardware- or software-based and may deliver all the information keyed in by a potential victim to fraudsters. Key loggers capture all our keystrokes without our knowledge or consent. A key logger captures everything that is typed through the keyboard, which may include personal data such as our passwords, credit card numbers and banking details.

5.3.2.2. SSL Technology and Key Logging

By ensuring a secure connection when accessing Web pages through the browser does not mean thieves will not get hold of your information. SSL technology will provide some security of our information between the browser and the server computer. SSL will not encrypt data that is typed from our keyboard into the browser.

Details on how key loggers are installed, the reasons why fraudsters use key logging and current key logging software versions are discussed in Appendix 4 (6.1. - 6.3.).

There are many versions of software key loggers. A common area where key loggers are rife is the Garden Route along the coast of South Africa. These are the parts of the country where tourists are most likely to use an Internet access point at a public place, such as Internet cafes. Another common strategy somewhat related to key logging software is when tourists attempt to access the Internet using a wireless hotspot in a public place.

5.3.3. Wireless Attacks

Wi-Fi is the common name for wireless technology supported by nearly every personal computer operating system. Wi-Fi is used in networks, cell phones and more. In addition, the wireless technology enables easy wireless access to applications and data. Compatibility and cohesiveness are ensured without the conventional cabling and wiring, switches, adapters, plugs and connectors.

Network security regarding wireless attacks is discussed in Appendix 4 (section 7).
5.3.3.1. Threats to Security [Krebs, B. 2006]

The ever-present Wi-Fi hotspots have become a genuine target for criminal behaviour.

The attacker sets up a counterfeit hot spot nearby a legitimate hot spot (such as an Internet cafe or coffee shop), also called an “evil twin”. When customers log in to the overlapping “evil twin” network, every movement is monitored and sensitive information is stolen by the thieves.

5.3.3.2. Evil Twins [Krebs, B. 2006]

An evil twin network is a fraudulent hot spot targeted at wireless networks. The fake overlapping Internet service looks like a legitimate service where the fraudster can gather our sensitive and PII. When the victim connects, the thief may launch a man-in-the-middle attack on transactions on the Internet, or alternatively may ask for credit card information from the victim when logging in on the pay-per-access deal.

In this section the threats to security and the concept of evil twins were mentioned briefly to give an overview of wireless attacks. Wireless attacks are not the only means for perpetrators to gain access to sensitive information. Another methodology used by fraudsters to gain access to computer systems is peer-to-peer file-sharing.

5.3.4. Risk of File-sharing (P2P Networks)

Users connected to the Internet allow computers to be connected to a variety of other computers around the world. File-sharing programs easily downloaded from the Internet can be software which allows our computer to connect to another informal network. Peer-to-peer (P2P) file-sharing programs enable users to share music, games, various software programs and other information among one another all over the world. Downloading such software enables other users to access not just the files made available for sharing, but other files too.

Other files could also grant unwanted access to confidential information stored on your hard drive and encourage illegal activity. You may also unintentionally download material protected by copyright, or pornography labelled as something innocent. P2P networking may act as a breeding ground for the following activities, but is not limited to the two concepts of:
• **Computer hacking:** P2P networking has opened up yet another area for the spread of unsolicited activities by criminals and the spread of viruses, worms and Trojans. Such malicious activities have been created specifically to spread over the P2P networks. If the P2P networking program is not configured properly, users may be exposing their entire hard drive to cyberspace, thus exposing private sensitive information to perpetrators.

• **Copyright infringement:** the illegal distribution of music, games, videos and other intellectual property of the producers and creators thereof is a violation of copyright law. Any entity involved in such intellectual property theft may be up for possible criminal prosecution and investigation.

Other sharing risks, such as some worms and viruses, may take advantage of the file-sharing option to spread throughout the Internet, and are discussed in Appendix 4 (section 8). A form of controlling a group of computers is done by spreading worms and Trojan viruses, commonly known as Botnets.

5.3.5. **Botnets [Krebs, B. 2006]**

A botnet (robot network) is a network of compromised computers under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam e-mail, identity theft, denial of service attacks, and spreading malware to other computers on the Internet [Internet Crime Complaint Center (IC3), 2008a].

Perpetrators may infect target computers with a Trojan that allows the computer to be controlled remotely. An attack may then be launched from the victim’s home computer onto a complete stranger. Web servers are set up on the victim’s computer to host fraudulent phishing Web sites. As a result, thousands of these hijacked machines can be used as “zombies” to secretly send spam or to host fake Web sites. These botnets allow criminals their anonymity while assigning massive processing power of numerous machines.

Another form of hijacking, also through the spread of viruses, is known as browser hijacking.

5.3.6. **Browser Hijacking [Sauver, J.S. 2004]**

Microsoft Internet Explorer (IE) has been a frequent target owing to its popularity and reputation for its security vulnerabilities. It has become an obvious point of attack into Windows.
Browser hijacking occurs when the Web site we attempt to visit is redirected to another Web site using a Browser Help Object (BHO). It is common for the hijacker to redirect the browser to an alternative Web site featuring explicit adult content, which can be a rather disconcerting experience.

This is known to happen in IE which has not been patched or updated for known security vulnerabilities.

In some cases, the following security issues may be caused by the modifications made by the browser hijacking code:

- The system may be presented with system stability issues or general system performance degradations.
- Privacy and security may be compromised by sending information back to the hijackers on the Web sites visited, or even the information entered into those Web sites.
- The system may display pop-up advertisements on the desktop.
- Removal of the infection may be resisted when using standard anti-spyware or anti-virus programs.

In an attempt to remove the infection and regain control of the system, we think an anti-spyware download might do the trick. But beware of the fraudulent anti-spyware programs advertising false claims.

### 5.3.7. Anti-spyware Scams [WordPress.com. 2008]

A large number of fraudulent anti-spyware programs have been released advertising spyware removal of infected systems through Web banner advertisements. These fraudulent anti-spyware programs do not remove anti-spyware, but do quite the contrary: they append additional spyware instead.

Another name for this type of software is rogue software, which claims to be either anti-spyware, anti-virus or registry cleaners. The software is then installed by clicking on the advertisement.

This section covered the malicious software epidemic and how it can infect a user’s computer system, compromising privacy and other security matters. Anti-spyware scams, browser hijacking, botnets, peer-to-peer file-sharing, wireless attacks, key loggers and spyware and malware were presented. Compromise of sensitive data does not only take place through covert malicious software programs, but can also occur when a user responds to one or all of the following fraud schemes. A popular fraud scheme is known as Nigerian 419 scams/advance fee fraud, which is discussed next (refer to Table 5).
5.4. Category 4: Fraud Schemes

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 4 FRAUD SCHEMES | 4.1. Nigerian 419 scams/advance fee fraud  
4.2. Debt elimination  
4.3. Escrow services fraud  
4.4. Investment fraud  
4.5. Auction fraud |

5.4.1. Advance Fee Fraud/Nigerian 419 Scams [PIC Mailblock]  
[Internet Crime Complaint Center (IC3), 2008a]

419 fraud is also known as advance fee fraud or job scams. Advance fee fraud scams, which are more commonly known as Nigerian 419 scams, have been in operation for a long time. The Nigerian 419 scam originally began in the form of letters (snail mail) and later also by fax and telephone call. A recent estimate by the US Secret Service has 80% of all Nigerian 419 scam incidences now being initiated via e-mail [PIC Mailblock].

These scams are used to trick people into revealing personal data. The naivety and greed of people have become the prime factor contributing to the success of these crimes.

See Appendix 4 (9.1. - 9.4.) for explanations and examples of:

- The most common 419 scams
- Job scams
- Lottery wins
- Inheritance payouts
Scams such as the inheritance payout, lottery win and job scams are used to trick people into revealing personal data. Another form of trickery is the debt elimination scam.

5.4.2. **Debt Elimination** [Internet Crime Complaint Center (IC3). 2008a]

All personal information is provided to the fraudster, which increases the risk of identity theft. A legal way to dispose of mortgage loans and credit card debts is advertised on Web sites. The participant is required to send a certain amount of money to the fraudster, including all personal information such as loan details, and a special power of attorney to gain authorization to enter into transactions regarding the title of the participant’s homes on their behalf.

Confirmation documents and bonds are then issued to the lenders that falsely claim to legally satisfy the debts of the participant. The participant is required to pay a certain percentage of the satisfied debts to the fraudster.

Scams other than debt elimination may also have undesired similar results, such as escrow services fraud and investment fraud, discussed in the following sections.
5.4.3. Escrow Services Fraud [Internet Crime Complaint Center (IC3). 2008a]

A legitimate escrow services Web site is compromised by fraudsters to gain an unfair advantage by offering escrow services facilitating the exchange of money and merchandise.

Also known as Web spoofing, the compromised Web site resembles the original one. The victim then sends ordered goods to the customer or sends payment for an order and never receives the funds as the escrow site is not legitimate. These falsified escrow sites target unwary Internet auction participants.

5.4.4. Investment Fraud [Internet Crime Complaint Center (IC3). 2008a]

“Investment fraud is an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities” [Internet Crime Complaint Center (IC3). 2008a].

One example of investment fraud is the Ponzi/pyramid fraud scheme.

Ponzi/Pyramid Fraud

Ponzi/pyramid fraud schemes are investment scams where investors are promised abnormally high returns on their investments. The system collapses when the first investors receive returns from the money received from the most recent investors. The most recent investors lose their initial investment as no investment is actually made.

5.4.5. Auction Fraud [Internet Crime Complaint Center (IC3). 2008a]

Auction fraud is the process whereby an item is fraudulently advertised for sale on an Internet auction site. The result is the non-delivery of the product after the required funds have been transferred to the illegitimate seller.
Examples of the types of auction fraud, such as the Romanian auction fraud and phony escrow services fraud, are given in Appendix 4 (10.1. – 10.2.).

Category 4 representing fraud schemes such as investment fraud, debt elimination and Nigerian 419 scams/advance fee fraud was described. Other forms of fraud fall under the extortion category, where criminals get away with blackmailling to gain an unfair advantage by using or gaining user information. The first form of extortion discussed is the information broker, followed by Internet extortion. Refer to Table 6.

5.5. Category 5: Extortion

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 EXTORTION</td>
<td>5.1. Information brokers</td>
</tr>
<tr>
<td></td>
<td>5.2. Internet extortion</td>
</tr>
</tbody>
</table>

5.5.1. Information Brokers [Krebs, B. 2006] [Obringer, L.A. 1998-2008]

Information brokers, also known as data thieves, obtain personal information through illegal activities. These illegal activities may include paying off, bribing or offering a cut of the profits to insiders such as employees, and breaking into computer systems in order to sell personal information. This personal information may also include PII about other employees.

Often personal data is sold on Internet Relay Chat (IRC) or exchange the PII for other illegal goods on Web forums that cater to identity thieves. An example of such a Web forum is shadowcrew.com, where criminals could buy and sell credit card information, social security numbers and mothers’ maiden names. The Web site operated as an identity-theft eBay but was put out of operation by the US Secret Service in October 2004.
5.5.2. Internet Extortion [Internet Crime Complaint Center (IC3). 2008a]

Control is gained over an industry database usually containing valuable sensitive credential information either of employees, customers, or similar. The hackers then pledge to release ownership of the database back to the company if the company grants them a Web administrative job, or pays funds in exchange for it. The hackers may threaten to compromise or sell the information contained in the information database of the company.

The concept of extortion was introduced, with examples of information brokers and internet extortion activities. Other illegal activities include identity theft, online gambling and conventional fraud (refer to Table 7).

5.6. Category 6: Illegal Activities

TABLE 7. Preview of illegal activities category (category 6)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>6.1. Identity theft</td>
</tr>
<tr>
<td></td>
<td>6.2. Online gambling</td>
</tr>
<tr>
<td></td>
<td>6.3. Conventional fraud MO</td>
</tr>
</tbody>
</table>

5.6.1. Identity Theft [FNB. 2007] [Anonymizer. 2008a] [Wallace, J. 1998-2008]

5.6.1.1 How Does It Happen?

Identity theft is not necessarily a new crime, or even strictly a digital one. In fact, identity theft goes back to the Old Testament where Jacob impersonated Esau. The criminal activity of stealing someone else’s PII - and clean credit ratings - has escalated thanks to the birth of the Internet.

We all think no one is interested in our personal information. Think again. “We may think identity theft will never happen to us but that is what happened to over 10 million people last year alone” [Anonymizer. 2008a]. Cybercriminals form groups targeting consumers and businesses online. In the wrong hands, our stolen identity can provide unauthorized access to accounts and credit cards.
Internet thieves steal money through identity theft. “US Treasury adviser Valerie McNiven claimed that cybercrime had become a more profitable industry than illegal drug trafficking” [Krebs, B. 2006: 28].

The thief pretends to be the owner of the identity and by using the victim’s PII, may access the information by [FNB. 2007]:

- Breaching security measures and hacking into industry or individual computer databases
- Deceiving consumers into disclosing personal or financial information by:
  - phishing, or
  - sending e-mail or
  - sending pop-up messages.
- Directing customers to fraudulent Web sites which look identical to a trusted site, such as a bank by means of spoofing to phish for personal information
- Distributing spyware through the Internet entering users’ computers to collect personal information

As seen above, there are many possibilities of how fraudsters may access PII. Identity theft is used as a vehicle to commit crimes, and in the next section, the primary objectives and negative consequences of identity theft as well as the numbers of people who fall victim to such crimes are presented.

5.6.1.2 What is Identity Theft? [Wallace, J. 1998-2008]

Identity theft occurs when an offender obtains our personal and confidential information like names and credit card numbers without permission to commit fraud or other illegal crimes [Wallace, J. 1998-2008].

This can occur in the virtual or physical world and are often interlinked. Offenders can use personal information to apply for loans, rent accommodation, steal money from accounts, open a new telephone account and new credit accounts using stolen PII. These acts can damage our credit and leave us with unwanted bills. The unauthorized use of an identity can cause us countless hours, even years, of inconvenience to clear our name.

In Appendix 4 (11.1. – 11.3.) more details are given on identity theft, such as:

- How it is used as a vehicle to commit crimes
- The primary objectives of identity theft
- How identity theft figures escalate in numbers
The concept of identity theft has been introduced and defined. The rest of the chapter describes how fraudsters can get hold of information to commit identity fraud, as well as how we can put ourselves at risk when gambling online.

5.6.2. Online Gambling [FBI. 2008]

It is against the law to gamble online; at least in the United States. Even if we do not get caught gambling, the money we keep in an online gambling account may be lost if the company faces charges. In these cases, the US government confiscates all assets whenever possible.

Gambling can be done legally if we go to legitimate gambling places.

5.6.3. Conventional Fraud Modus Operandi

Conventional fraud methodologies to steal credential information can also be used the old-fashioned way, but are still in use today. This section will introduce the concepts of dumpster diving, changing of address, old-fashioned stealing and pretexting.

5.6.3.1. Dumpster diving

The offender searches through trash looking for bills, statements or other paper with your personal information on it.

5.6.3.2. Changing the victim’s address

The offender diverts the victim’s billing statements to another location by completing a change of address form.

5.6.3.3. Old-fashioned stealing

The thief steals wallets and purses, mail including bank and credit card statements, pre-approved credit offers, cheques, chequebooks or tax information. Thieves have the ability to steal personnel records, or bribe employees who have access.
5.6.3.4. Pretexting

The thief uses false pretences to obtain our personal information from financial institutions, telephone companies and other sources.

THE CONCERNS OF 1907…

THE CONCERNS OF 2007…

Reproduced with permission. Please visit www.SecurityCartoon.com for more material. Cartoons © 2007 By Sukamol Srikwan & Markus Jakobsson

Below is a table summarizing all the different categories (see Table 8).

5.7 Summary of MO and Respective Categories

Each MO has been explained and described and each belongs to a certain category, summarized in Table 8.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 BANKING</td>
<td>1.1. Credit card fraud</td>
<td>Results in money stolen from the victim or the victim’s bank account</td>
</tr>
<tr>
<td></td>
<td>1.2. SIM swap scam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3. Payment confirmation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.4. Counterfeit cashier’s cheque</td>
<td></td>
</tr>
</tbody>
</table>
The way in which fraudsters operate can be quite a disconcerting experience, especially when we discover that we have been victimized. There are preventative measures and precautions that can be taken by understanding the corresponding awareness strategies.

The next chapter is dedicated to preventing MO subterfuge based on the same approach followed in this chapter. Chapter 6 illustrates how the risks of each MO presented in Chapter 5 can be prevented and mitigated.
Part III

Compromise of Sensitive Information

Chapter 6
Preventing MO Subterfuge
THE DILEMMA THAT WE AS END-USERS OF AUTOMATED ENVIRONMENTS SUCH AS INTERNET BANKING HAVE IS THAT

the responsibility for SECURING YOUR PRIVATE INFORMATION is becoming more and more your own responsibility.

INDEPENDENT ONLINE. 2008.
Chapter 6
Preventing MO Subterfuge

6.0. Overview

Various Internet crime schemes are used by perpetrators as a method of operating to achieve their motive. By using the various MO, which were introduced in Chapter 5, victims risk losing their identity, resulting in financial and credibility loss.

The following are preventative measures that will assist us to be informed and aware prior to entering into online transactions over the Internet. The preventative measures provided in this chapter are not necessarily fool proof, but will mitigate the risks of compromising sensitive and valuable information.

“With an increasing number of brazen criminals targeting individuals, it is important that you know how to protect yourself from becoming a victim as well as what to do in the event of being targeted” [Federal Bureau of Investigation. 2008].

The preventative measures for the different and most common methodologies used by perpetrators to commit crimes and gain access to credential information are described in this chapter and organized into relevant categories. There are six categories in total and each MO is sorted into its applicable category (see Table 9), following much the same approach as in Chapter 5. This chapter also contains cartoon strips to better explain certain fraud methodologies and to create a better understanding and awareness.
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 1 BANKING         | 1.1. Credit card fraud  
|                   | 1.2. SIM swap scam    
|                   | 1.3. Payment confirmation  
|                   | 1.4. Counterfeit cashier’s cheque |
| 2 SOLICITATION    | 2.1. Phishing        
|                   | 2.2. Spoofing         
|                   | 2.3. Social engineering  
|                   | 2.4. Social networks  |
| 3 MALICIOUS SOFTWARE | 3.1. Spyware and malware  
|                   | 3.2. Key loggers      
|                   | 3.3. Wireless attacks  
|                   | 3.4. Peer-to-peer file-sharing  
|                   | 3.5. Botnets          
|                   | 3.6. Browser hijacking  
|                   | 3.7. Anti-spyware scams  |
| 4 FRAUD SCHEMES   | 4.1. Nigerian 419 scams/advance fee fraud  
|                   | 4.2. Debt elimination  
|                   | 4.3. Escrow services fraud  
|                   | 4.4. Investment fraud  
|                   | 4.5. Auction fraud    |
| 5 EXTORTION       | 5.1. Information brokers  
|                   | 5.2. Internet extortion  |
| 6 ILLEGAL ACTIVITIES | 6.1. Identity theft  
|                   | 6.2. Online gambling  
|                   | 6.3. Conventional fraud MO   |
6.1. Category 1: Banking

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 1 BANKING| 1.1. Credit card fraud  
|          | 1.2. SIM swap scam  
|          | 1.3. Payment confirmation  
|          | 1.4. Counterfeit cashier’s cheque |

6.1.1. Preventative Measures: Credit Card Fraud [Internet Crime Complaint Center (IC3). 2008b] [James. 2008]

Fraudulently acquiring money or property through the use of an unauthorized credit card, debit card or credit card number is considered credit card fraud. Credit or debit card numbers can be stolen from unsecured Web sites or an identity theft scheme. Ensure the following to mitigate the risks of credit card fraud in an online environment:

- Always do some research on the Web site before providing credit card details online. This can be done by:

  - Researching the legitimacy of the individual or company.
  - Ensuring that the Web site is secure.
  - Not trusting a Web site just because it claims to be secure.
  - Ensuring that the merchandise is from a reputable source.
  - Regularly checking credit card statements to ensure that no unauthorized charges have taken place.
  - Never providing any credit card information by e-mail, especially when requested through unsolicited e-mail.
  - Addressing any queries directly to the bank and obtaining telephone numbers independently such as on statements or a telephone directory.
  - Not responding to e-mails, telephone calls, or text messages requesting personal information, especially if contact was first initiated by the other party.
6.1.1.1. Mitigating credit card fraud

To further mitigate the risks of credit card fraud:

- Ensure that the credit or debit card is never left unattended and is always treated as cash.
- Never reveal your PIN to anyone, even if it is bank staff.
- Never divulge the credit card number over the telephone.
- The bank must be contacted immediately if the credit card is lost or stolen:
  - Get a reference number.
  - Keep a record of the date and time of the call, as well as the name of the person who took the call.
  - Follow up on the call to ensure that the card has been stopped.
- Keep copies of all receipts.
- Check bank statements carefully and query any unauthorized transactions immediately.

6.1.1.2. Reporting Credit Card Fraud [Watson, L. 2008]

It is advisable to always query a transaction you may suspect and find out later that it was a transaction you were merely confused about, rather than that your credit card has been used to commit fraudulent activities.

Credit card fraud can be reported on the following numbers in South Africa:

- Nedbank: 011 667 8761
- ABSA: 012 317 3721
- Standard Bank: 0800 301 450
- FNB: 011 352 5910 or 0800 004 500

Additionally, helpline numbers can be found out from various branches, on ATM and bank cards, the bank’s Web site as well as ATMs.

See 6.1.1. on identity theft for more information or on how to place a fraud alert on your credit report. There are other developments taking place which will significantly reduce credit card fraud, namely the new microchip or smart card, which is discussed briefly in Appendix 5 (1.2.).

Directly related to credit card fraud is credit card skimming. The steps and details on how to prevent skimming are discussed in Appendix 5 (1.1.).
Another common methodology to grasp a victim’s finances is what is commonly known as the SIM swap scam.

6.1.2. Preventative Measures: The SIM Swap Scam

The details on how a SIM swap scam works were given in Chapter 5. The actions to take to mitigate the risks of a SIM swap scam are described next.

6.1.2.1. How to Find Out

The only way to know that we are a victim of the SIM swap scam is that we will have a loss of signal on our cell phone SIM card. A loss of signal means that we will not be able to receive notifications from the bank, nor make or receive any phone calls or SMS messages.

Fraudsters swap our cell number, unbeknown to us, and can then receive the bank’s random verification number (RVN), or one-time PIN (OTP).

6.1.2.2. What Actions to Take

The second there is a lost signal on the cell phone or we suspect that this has occurred, we must:

1. Immediately contact our cellular service provider.
2. Contact the Internet banking helpdesk to cancel our Internet banking access immediately. This will prevent the perpetrator or anyone else from gaining access to our banking accounts.

6.1.2.3. Countermeasures by Service Providers

MTN is implementing a security countermeasure to the SIM swap scam. In order to allow time for the owner of the SIM card to respond, an SMS will be sent to the subscriber informing him of the request before the original SIM card is replaced.

This allows time for the subscriber to respond before the SIM swap takes place.
6.1.3. Preventative Measures: Payment Confirmation

As discussed in Chapter 5, section 5.1.3., an electronic payment is made into our account and the proof of payment is altered and faxed/sent to us by e-mail. Sometimes the thief will claim that an overpayment was made and request a reimbursement.

To avoid becoming a victim of the payment confirmation scam, always make sure the funds are in the account concerned before refunding any money whatsoever. This will prevent us, the victim, from transferring funds back to the perpetrator which are not available.

This defrauding scheme can also occur when receiving cheques.

6.1.4. Preventative Measures: Counterfeit Cashier’s Cheque
[Internet Crime Complaint Center (IC3). 2008b]

In chapter 5, section 5.1.4., it was explained that the bank only notifies the victim of the counterfeit cashier’s cheque after the funds stipulated on the cash cheque have been transferred. The victim is then held responsible for reimbursing the bank for the funds owing. To prevent such a scam from being transacted, always conduct a thorough inspection of the cash cheque by:

- Ensuring that the figures and words match the amount stipulated on the cheque.
- Ensuring that the account number is not shiny in appearance.
- Examining the drawer’s signature to ensure that it has not been traced.
- Checking for perforation on one side, as official cheques are perforated on one side.
- Checking for deletions, additions and other alterations.
- Contacting the financial institution to ensure the legitimacy of the cheque which was drawn.
- Obtaining the bank's telephone number independently and not from the cheque itself.
- Always being wary when conducting business with individuals from foreign countries.

In this category, the concepts of the counterfeit cashier’s cheque, payment confirmations, the SIM swap scam and credit card fraud were discussed. The next category, solicitation, deals with how criminals solicit confidential information from a user. The first common solicitation scheme discussed is phishing, and protecting ourselves from such solicitation scams is explained (refer to Table 11).
6.2. Category 2: Solicitation

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
</table>
| 2  | 2.1. Phishing  
|    | 2.2. Spoofing  
|    | 2.3. Social engineering  
|    | 2.4. Social networks |

6.2.1. Preventative Measures: Phishing [MSN.co.za. 2008]

With phishing scams, looks can be deceiving. The e-mail is never from whom it appears to be and it may not always be obvious at first glance that what is in the victim’s inbox is not a legitimate e-mail from the company with whom the victim does business. Phishing e-mails can appear to come from anywhere where a person has registered for an account and supplied financial information, and may include Web sites such as PayPal, eBay, credit card companies, online retail stores and banks.

6.2.1.1. Phishing Golden Rules [FNB. 2008]  
[Internet Crime Complaint Center (IC3). 2008b]

The Golden Rule is that we should never access our Internet banking portal by clicking on a link. We must always type our bank’s URL into our Internet browser manually. We must never respond or reply to or interact with the sender of an e-mail that:

- Issues directions to enter personal information such as user ID, password or account numbers or to submit the information entered into the e-mail in any way.
- Displays urgency and threatens to suspend the account if immediate action is not taken by responding with personal information.
- Encourages entering of personal information in a survey.
• Asks for confirmation of account information, when claiming that the account has been compromised or third-party activity has taken place.
• Encourages entry into a draw to win a holiday trip or financial reward by requiring banking details. When the link is clicked, we are directed to a fraudulent Web site.
• Requires confirmation and verification to refresh the account details, credit card or address information.

The most important rule to remember is that your bank will never ask for sensitive information by e-mail. Any e-mail is at risk of being intercepted. For this reason we must never send our personal and financial information by e-mail, and we can stay safe by:

• Understanding how the e-mail address will be used before entering it on third-party Web sites.
• Comparing the link contained in the e-mail to the redirecting link.
• Not opening e-mail with attachments if the sender is unidentified.
• Entering the URL to the official Web site instead of clicking on the link contained in the e-mail.
• Contacting the business that the e-mail appears to have come from to verify its contents.

6.2.1.2. Take Action if We have been a Phishing Victim [MSN.co.za. 2008]

If we feel our personal information has been compromised or stolen, we need to take the following actions:

• Any accounts which were opened or accessed without our permission must be closed immediately.
• All the passwords and PINs to all online accounts must be changed immediately.
• See the part on identity theft on how to create a fraud alert on the credit report.

Appendix 5 (2.1 – 2.5.) provides details explaining:

• How to spot a phishing scam
• What to do if phisher e-mail is received
• What are the warning signs?
• Spoofed e-mails and their common phrases
• Additional resources should we wish to acquire more information from different sources

Similar to the phishing concept is spoofing. The term “spoofing” refers to the fabrication of electronic documents claiming to be a legitimate or trusted business.
This practice includes falsified e-mails and Web pages and is explained in the next section.

### 6.2.2. Preventative Measures: Spoofing

As described previously in Chapter 5, 5.2.2., spoofing means to fool. A spoofing attack in networking terms describes a situation where one computer is able to masquerade as a different computer or program. Spoofing generally refers to fraudulent e-mail masquerading as the actual source to gain an unfair advantage.

Because jurisdictions fail to effectively control people’s activities on the Internet, the most effective solution is a technological one. Control can be increased by means of restricting what can and cannot be done and can be used as a defence mechanism against attackers. We can defend ourselves from such attacks by implementing:

- **Technological solutions**
  - Clearing the cache
- **Mechanisms and defence strategies such as:**
  - Configuring the border router
  - Configuring a firewall
  - Ensuring proper authentication mechanisms
  - Ensuring the integrity of messages

These are explained in detail in Appendix 5 (3.1. – 3.2.). For the purpose of this discussion the short-term solutions are provided here.


There are ways to mitigate the risks of the JavaScript attacks on the location line and status bar (discussed in Appendix 5 (2.2.3. and 2.2.4., respectively), including other items such as the menu bar (discussed in Chapter 6, 6.2.2.2.). Methods to counteract these attacks are to:

1. Disable JavaScript in the browser.
2. Ensure that the location line is visible at all times.
3. Ensure that the URL displayed in the browser’s location line always points to the correct server.

JavaScript, ActiveX and Java introduce security vulnerabilities leading to spoofing attacks. Disabling these features means limited functionality, but these features can
be reactivated when visiting a trusted site. Another technique to attempt to uncover spoofing attacks is to view the document source.

### 6.2.2.2. View the Document Source [Anti-Phishing.info. 2008]

The spoofing attack can also be uncovered in the HTML source of the Internet browser. Viewing the HTML source of the displayed Web page reveals the code used to display the Web page, and rewritten URLs in the source may be identified. Usually in Internet Explorer, clicking on “View” in the menu bar and then “View Source” reveals the HTML code. HTML source code will not be easy for novice users to read and understand. Because it is inconvenient to look at the source code each time one visits a Web page, this procedure cannot really be used as a safeguard mechanism.

The location of the attacker’s server must be revealed in order to carry out the attack. Evidence of that location will be available after an attack is detected. However, this information cannot be relied on since most attackers hack into an innocent person’s computer and execute the attack from there. In some cases the perpetrators use stolen computers.

However, JavaScript can also be used to replace the menu bar with a fraudulent one which looks identical to the original one. If the above procedure were to take place to check the HTML source, a new window would be displayed demonstrating the original HTML source from the original Web site.

This is not the only way in which we can become a victim to surrendering personal data. A common technique called social engineering can also be used to solicit personal and sensitive credential information.

### 6.2.3. Preventative Measures: Social Engineering

Social engineering occurs when confidential and financial information is elicited from the victim. This concept is similar to that of phishing, pretexting, spoofing and stealing information through malicious software. To avoid becoming a victim of one of the most common forms of social engineering scams such as the parcel courier e-mail scheme, see its countermeasures and defence mechanisms listed in Appendix 5 (section 4).
6.2.3.1. SPAM [MSN.co.za. 2008]

Spam is known as unsolicited bulk e-mail, used for social engineering purposes to extract information from users, such as sensitive personal and credential information. With improved technology and worldwide Internet access, bulk e-mail is sent simultaneously through numerous identical messages. The concept of mitigating the risks of e-mail and MSN Messenger spam is discussed in the following sections. MSN Messenger spam is included in this discussion, owing to its popularity amongst Internet users.

6.2.3.2. E-mail SPAM [ninemsn. 1997-2008] [PIC Mailblock]

Mitigating the risks of spam is straightforward. Don’t respond to spam, and report it to those who can do something about it (as discussed in under phishing). Keeping the primary e-mail address as private as possible is always a good idea. Examining the privacy policy of Web sites before entering an e-mail will cause fewer headaches in the future. Combating spam can be done in the following ways:

- Make use of the anti-spam modules provided by our ISP, e-mail program and anti-virus program.
- Keep the primary e-mail address for trusted, more formal sources only. The secondary e-mail address can be used for other purposes.
- By reading the privacy policies of Web sites, it can be determined if the e-mail address will be released to third parties. In such a case, we should not reveal our e-mail address to that Web site.
- Downloading images and responding to the e-mail (such as clicking on the “unsubscribe” or “remove me”) can be used to confirm that our e-mail address is valid, and will lead to a big increase in spam.
- If spam is received, we must not open it. Rather delete the e-mail unread.
- We should never release our e-mail address unless we know what purpose it will be used for.
- Never post our e-mail address on blogs and bulletin boards. The e-mail address may be broadcast and Web spiders (programs) that search the Internet may collect the e-mail for spamming purposes.
- Never respond to or purchase from advertisements contained in unsolicited e-mail which may encourage us to purchase merchandise.
- Be wary about attachments at all times. By opening attachments, malicious software can be downloaded to the computer. Rather check the attachment with anti-virus software before opening it.
• If the e-mail appears to come from a charity and requires a donation, we should phone the charity to find out how we can make a contribution and must not reply or respond to the e-mail request.
• Predators start forwarding chain e-mail messages to gather e-mail addresses. We should not respond to chain letters as we may lose control over who sees our e-mail address.

6.2.3.3. MSN Messenger SPAM [ninemsn. 1997-2008]

Protecting ourselves from MSN Messenger spam can be done by blocking messages from strangers. From the “Tools” menu, click on “Options” and in the privacy tab, check “Alert me when other users add me to their contact list”. This prevents strangers from accessing us through Messenger without our permission, and ultimately, our computer. If it is a stranger we do not want to talk to, that person may be blocked to allow for tighter security.

A common medium through which we may unknowingly and voluntarily compromise sensitive information about ourselves is known as social networks.

6.2.4. Preventative Measures: Social Networking

The personal information from social networks, such as Facebook and MySpace, can be used to the perpetrator’s advantage. Do not provide any personal information on these Web sites, especially not credit card numbers, usernames or passwords. If possible, never send sensitive data through this channel to a friend or family member. The ultimate solution is to not subscribe to or use these services in the first place.

Information can also be solicited without our knowledge through the use of malicious software mechanisms (refer to Table 12).
6.3. Category 3: Malicious Software

### TABLE 12. Preview of the malicious software category (category 3)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 MALICIOUS SOFTWARE</td>
<td></td>
</tr>
<tr>
<td>3.1. Spyware and malware</td>
<td></td>
</tr>
<tr>
<td>3.2. Key loggers</td>
<td></td>
</tr>
<tr>
<td>3.3. Wireless attacks</td>
<td></td>
</tr>
<tr>
<td>3.4. Peer-to-peer file-sharing</td>
<td></td>
</tr>
<tr>
<td>3.5. Botnets</td>
<td></td>
</tr>
<tr>
<td>3.6. Browser hijacking</td>
<td></td>
</tr>
<tr>
<td>3.7. Anti-spyware scams</td>
<td></td>
</tr>
</tbody>
</table>

6.3.1. Preventative Measures: Spyware and Malware (Malicious Software)

Awareness and various user practices may also reduce the chance of getting spyware on a system. Minimizing the risks of spyware may involve the processes of running a clean install to prevent spyware from further opening doors to other forms of malware, as well as choosing an Internet browser which is less targeted by hackers.

6.3.1.1. Minimizing the Chances of Malware

Download [Paz, U. 2002] [OnGuard Online. 2008a]

Downloading malware to a computer can be hazardous to the personal information and other data stored on that computer. This was discussed in detail in Chapter 5. Keeping aware can minimize the chances of compromising sensitive data:

- Never click on a link or open an e-mail attachment as the links may direct us to sites which download malware.

- Free software such as file-sharing programs, customized toolbars, free games and free anti-spyware programs may sound attractive but free software may be, or may download, malware.

- Avoid clicking on pop-ups, or revealing PII anywhere online.
• Use anti-malware programs to prevent malicious content download. An example of such software is a firewall, which may block and identify many types of adbots and malicious advertisements. Anti-malware programs are discussed in detail in Chapter 7.

Although every effort can be made to mitigate the risks of malware download, compromising the computer and our privacy, malware may still find its way into the system. Appendix 5 (5.2) explains what can be done if malware really did enter the system, which is likely to happen. The next section outlines anti-virus golden rules.

6.3.1.2. Anti-virus Golden Rules

The three golden rules will help us to prevent malware from entering, infecting and compromising sensitive data:

1. Our anti-virus software program must be properly installed and functioning correctly on our computer.
2. Perform updates on a daily basis.
3. Perform a scan **daily**, especially before conducting online activities such as online banking. This reduces the risk of any malicious viruses capturing our banking information.

Even if the anti-virus program does not recognise all threats, some protection is better than none at all.

A discussion on minimizing the risks of spyware and what to do if malware has infected a computer is provided in Appendix 5 (5.1.–5.2.).

Another key concept related to malicious software is key loggers.

### 6.3.2. Preventative Measures: Key Loggers

Every keystroke may be monitored through various mechanisms, such as key loggers. Key loggers are installed through the use of viruses and Trojans to carry out some phishing attacks. The information keyed in is sent directly to the attacker, and may include credit card numbers, usernames and passwords as well as banking details. To prevent the system from becoming infected with viruses or Trojans, we need to know what safety precautions to take.

**Key Logging Counterstrategies [Webby. 2008]**

The following counterstrategies may protect us against key logging infections:

- Do not leave workstations unattended, especially when connected to the Internet.
- Ensure that the workstation is inspected regularly by trusted IT specialists.
- Effective anti-virus, anti-spyware and firewall software packages must be properly installed and updated on a regular basis.
- Promote tourist awareness about the risks involved when using a public terminal.

The details on what to do if the system is infected and tips to prevent key logging from taking place are discussed in Appendix 5 (6.1.–6.2.).

Another common strategy related to key logging software is when tourists and users attempt to access the Internet using a wireless hotspot in a public place.
6.3.3. Preventative Measures: Defending Wireless Attacks
[Spanbauer, S. 2003]

The risks of wireless attacks were set out in section 5.3.3. The most effective preventative measure in this case is to never use an Internet terminal in a public place, especially when conducting confidential transactions such as online banking that requires usernames and passwords.

On a more technical note, driver and firmware updates for Wireless Protect Access (WPA) standard are released by wireless-networking vendors for their products. Visit the Microsoft Web site to download Microsoft’s WPA update for Windows XP.

However, wireless attacks are not the only workaround for perpetrators to gain access to sensitive information. Another methodology used by fraudsters to gain access to computer systems is peer-to-peer file-sharing.

6.3.4. Preventative Measures: Peer-to-peer File-sharing [OnGuard Online. 2008b]

The risks of P2P file-sharing applications were discussed in section 5.3.4. These risks include connecting to a network where millions of users can be connected to one another simultaneously, allowing others to view and copy private files, downloading material subject to copyright laws and even downloading viruses compromising the security of the system. It may be useful in this case to consider the precautions when insisting on using P2P file-sharing applications.

P2P File-sharing Precautions

The primary concern is downloading a file-sharing program that can be trusted and is not in itself malware. That software and the operating system must then be kept up to date to prevent a breach of security. It is also advisable to adjust the preferences, options or controls of the program and instruct it not to connect to the network at all times; even when closed the application may continue to run in the background. Further details to avoid unrestrained distribution of confidential documents, such as tax returns, e-mail messages, medical records, photos, account statements and other personal documents, along with the files you want to share are listed in Appendix 5 (section 7).
Some worms and viruses take advantage of the file-sharing option to spread throughout the Internet. A form of controlling a group of computers is done by spreading worms and viruses, known as Botnets.

### 6.3.5. Preventative Measures: Botnets

As introduced in chapter 5, section 5.3.5., a botnet is a network of compromised computers under the control of a single user. Perpetrators may infect target computers with a Trojan that allows the computer to be controlled remotely, effectively controlling many computers simultaneously.

The preventative measure in this case is to implement firewall, anti-spyware and anti-virus software to prevent access to the computer from external sources. Any Trojan viruses detected by the anti-virus software before they can be exploited will disallow the attacker the advantage of gaining easy access and control of compromised systems. The firewall will serve to avoid any attempts to gain unauthorized access to the system.

Another form of hijacking, also through the spread of viruses, is known as browser hijacking.

### 6.3.6. Preventative Measures: Browser Hijacking [Sauver, J.S. 2004]

The concept and realistic possibility of browser hijacking was introduced in section 5.3.6. Browser hijacking occurs when the Web site we attempt to visit is redirected to another Web site using a BHO. What to do when the system is already compromised, and the preventative measures to mitigate the risks of being infected are explained below.

#### 6.3.6.1. When the System is Compromised

The browser has been hijacked if the page we attempt to visit keeps redirecting to a different page. If this occurs, run a reputable anti-virus program immediately. Ensure that it is fully updated and run a full system scan. The second step is to run an anti-spyware program such as Spybot Search and Destroy, or Lavasoft’s Ad-Aware to remove anything the anti-virus program may have missed.

If the browser is still hijacked, visit SpywareInfo’s Browser Hijacking Web site at [http://www.spywareinfo.com/articles/hijacked/](http://www.spywareinfo.com/articles/hijacked/), which provides additional excellent suggestions to regain control of the Internet browser.
If none of the suggestions help to remove the infection, the last resort is to do a low-level format of the hard drives and reinstall the operating system. Ensure that all the relevant backups have been made. Additionally, the newly installed system must be fully patched and updated for any security vulnerabilities before reconnecting to the Internet (this includes Service Packs for Windows OS). If these updates are not done, additional viruses may enter the system.

**6.3.6.2. Precautions to Avoid Future Infections**

As a precaution to avoid future infections, always run an update to install critical security updates and patches on the operating system. For Windows, visit [http://windowsupdate.microsoft.com/](http://windowsupdate.microsoft.com/) to perform an update.

In an attempt to remove the infection and regain control of the system, we may assume that an anti-spyware download is likely to remove the infection. But beware of fraudulent anti-spyware programs making false claims.

**6.3.7. Preventative Measures: Anti-spyware Scams**

A large number of fraudulent anti-spyware programs have been released advertising spyware removal of infected systems through Web banner advertisements. These fraudulent anti-spyware programs do not remove anti-spyware, but do quite the contrary by appending additional spyware instead.

Some known offenders include AntiVirus Gold, ContraVirus, Errorsafe (also known as System Doctor), MacSweeper, PALSpywareRemover, SpywareStrike, Spyware Quake, SpyShredder, Spy Sheriff, Spy Wiper, UltimateCleaner, WinAntiVirus Pro 2006, WinFixer and WorldAntiSpy.

It is recommended that we do not install any freeware claiming to be anti-spyware unless it is verified to be legitimate.

This section set out the preventative measures for the malicious software epidemic and how infections of the computer system, which may compromise privacy and other security issues, can be avoided. The preventative measures of anti-spyware scams, browser hijacking, botnets, P2P file-sharing, wireless attacks, key loggers and spyware and malware were presented. Compromise of sensitive data does not only take place through covert malicious software programs, but can also occur when a user responds to one or all of the following fraud schemes. A popular fraud scheme
is known as the Nigerian 419 scams/advance fee fraud, which is discussed next (refer to Table 13).

### 6.4. Category 4: Fraud Schemes

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 FRAUD SCHEMES</td>
<td>4.1. Nigerian 419 scams/advance fee fraud</td>
</tr>
<tr>
<td></td>
<td>4.2. Debt elimination</td>
</tr>
<tr>
<td></td>
<td>4.3. Escrow services fraud</td>
</tr>
<tr>
<td></td>
<td>4.4. Investment fraud</td>
</tr>
<tr>
<td></td>
<td>4.5. Auction fraud</td>
</tr>
</tbody>
</table>

#### 6.4.1. Preventative Measures: Advance Fee Fraud/Nigerian 419 Scams [Internet Crime Complaint Center (IC3). 2008b]

These scams are used to trick people into revealing personal data. The naivety and greed of people have become the prime factor contributing to the success of these crimes. We must never disclose any personal data about ourselves to anyone, by e-mail or telephone, no matter what personal information is asked for. For more details on advance fee fraud, see Chapter 5, section 5.4.1.

**Reporting Advance Fee Fraud [PIC Mailblock]**

Advance fee fraud may be reported to the relevant authorities based on which countries are mentioned in the e-mail and the recipient’s country. The incident should be reported to the local police service if the e-mail contains threats to your safety.


However, when receiving such mail, do not reply by sending humorous or strange replies. The people behind these scams are usually organized and sometimes very dangerous gangs.
Reporting advance fee fraud has been discussed. Money laundering, job scams and lottery win preventative measures are listed in Appendix 5 (8.1. – 8.3.). Another form of trickery relying on the characteristics of naivety and greed of people is the debt elimination scam.

6.4.2. Preventative Measures: Debt Elimination [Internet Crime Complaint Center (IC3). 2008b]

All personal information is provided to the fraudster, which increases the risk of identity theft. A legal way to dispose of mortgage loans and credit card debts is advertised on Web sites. The participant is required to send a certain amount of money to the fraudster, including all personal information such as loan details, and a special power of attorney to gain authorization to enter into transactions regarding the title of the participant’s homes on their behalf. To prevent from becoming a victim of such criminal activities, we need to take the following precautions:

- Do extra research to ensure that we know who we are dealing with by obtaining the name, address and telephone number of the individual or company.
- Do extra research on the individual or company to ensure that they are who they claim they are.
- Ensure the legitimacy of the company by contacting the Better Business Bureau.
- Always take extra care when communication with people in a foreign country and ensure that we understand all terms and conditions of any agreement.
- Be extra cautious of businesses that operate from P.O. boxes or mail drops.
- Contact other customers of the particular individual or company by asking for their names and contact details.
- If the offer or opportunity sounds too good to be true, it probably is.

Scams other than debt elimination may also have undesired similar results, such as the escrow services fraud and investment fraud, discussed in the next section.

6.4.3. Preventative Measures: Escrow Services Fraud [Internet Crime Complaint Center (IC3). 2008b]

A legitimate escrow services Web site is compromised by fraudsters to gain an unfair advantage by offering escrow services facilitating the exchange of money and merchandise.
The following tips will mitigate the risks of falling victim to such fraudulent activities:

- Always type the URL manually into the browser instead of clicking on the link to direct you there.
- Works of other companies will never be duplicated by legitimate companies.
- When a Web site requests payment to an agent instead of a corporate entity, be extra cautious.
- Be wary when escrow service sites only accept wire transfers or e-currency.
- Look out for spelling and grammatical errors, or inconsistent information.
- Be wary if the Web site offering escrow services requests extremely low fees.
- If you did not post auctions, never agree to accept wire payments for those auctions.
- Be extremely cautious when the individual states that his country will not allow receipt of funds from a different country, and when dealing with people in a foreign country.

Another type of fraud constructed to defraud us is known as investment fraud.

6.4.4 Preventative Measures: Investment Fraud [Internet Crime Complaint Center (IC3). 2008b]

Investment fraud was introduced in Chapter 5, 5.4.4. Ponzi/pyramid fraud schemes are investment scams where investors are promised abnormally high returns on their investments. The following tips will aid us to identify when such an investment scam situation is presented to us:

- If the offer or opportunity seems too good to be true, it probably is.
- Promises for making fast profits and investments that offer high return at little or no risk should send off alarm bells.
- We must always verify the terms and conditions of any investment we intend to make and do not invest anything unless we understand the deal.
- Do research to ensure the legitimacy of the investment and the parties involved, and do not assume a company is legitimate based on the Web appearance.
- To determine the legitimacy of the company, contact the Better Business Bureau.
- Never respond to investment offers contained in unsolicited e-mail, especially if the other party initiated the contact.
- Beware of any references obtained from the promoter.
- Do extra research when doing business with people in a foreign country and do not take their presence at face value.
Another type of fraud constructed by individuals for their own personal gain is known as auction fraud.

6.4.5. Preventative Measures: Auction Fraud [Internet Crime Complaint Center (IC3). 2008b]

Auction fraud is the process whereby an item is fraudulently advertised for sale on an Internet auction site. Auction fraud and the different types of common auction fraud were discussed in Chapter 5, 5.4.5. The result is the non-delivery of the product after the required funds have been transferred to the illegitimate seller. It is recommended that extra care be taken when sellers exhibit the following behaviour, especially when entering into Internet transactions:

- Beware of people who post auctions under one name and request the funds to be transferred to another individual, or the person requests the funds to be transferred directly to him using Western Union, MoneyGram or bank-to-bank wire transfer, deeming the fund unrecoverable when using these services.
- The seller may post auctions as if he resides in the US, then responds with an e-mail claiming he is outside of the US for business reasons, family emergency, and so on.
- Avoid sellers acting as authorized dealers when there should be no such dealers in those particular countries.
- We need to avoid buyers who ask us to ship the order using a certain method to avoid customs or taxes.
- Ensure that the card holder’s authorization has been received before shipping any products and additionally, be suspicious of any credit card purchases where the address of the card holder does not match the shipping address.
- It is a good idea to contact the seller with any questions we may have before placing our bid.
- Always do extra research when dealing with people in a foreign country.
- Determine and verify the amount for the shipping charges before we purchase the item and always ensure that we understand refund, return and warranty policies.
- In case an escrow service is used, always research and ensure that the service is a legitimate one.
- It may be a good idea to review the seller’s and buyer’s feedback and be wary if the seller only accepts wire transfers or cash.
- Be wary of unsolicited offers, especially if the contact was first initiated by the third party.
- It may also be a good idea to consider insuring the item.
The category representing fraud schemes has been presented, including how to prevent and be aware of auction fraud, investment fraud, escrow services fraud, debt elimination and Nigerian 419 scams/advance fee fraud. Other forms of fraud fall under the extortion category, where criminals get away with blackmailing to gain an unfair advantage by using or fraudulently acquiring user information. The first form of extortion and its preventative measures discussed is the information broker, followed by Internet extortion in category 5 (refer to Table 14).

### 6.5. Category 5: Extortion

**TABLE 14.** Preview of extortion category (category 5)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5.1. Information brokers</td>
</tr>
<tr>
<td>EXTORTION</td>
<td>5.2. Internet extortion</td>
</tr>
</tbody>
</table>

#### 6.5.1. Preventative Measures: Information Brokers

As discussed in chapter 5, section 5.5.1., information brokers are also known as data thieves, who obtain personal information through illegal activities. In most cases, it is the responsibility of the organization which collects sensitive customer information to prevent data leaks to third parties. There is little we can do in this regard to protect sensitive information, where personal data can be leaked from the organization itself. If avoiding this is desired, prevent from conducting any online transactions or subscribing to any online services requiring personal data. This is an ideal solution, but not necessarily a realistic one.

Another variant of information brokerage is Internet extortion.

#### 6.5.2. Preventative Measures: Internet Extortion [Internet Crime Complaint Center (IC3). 2008b]

As discussed in Chapter 5, section 5.5.2., Internet extortion is closely related to various forms of blackmail, depending on the attacker’s agenda. To prevent attackers from gaining access to and retaining control over valuable information, the following is advised:
• Barriers need to be built to keep intruders out of the system as much as possible. This means that the security implemented needs to be multi-layered.
• Ensure that every possible entry point has been blocked with some kind of security measure, by downloading and installing the most recent updates for the operating system and all software.
• Assess the security measures implemented on each machine.
• Identify the ports our system and servers may be using, and whether they are known to present security vulnerabilities.

The concept of extortion and its preventative measures were discussed, along with examples of information brokers and Internet extortion activities. Other illegal activities include identity theft, online gambling and conventional fraud, which are introduced in category 6 (refer to Table 15).

6.6. Category 6: Illegal Activities

<table>
<thead>
<tr>
<th>TABLE 15. Preview of illegal activities category (category 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATEGORY Modus Operandi (MO)</td>
</tr>
<tr>
<td>ILLEGAL ACTIVITIES</td>
</tr>
<tr>
<td>6.1. Identity theft</td>
</tr>
<tr>
<td>6.2. Online gambling</td>
</tr>
<tr>
<td>6.3. Conventional fraud MO</td>
</tr>
</tbody>
</table>


We can find out if our identity was stolen by checking our accounts, bank statements and credit reports regularly. We may thus be able to limit the damage caused to us through identity theft. Profiles are contained and can be requested from the credit bureau. The three main credit agencies - Equifax, TransUnion and Experian - offer subscriber-based, online fraud alerts (see step 2 in 6.6.1.1. for more information).

We (most victims) may only find out that we have indeed been a victim of identity theft when some damage has already been done:

• Bill collection agencies contact us for overdue debts never incurred.
• When applying for a mortgage or car loan, there may be problems with the credit history, which will cause issues and delays.
• Receiving mail in our post about a flat never rented, a house or a car never bought, or a job never held.
• We may find out that we have unknowingly been married.

Additional tips for organizing our case, how long the effects of identity theft last, how to fight back against identity theft, what to do if our information has been compromised but not yet misused as well as additional tips and preventative measures are discussed in Appendix 5 (9.1. – 9.5.).

6.6.1.1. What are the Steps We Should Take if We are a Victim of Identity Theft? [Federal Trade Commission. 2008c] [Credit Health. 2007]:

If we are a victim of identity theft, we need to take the following four steps as soon as possible, and keep a record of the details of our conversations and copies of all correspondence.

Step 1: Immediately notify the bank.

Our bank should work with us to make appropriate corrections of unauthorized transactions, and protect us from any future account fraud.

Step 2: Review and place fraud alerts on all credit reports.

If our identity has been stolen, a fraud alert will prevent the offenders from opening any further accounts in our name. Visit http://www.experian.co.za/ or http://www.transunion.co.za/ for more information and to obtain a credit report.

Companies such as the South African Fraud Protection Services (SAFPS) offer such services where the alert tells creditors to follow certain procedures before they open new accounts in our name or make changes to our existing accounts. Where there is evidence of impersonation by another person, the theft or loss of identity books and other personal documents can be registered. A facility for such issues is offered to the members of the public and is a free protective registration facility. Registrations and all relevant contact information relating to such issues are available on the Internet through the SAFPS Web site at http://www.safps.org.za/.

Credit reports, once received, must be reviewed carefully and we must look for enquiries from companies we have not contacted, accounts we did not open and debts on our accounts that we cannot explain. We need to check that information like our identity number, addresses, name or initials and employers are correct. Get any fraudulent or inaccurate information removed.
We must continuously check our credit reports, especially for the first year after we discover the identity theft, to make sure no new fraudulent activity has occurred.

**Step 3: Accounts which have been opened or tampered with must be closed immediately.**

We must contact someone in the security or fraud department of each company. We must follow up in writing and include copies, not originals, of supporting documentation. It is imperative that credit card companies and banks be notified in writing. We must send our letters by registered mail, return receipt requested, so we can document what the company received and when, and keep a file of all correspondence and enclosures.

When opening new accounts, we must use new PINs and passwords. We must avoid using easily available information like our mother's maiden name, our birth date, the last four digits of our identity number or our phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on our accounts, or has fraudulently opened accounts, we must ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, we must ask the representative to send us the company's fraud dispute forms. If the company does not have special forms, we must write our own to dispute the fraudulent charges or debits. In either case, we must write to the company at the address given for "billing enquiries," NOT the address for sending our payments.
- For new unauthorized accounts, we can either file a dispute directly with the company or file a report with the police and provide a copy to the company.

Once we have resolved our identity theft dispute with the company, we need to ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is our best proof if errors relating to this account reappear on our credit report or if we are contacted again about the fraudulent debt.

**Step 4: File a report with the police where the identity theft took place.**

Even if the police cannot catch the identity thief, having a police report can help our bank with the investigation.
6.6.1.2. How do We Prove that We are an Identity Theft Victim? [Federal Trade Commission. 2008a]

We can prove that we are an identity theft victim by presenting various applications, transaction records and transcripts. These transcripts can be issued by companies if requested in writing and must be accompanied by a police report. These documents may contain valuable information about the identity thief. An example is viewing the signature on these documents and proving that it is not ours.

Online gambling is another illegal activity not directly related to identity theft.

6.6.2. Preventative Measures: Online Gambling [FBI. 2008]

Online gambling is illegal in the US, which disallows placing cyber bets in virtual card games or on sporting events, the electronic transfer of money for gambling or betting in Internet casinos even if they are placed in a foreign country.

There are online activities which are legal, however. These activities include some free online games, fantasy leagues and Indian gaming sites that are not strictly defined as Internet gambling.

The conventional approach does not concern the modern online approach, but has been around for much longer. Protecting our information from being acquired through the conventional fraud strategies is discussed next.

6.6.3. Conventional Fraud Protection Strategies [Krebs, B. 2006] [The Mercury. 2008]

Conventional fraud methodologies to steal credential information can also be used in the old-fashioned way, but are still in use today.

6.6.3.1. Keep PC Clean

Anti-virus and anti-spyware programs are the key to keeping malicious software and thieves out of a user’s sensitive information. Keep the programs running at all times.
and up to date. Anti-virus and anti-spyware software packages are discussed in more
detail in Chapter 7.

6.6.3.2. Build a Barrier

Implement firewalls. Ensure that the Windows firewall is enabled but also install a
different firewall, such as Zone Labs' ZoneAlarm, or get an anti-virus security suite
which comes with a built-in firewall. It is also a good idea to purchase a router which
has a built-in firewall for added protection. Create a secure computer environment
with a personal firewall, anti-virus and anti-spyware software and anti-spam filters.

6.6.3.3. Prevention is Better than Cure

Any organization on the Internet can have a Web presence – even fraudulent ones.
Do research before doing business with any company presented on the Web. Obtain
a fixed address and landline number and ensure that the Web site is secure.

It is vital that we never leave our ID lying around anywhere, nor at the office or at
home or leave important, confidential documents out in the open. Never do any
type of online transaction from an Internet cafe as these public places are at most
infected with malware.

If receiving e-mail requesting entry of any personal information such as account or
credit card information, we should not respond. Furthermore, we can set up SMS
notifications with our respective bank to alert us of any transactions that take place.

6.6.3.4. Don't Get Fooled

Never respond to any e-mail asking for personal information. No bank will ever ask
any of their customers to update their personal information by e-mail. If we are
uncertain, we should phone the bank to verify the authenticity and validity of the
message.

In general, the Internet is a reflection of the real world, where con artists try to lure
the gullible. So, if anything looks too good to be true, it probably is, and may well be
a scam.

In addition, be cautious about personal information, like our date of birth, that we
make available in online forums or on social networking sites such as Facebook or
MySpace.
6.6.3.5. Think Before We Click

Many worms and viruses infecting a user’s computer are due to a single click on a URL in an e-mail message. If an e-mail launches itself to a designated Web site requesting PII, try to re-enter that URL manually. Additionally, never open attachments in e-mails as they could contain malware, especially if received from anyone we don't know or from an unreliable source.

6.6.3.6. Check Up on Ourselves

Bank and credit card statements must be checked carefully. Fraudsters will sometimes only make minor purchases to avoid being detected.

6.6.3.7. Get Rid of Our Paper Trail

We need to be sure to destroy any credit card and loan applications before discarding them into the trash can, and shred anything with our personal details on it, such as name and address.

6.6.3.8. Act Quickly

We must contact our bank immediately if we notice any suspicious activity on our account, and if our cell phone stops working for no reason, we need to contact the service provider immediately.

In the event of a stolen ID, contact the major credit bureaus and SA Fraud Prevention Service to file an alert. The Fraud Prevention Service is a non-profit service whose Web site contains useful information about identity fraud. Visit http://www.safps.org.za for more information.
In this category, the preventative measures against illegal activities such as conventional fraud methods, online gambling and identity theft were discussed. The next section provides a table summarizing all the different categories (see Table 16).

### 6.7. Summary

The actions for all concepts introduced in this chapter can be summarized as staying alert and preventing. It is imperative to be aware of the possibility that we may be targeted. Table 16 is a brief overview summarizing each category.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Modus Operandi (MO)</th>
<th>Summary of Preventative Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 BANKING</td>
<td>1. Credit card fraud</td>
<td>Do not respond immediately to any activity, particularly when it involves a fraudulent proof of payment or cheque.</td>
</tr>
<tr>
<td></td>
<td>1.2. SIM swap scam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3. Payment confirmation</td>
<td></td>
</tr>
</tbody>
</table>

### Chapter 6 – Preventing MO Subterfuge

<table>
<thead>
<tr>
<th>2 SOLICITATION</th>
<th>1.4. Counterfeit cashier’s cheque</th>
<th>Never allow your credit card out of full view and take immediate action if the signal fails on your cell phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1. Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2. Spoofing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3. Social engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4. Social networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 MALICIOUS SOFTWARE</td>
<td></td>
<td>Never respond to any e-mail requiring sensitive data and always be aware of the warning signs, such as spelling and grammatical errors on fraudulent Web sites, when doing any type of activity online</td>
</tr>
<tr>
<td>3.1. Spyware and malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2. Key loggers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3. Wireless attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4. Peer-to-peer file-sharing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5. Botnets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6. Browser hijacking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7. Anti-spyware scams</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 FRAUD SCHEMES</td>
<td>4.1. Nigerian 419 scams/advance fee fraud</td>
<td>Install, download and configure all anti-malware and firewall software accordingly. Beware of free software downloads.</td>
</tr>
<tr>
<td>4.2. Debt elimination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.3. Escrow services fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4. Investment fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.5. Auction fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 EXTORTION</td>
<td>5.1. Information brokers</td>
<td>Do the necessary research before entering any business deal with any online company. General guideline: if it sounds too good to be true, it probably is.</td>
</tr>
<tr>
<td>5.2. Internet extortion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 ILLEGAL ACTIVITIES</td>
<td>6.1. Identity theft</td>
<td>Build multi-layered security barriers to keep intruders at bay. At best, avoid online transactions altogether.</td>
</tr>
<tr>
<td>6.2. Online gambling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3. Conventional fraud MO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4. Burglary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5. Tax evasion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.6. {other illegal activities}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

113
The preventative measures for the various types of MO were discussed in this chapter, from conventional fraud to credit card fraud (all summarized into respective categories (see Table 16)). The way in which fraudsters operate can be quite a disconcerting experience, especially when we discover that we have been victimized or targeted.

By understanding the corresponding awareness strategies, the risks of each MO can be mitigated. Chapter 7 is dedicated to general security practices, such as ensuring secure passwords and implementing anti-malware software.
Part IV

General Preventative Measures

Chapter 7
Non-technical and Technical Preventative Measures
The number of poisoned Web sites is increasing.

1 in 1000 Web pages are infected with malicious drive-by downloads.”

- IDG News
Chapter 7
Non-technical and Technical Preventative Measures

7.0. Overview

The aim of this chapter is to address other preventative measures not directly related to the MO discussed in Chapter 5. All the preventative measures discussed in Chapter 6 addressed the risks of each MO introduced in Chapter 5. This chapter is dedicated to providing non-technical and technical preventative measures to ensure secure transactions and online Internet banking in general. Other security measures, such as choosing the most secure passwords, and implementing technical preventative measures, such as anti-virus programs, are now discussed in detail.

Multiple security mechanisms and programs can be used for added protection. The most common and most important security mechanisms are discussed in this chapter, where more than one of these concepts can be implemented simultaneously.

The main purpose of this chapter is to provide a general outline of which technical and non-technical preventative measures are available that may be used to advance security. Firstly, the non-technical preventative measures are discussed, followed by the technical preventative measures.
7.1. Non-technical Preventative Measures

This section focuses mainly on the non-technical preventative measures, namely user responsibilities. The objective of this section is to minimize the risks of compromising our PII and other sensitive information such as credentials and financial information. Another concept briefly introduced is the guidelines to securing unattended user equipment.

7.1.1. Passwords

A major problem concerning the electronic world is the use of passwords. Writing the password down, sharing it with others and forgetting it are cause for concern. Such negligent practices can lead to compromise of sensitive data and other unforeseen problems, such as financial loss. The various methods used by perpetrators to gain access to passwords as well as tips to choosing and memorizing passwords are discussed in Appendix 6 (1.1. – 1.2.).

Preventative Measures: Guidelines to a Secure Password (ISO/IEC 17799. 2005: 64)

1. Confidentiality of passwords must be maintained at all times. This means no sharing of passwords with friends or trusted colleagues.
2. Keeping a record of passwords should be prevented. Don’t write the password down on a piece of paper and keep it under our mouse pad, or store it electronically on the computer or in a hand-held device.
3. Change the password whenever we have reason to suspect compromise of the password.
4. Change temporary and default passwords at first logon.
5. Do not store passwords in any automatic logon process such as macros, function keys or in browsers.
6. Do not use the same password for every service including business and non-business purposes.
7. Do not use the same consecutive characters after each other.
8. Passwords must always be of sufficient minimum length (usually a minimum of six to eight characters, but longer is usually better).

A typical user should never leave a workstation unattended and unprotected. We must always log out of active sessions and ensure that access cannot be gained to the workstation without a password.

Screensavers may activate after a few minutes of inactivity. Screensaver passwords are also efficient to maintain privacy and prevent unauthorized access to unattended workstations.

Sensitive information on paper or electronic storage media should be stored in a safe location out of plain sight. Sensitive information stored on a computer terminal should be protected by means of encryption and must be password protected.

Sensitive and confidential information, such as financial statements, should be removed from the printer immediately and put into safe storage. When discarding
such information, including bills, which may lead to our identity, these should be shredded or destroyed by other means before entering the bin.

The guidelines to securing unattended user equipment and how to choose a secure password have been given. The next section introduces practices to implement technical preventative measures, and also talks about the why and how, and not only the what.

7.2. Technical Preventative Measures

This section covers implementing anti-virus, anti-spyware, firewall systems, identity protection, secure Internet browsers, secure e-mail clients and encryption mechanisms.

7.2.1. Anti-virus Software Packages [AVG Technologies. 2008]

There is a lot of talk about implementing anti-virus software but there is little explanation about which anti-virus software would be the best to use, what to do to ensure ultimate protection and why. The why aspect has been discussed in detail throughout this dissertation: to prevent the security risks relating to identity theft, financial fraud and compromising privacy in cyberspace. How these security risks can materialize has also been discussed in detail.

The ultimate goal of anti-virus software packages is to provide protection against new viruses before they can infect a user’s computer. An effective anti-virus package may include, but is not limited to:

- **Protection from hacker attacks:** once a hacker is able to gain access to the computer, he can use the compromised machine to distribute spam and to steal credentials.
- **Protection from malicious Web sites:** drive-by downloads can be blocked and users can be prevented from entering a phishing Web.
- **Protection from infected downloads:** prevention of downloading infected files or exchanging infected files through instant messaging.
- **Protection from e-mail scams and phishing:** confirm validity of incoming e-mail messages and remove spam, scams and other potentially dangerous e-mails.
- **Protection from spyware:** prevention of installing and downloading spyware onto our computer (anti-spyware is discussed in detail in the next section).
It is advisable to purchase the bundle, as it is important to update regularly, preferably on a daily basis, to be protected against constant new threats. New threats develop all the time, infecting computers in new malicious ways and are refined and advancing at a rapid rate.

Anti-virus programs prevent spreading the infection to more files on our computer.

7.2.1.1. Fast Answers: Anti-virus Products

[ConsumerSearch, Inc. 2008]

It is important to choose the anti-virus program that will provide us with the best performance to eliminate the spread of infections. An overview is provided of which anti-virus software best suits our needs. The following conclusions and results are based on reviewing the reviews and are subdivided into the following categories: Best anti-virus software overall, best anti-virus software for expert users, free anti-virus software, security suite and most popular anti-virus software (see Table 17).

<table>
<thead>
<tr>
<th>Categories</th>
<th>Review of Reviews - Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best anti-virus software overall:</td>
<td>According to users, when compared to the average anti-virus program, Kaspersky Anti-Virus 7.0 comes with more software conflicts and issues. Regardless of the software conflicts and issues, a much higher level of satisfaction is expressed than with Norton or McAfee.</td>
</tr>
<tr>
<td>Kaspersky Anti-Virus 7.0.</td>
<td>According to reviews, on the other hand, Kaspersky remains the best anti-virus software overall because it is better than the bestseller Norton Antivirus 2008, excels at preventing viruses and will not slow the computer as much as other bestseller antivirus programs.</td>
</tr>
<tr>
<td>Best anti-virus software for expert users:</td>
<td>According to reviews of 2007, NOD32 2.7 has an unintuitive and confusing user interface. The new version (3.0) has some considerable improvements but still is not very elegant.</td>
</tr>
<tr>
<td>ESET NOD32® 3.0</td>
<td>According to computer experts, NOD32 offers great protection, does not slow down the computer and use up resources and has no software conflicts. While competitor anti-virus programs earn average ratings or worse, NOD32 earns top average rating and is proven through user satisfaction, which is much higher than with any other anti-virus program.</td>
</tr>
</tbody>
</table>
Free anti-virus software: All reviews conclude that the commercial version of AVG’s performance levels are poor compared to Kaspersky and NOD32, among others.

AVG Anti-Virus Free Edition 7.5. On the other hand, professional reviewers claim that AVG Anti-Virus Free Edition is the best when comparing free anti-virus programs. Free anti-virus software may be enough if we are diligent and careful about personal security practices.

Security suite: According to reviews, secondary features such as spam prevention are not very good. On the other hand, primary tasks such as anti-virus and anti-spyware features are excellent.

Panda Internet Security 2008 According to user reviews, Panda Internet Security 2008 has no conflicts with other programs. Panda’s standalone Anti-Virus 2008 is also cheaper than other security suites, but is not recommended in one of the earlier reviews.

Most popular anti-virus software: Norton AntiVirus exercises a high level of control over a system and only a quarter of its users give it a high rating.

Norton AntiVirus 2008 According to reviews, Norton is excellent at detecting viruses but half its users complain about the resources Norton uses up and that it slows the computer down to a crawl. Additionally, Norton conflicts with other software.

However, Norton continues to be the bestselling anti-virus program.

### 7.2.1.2. Consensus Report [ConsumerSearch, Inc. 2008]

The Consensus Report shows how many times the anti-virus software has been top-ranked by reviewers (see Table 18).

<table>
<thead>
<tr>
<th>Number of Picks</th>
<th>Anti-virus Software Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ESET NOD32 3.0/2.7</td>
</tr>
<tr>
<td>5</td>
<td>Kaspersky Anti-Virus 7.0/6.0</td>
</tr>
<tr>
<td>4</td>
<td>Grisoft AVG Anti-Virus Free Edition 7.5 (free)</td>
</tr>
</tbody>
</table>
Chapter 7 – Non-technical and Technical Preventative Measures

| 2     | Avira AntiVir Personal Edition Classic (free) |
| 2     | Norton AntiVirus 2008                         |

7.2.1.3. Summary [ConsumerSearch, Inc. 2008]

The following is a summary of the reviews conducted:

**Best anti-virus software: (out of 28 reviews)**
Kaspersky Anti-Virus 7.0, ESET NOD32 3.0, AVG Anti-Virus Free Edition 7.5

To see more useful resources for reviews visit:

There are also free virus removals available, as discussed in the next section.

7.2.1.4. Free Virus Removal [ESET. 1992-2008a]

ESET offers a free public service to anyone who would like to scan and remove any virus, spyware, key logger or any other malware which may have already compromised the system. The free scan and removal tools may be downloaded from http://www.eset.com/download/free-virus-remover.php.

Appendix 6 (2.1. – 2.3.) provides a discussion on anti-virus software in more technical detail and includes anti-virus performance comparisons, anti-virus comparison charts, which is the best anti-virus, as well as useful links.

7.2.2. Anti-spyware Software Packages

Tracking personal information such as login names, passwords, PIN codes and other information can be recorded through the use of spyware. Spyware has been closely related to identity theft, where the recorded information can be used to steal identities. Furthermore, PII can be used more directly to fraudulently gain access to a victim’s banking details and funds. Appendix 6 (3.1. – 3.3.) provides further information on what to do when a spyware program installs itself, rogue software and the relevant security practices. Details of different anti-spyware programs are described below.
7.2.2.1. Anti-spyware Programs

In extreme cases when spyware has infected a computer beyond repair it is necessary to format and reinstall the operating system. However, the time-consuming procedures of having to backup user data can be prevented by installing programs. These programs, known as anti-spyware programs, can remove or block spyware from entering a system.

Commercial firms have released anti-spyware programs designed to protect our computer from harmful or potentially harmful infections.

One of the most well-known commercial firms invested in GIANT Anti-Spyware, which was available for download for genuine Windows XP and 2003 users. The software was renamed Windows Anti-Spyware Beta and later on Windows Defender. Windows Defender was downloadable at no cost in October 2006. The software is now integrated into the Windows Vista Operating System.

Other anti-spyware programs are as follows:

- PC Tools’s Spyware Doctor
- Sunbelt Software’s Counterspy
- Trend Micro’s HijackThis
- Webroot Software’s Spy Sweeper
- ParetoLogic’s Anti-Spyware and XoftSpy SE

The trend is to offer anti-spyware functionality as an extension of the existing anti-virus products. Symantec, McAfee and Sophos are examples of major anti-virus firms that have adopted anti-spyware real-time protection as an additional security feature.

7.2.2.2. Anti-spyware Programs can Combat Spyware in Two Ways: [Computer Cleanup. 2007]

1. **Real-time protection:** All incoming network data is scanned for spyware (software) and threats are blocked from entering the system. Attempts to install start-up items or to modify browser settings may also be intercepted.

2. **Detection and removal:** Works similar to the common anti-virus program which detects spyware content already installed on the computer. The software scans registry, the operating system and program files.
7.2.2.3. Performing Updates on Anti-spyware Software [Safe Surf. 2006]

An anti-spyware program is effective when the latest updates are installed regularly. This is important because anti-spyware developers constantly update their definitions and signature files needed for the anti-spyware program to detect malicious content.

Some anti-spyware packages provide alerts when configuration settings within the systems registry or browser settings have been altered and do not rely on an internal database filled with definitions.

Our choice of Internet browser can impact our security which is targeted by malware. More information on Internet browsers will be provided in Chapter 7, section 7.2.5. Implementing anti-virus, anti-spyware and firewall software packages will provide a security barrier against unauthorized access and unnecessary harmful virus infections.

7.2.3. Firewall Software Packages [AVG Technologies. 2008]

A personal firewall is a software program designed to control network traffic entering and exiting the computer system and to prevent any unauthorized access based on a security policy. Firewalls work by examining packets of data through a variety of filters. They analyze the ports used by the data, the addresses through which the data flows, the data characteristics and the data protocols and types.

Firewalls are an important element to be implemented on any computer connected to the Internet. Hackers and perpetrators constantly reinvent themselves by looking for security loopholes to exploit. Once the perpetrator gains access to our computer, he can use the computer to his advantage, which includes stealing PII. A targeted computer may even be used as a thoroughfare to deliver spam. A firewall is designed to protect our computer from such attacks.

Personal firewalls have become increasingly popular, and many more people consider whether to use them. Yet, there are many misconceptions and misunderstandings about personal firewalls, what they do, what they cannot do, how to configure them correctly and how to understand them correctly.
7.2.3.1. Benefits of Using a Firewall

The benefits of employing a firewall are that we can rest assured that our personal information is not broadcast to the rest of the World Wide Web and the risks of virus infections will be mitigated. Firewalls provide levels of intrusion detection sometimes prompting us as to which action to take, configuring inbound and outbound connections.

7.2.3.2. A False Sense of Security

Although we may have the misconception that the firewall will and can protect our system from malware, intrusions and various security threats, it should not be considered a replacement for anti-virus and anti-spyware programs. A fully and regularly updated anti-virus program plays a much more significant role in protecting our home computer than a personal firewall.

7.2.3.3. Firewall Programs [SecurityFocus. 2007]

First off, Windows XP and Mac OS X both come with their own built-in firewalls, so if a user runs one of those operating systems, they already have a very basic firewall installed (but likely not turned on).

Popular freeware firewalls include Zone Alarm, Kerio Personal Firewall 2, and Agnitum's Outpost. Other firewalls that are either inexpensive and/or have free trials include Norton Personal Firewall, Black ICE PC Protection, McAfee Personal Firewall, and Tiny Personal Firewall.

The concepts of inbound vs. outbound filtering, application integrity, computer anonymity, firewall limitations, why firewalls are our responsibility, 10 false statements about firewalls, and false claims about hiding the computer are discussed in detail in Appendix 6 (4.1. – 4.6.).

The benefits of using a firewall, a false sense of security and available firewall programs were discussed above. Another concept closely related to that of hiding the computer (discussed in Appendix 6 (4.7.)) also enables us to protect our identities.
7.2.4. Protect Our Identity
[Anonymizer. 2008a, b, c]

Privacy issues are on the rise with victims surrendering their PII, credit card and password information unknowingly. An estimated 90% of computers are infected with spyware.

Because spyware technologies are becoming more advanced each year, anti-virus, anti-spyware and firewall solutions are not enough to keep cybercriminals from gathering PII.

The truth is that cybercriminals know who we are. Just by visiting a Web site our geographical information, browser used, operating system, IP address and cookie, information is gathered (see Figure 8). This poses a threat because the victim can locate and track down his next victim. Alternatively, the information can be used to determine which types of attacks will best work on the victim’s computer based on security vulnerabilities in the software installed on the machine.

7.2.4.1. Anonymizer Software Packages

Anonymizer is a software solution protecting a user’s online privacy and identity. Its main goal is to secure financial and sensitive information and prevent it from falling into the wrong hands using the latest technologies.

“Anonymizer Anonymous Surfing combines the protection of rotating anonymous IP addresses with the security of 128-bit SSL technology” [Anonymizer. 2008a]. Anonymizer specializes in products to prevent phishing, pharming, spoofing or hijacking an Internet connection. The product protects us from online identity theft and keeps the IP address private at all times, preventing hackers from building profiles on Internet activities (see Figures 8-10). It warns us before visiting unknowingly malicious Web sites. Anonymizer also provides a shield to keep us secure from even the most complex methods of online spying and interception. More information on the Anonymizer product range can be found at http://www.anonymizer.com/consumer/products/prod_matrix/.

7.2.4.2. Features of the Anonymizer Product Range
[Anonymizer. 2008b, c]

- Anonymous surfing
- Protects our connection with SSL encryption
• Encrypts our connection with Secure Shell (SSH) tunnelling
• Alerts us to phishing scams
• Protects against pharming sites
• Safeguards our wireless activities
• Detects and removes spyware
• Stops spyware from downloading to our PC
• Enables us to whitelist sites
• Schedules spyware scans
• Encrypts online communications
• Protects against spam
• Provides anonymous and disposable e-mail addresses
• Integrates seamlessly with our current e-mail
• Blocks pop-ups
• Removes cookies from our Internet browser
• Deletes Internet history
• Clears cache files
• Deletes unused files
• Provides an extra security layer with our anti-virus and firewall solutions

**Figure 8.** Information gathered by Web sites without our knowledge or consent

Figure 8 is a screenshot displaying a summary of the information that may be gathered by Web sites we visit. Such information includes our IP address, location, operating system, Web browser and cookies. Figures 9 and 10 show how easy it is to locate where we are connecting from, including our latitude and longitude.
coordinates. However, with Anonymizer turned on, the information gathered is not the accurate data (see Figure 9).

FIGURE 9. Information gathered With Anonymizer turned on

FIGURE 10. Information gathered with Anonymizer turned off
A free trial version of the Anonymizer software can be downloaded from http://www.anonymizer.com/consumer/products/trial/sss_trial.html. The product features included in this free trial version will protect our personal e-mail address from spam, protect our identity online, detect and remove spyware, including all cookies, cached files and history archives.

More details on Anonymizer can be found at http://www.anonymizer.com/.

A more technical discussion on the Anonymizer software package, not found on the Anonymizer Web site, is provided in Appendix 6 (section 5). Please note that at the time of writing, running Anonymizer and Firefox v. 3.0. beta 5 at the same time caused Firefox to crash.

## 7.2.5. Secure and Recommended Internet Browsers

Facades are not always what they seem on the Internet and using the right browser will help protect us from spyware, intruders, scammers and spammers.

The most commonly used Internet browser is Internet Explorer (IE) because it comes preinstalled with every version of Windows and is employed by a larger user base. It is therefore at a greater risk of being infected with spyware and faces exposure to security vulnerabilities such as ActiveX.

In most cases it is uneconomical for attackers to target users using a different Internet browser. This does not mean that browsers other than IE have not suffered their own security vulnerabilities, but keeping in the minority ensures greater security.

Because Mozilla Firefox is used by a minority of the Internet market and offers the most enhanced security technologies, it is the most desirable when security is a top priority. The security levels of Mozilla Firefox Internet browser are discussed in Appendix 6 (6.1. – 6.3.) in detail. Mozilla Firefox was chosen for this discussion because it is also compatible with various operating systems such as Linux, Windows and Mac OS X. Web browser usage statistics are also provided in Appendix 6 (6.4.) to help us select which browser may be the most secure based on the usage statistics. The latest versions of the preferred Internet browser are available as a free download from the manufacturer’s Web site.
Using the Latest Internet Browser Securely

An Internet browser is used to display a desired Web page on our screen. The latest release always uses the latest encryption technology. The encrypted data is then decrypted by the server. We must make sure we are connected using an SSL connection (see Appendix 2 (2.6.)). We can do this in two ways:

- In the URL http should change to https.
- In the status bar of our browser window we should have a padlock icon (the latest browser at the time of writing has the padlock icon at the top right of the browser next to the URL). This icon ensures that we are in SSL mode. Whenever visiting an online transaction Web site we must always look for the padlock icon in the browser window.

Another concept related to Mozilla is the Thunderbird e-mail client, putting great emphasis on the security offered through Thunderbird.

7.2.6. Secure E-mail Clients [Mozilla. 2005-2008a, b]

Similar to the Firefox browser, Mozilla Thunderbird is an e-mail client offering greater security owing to its use by the minority. Security and privacy measures integrated within Thunderbird ensure that our identity and communications remain secure. The program can be used on Windows, MAC OS X and Linux to prevent spam, provide phishing protection and robust privacy. These concepts are discussed in more detail in Appendix 6 (7.1. – 7.5.).

7.2.7. Updates and Patches

As a rule of thumb, it is always important to download the latest updates and patches released. The latest updates ensure that any security loopholes are fixed in an effort to mitigate potential risks and security threats that may compromise our computer.

7.2.8. Encryption Mechanisms

“Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting
encrypted data back into its original form, so it can be understood” [TechTarget. 2003-2008a]. The purpose of employing encryption techniques is to maintain the confidentiality and integrity of data sent and received between two parties.

Encryption methods can be categorized into two main groups, namely symmetric and asymmetric encryption [Hitek Software LLC. 1999-2008]:

1. **Symmetric encryption:** The same key is used for encryption and decryption of the same data file. It is recommended that this technique be used for personal use only and that the password not be shared with anyone else. This technique is also known as password based and secret-key based encryption.

2. **Asymmetric encryption:** Different keys are used to encrypt and decrypt data. The public key which is known by everyone is used to encrypt the file but can only be decrypted using a private key – a key only we should have access to. The public key can be sent to anyone who needs to send data to us.

More information on encryption with symmetric and public keys is provided here: [http://www.pcstats.com/articleview.cfm?articleid=252&page=3](http://www.pcstats.com/articleview.cfm?articleid=252&page=3)

Another reason to use encryption is to prevent any sniffing programs from accessing usernames and passwords, which may be installed somewhere between the client and remote computer. FTP and telnet are examples of such programs that send usernames and passwords for authentication over the Internet without any encryption. If we do not have the option to use such encryption mechanisms, the best thing is to change the passwords regularly [Paz, U. 2002].

7.2.8.1. **Instant Messaging Encryption Techniques**

Like online transactions, the messages we send and receive over instant messaging (IM) applications such as IRC can be intercepted and read by an unknown third party. Instant messaging can compromise our privacy and may become a risk. For this reason, it is important to note what not to send over messaging lines.

7.2.8.2. **IM Golden Rules**

Golden rules to note of what not to do when conversing over the Internet:

1. **Never send credit card or personal details** over any chat client, irrespective of whom we think we may be dealing with.
2. **Never accept unknown files the other party may be sending.** These files may contain viruses such as Trojans, key loggers or spyware, and can infect the computer compromising sensitive data residing on the hard drive or data keyed-in by us.

### 7.2.8.3. Encrypting Messages in IM [Pidgin. 2008]

Pidgin is an IM program freely available to those who want a secure online environment to converse in. Pidgin allows us to use multiple IM programs simultaneously based on a multi-protocol system.

It is available for all platforms, including Windows, BSD, Linux and other UNIX OS.

The Pidgin plug-in uses RSA encryption and transparently encrypts all messages sent (and received) through instant messaging (see Figure 11).

The plug-in features are listed in Appendix 6 (section 8).

The Pidgin-Encryption plug-in and Pidgin IM software can be used with AIM, ICQ, Jabber/XMPP, MSN Messenger, Yahoo!, Bonjour, Gadu-Gadu, IRC, Novell GroupWise Messenger, QQ, Lotus Sametime, SILC, SIMPLE, MySpaceIM, and Zephyr.

**FIGURE 11.** Automated encryption with Pidgin-Encryption

Pidgin is licensed under the GNU General Public License (GPL) version 2, meaning that the software is free to anyone who wishes to download and use it. To download
7.2.9. Other Encryption Mechanisms and Techniques

Encryption mechanisms and techniques not yet described feature in Appendix 6 (9.1. – 9.5.). The encryption mechanisms are included for users interested in the more technical solutions available. These include SSH, Single Sign-On, Kerberos Authentication, VeriSoft and Secure IMAP (Internet Message Access Protocol) vs. POP (Post Office Protocol). The most popular encryption mechanism to ensure integrity of data in transit is known as PGP.

**PGP (Pretty Good Privacy) [Georgia Institute of Technology. 2002]**

PGP has been widely adopted for its uses in ciphering a message delivered over networks. The risks of an important message being intercepted, or altered during transit have been publicized, which resulted in a call for security measures.

PGP ensures message integrity, confidentiality and authenticity. One of PGP’s major uses is in e-mail encryption to ensure that only the intended recipient can decrypt the content of the message. Another use of PGP is to verify that the message came from whom the message says it is from and to further encrypt files stored on the local hard drive.

PGP is compatible with Windows, MAC OS X and UNIX. Additionally, messages can be interchanged from one platform to another.

For more information on PGP visit: [http://www.pgp.com/downloads/research_reports/index.html](http://www.pgp.com/downloads/research_reports/index.html)

Beware of fake encryption software advertised in and around the Web. Examples of such programs are Cryptainer LE and Autokrypt.

7.3. Summary

The main purpose of this chapter was to provide a general outline of which technical and non-technical preventative measures are available that may be used to advance security. The use and implementation of multiple security mechanisms and programs for added protection were explained. The most common and most important security mechanisms were discussed in this chapter.

The development sector (namely the ISAP) presents downloads and easy-to-access information to promote user awareness in the World Wide Web.
Part V

ISAP Discussion and Conclusion

Chapter 8

ISAP Overview
Part I
Dissertation Outline
Chapter 1: Introduction and Background

Part II
Prologue to the Internet and Internet Transactions
Chapter 2: Computers and the Internet
Chapter 3: Internet Transactions

Part III
Compromise of Sensitive Information
Chapter 4: Introduction to Online Fraud and Finding Personal Information Techniques
Chapter 5: Modus Operandi (MO) Techniques for Committing Online Fraud
Chapter 6: Preventing MO Subterfuge

Part IV
General Preventative Measures
Chapter 7: Non-technical and Technical Preventative Measures

Part V
ISAP Discussion and Conclusion
Chapter 8: ISAP Overview
Chapter 9: Conclusion
To say that we are at risk IS AN understatement.

Chapter 8
ISAP Overview

8.0. Overview

The Information Security Awareness Portal (ISAP) is designed to facilitate the accessibility of the information provided in this dissertation. To provide complete user awareness the portal will be accessible at three different levels, the first level being the most basic one as an introduction to the various risks to accommodate even the least unaware person. The look and feel of the ISAP must exhibit simplicity and its use must be self-explanatory.

This chapter introduces the software requirements to be able to view the ISAP, the different aspects and functionality of the ISAP, as well as the different technologies used in its development.
8.1. Software Requirements to View the ISAP

The ISAP consists of a Web site which can be accessed online. To be able to view the Web site the following are needed:

- A computer with Internet access
- A Web browser (such as Internet Explorer 7 or Firefox version 3.0.2) which is Flash and JavaScript enabled
- Macromedia Flash Player

Once the relevant requirements have been met, the Web site and its functionality can be viewed and used.

8.2. Overview of ISAP Functionality

When the Web site is first loaded, it will display the home page (see Figure 12). The Web site can be accessed at http://www.securityportal.co.za (this link is temporarily available and may be subject to change). The home page presents us with a 3D carousel, a link bar and the page contents. The 3D carousel and the link bar remain consistent on all pages.
8.2.1. The 3D Carousel

The function of the carousel is to draw our attention to the most important aspects from a security point of view.

The 3D carousel featured in the banner of the page rotates clockwise or anti-clockwise according to left or right mouse movement. The further the mouse is moved in either direction, the faster the carousel rotates. This is effective for user interaction and to highlight important aspects. When the mouse hovers over one of the icons, a message is displayed about the icon (see Figure 13).

Furthermore, the carousel serves as a mini Flash site. When a user clicks on an icon, the carousel zooms out and presents the relevant awareness citation which has been featuring in this literature (see Figure 14). When the user clicks on the icon, they return to the carousel. This approach is effective to draw their attention to important security aspects highlighted in this dissertation, especially for those who do not wish to read chapters of information.

**FIGURE 13.** 3D carousel in the banner of the page

**FIGURE 14.** 3D carousel serves as a mini Flash site

Internet Causes Risks to Our Finances
8.2.2. The Link Bar

The link bar presents the different key sections. These links include Home, The Internet, Online Transactions, Risks and MO, Countermeasures and Downloads.

8.2.3. The Home Page Contents

The contents of the home page (see Figure 12):

- Provide an introduction to the ISAP.
- Provide three of the many risks identified in the literature. Each of these concepts is introduced briefly, and should the user wish to read more, they can click on the link entitled “Read more”, which will redirect them to the relevant page.
- Provide the security cartoons section, which introduces the portal’s cartoon character and simultaneously provides a security cartoon featured from the literature.

8.2.4. The ISAP Web Page Contents

The other key sections besides the home page consist of a slightly different content layout (see Figure 15).

The content layout presents a collapsible panel on the left. When the user clicks on one of the tabs, the corresponding subheadings will slide open or closed. When the user clicks on one of the subheadings, they are redirected to the corresponding section.

The centre of the page contains the relevant content about each topic featuring at the current time. Where there is a link within the content, it will redirect the user to the page providing more detail about that particular topic when clicked on. This is level 2 of the contents described in Chapter 1.

The cartoons panel on the right randomly presents a cartoon strip presented in the literature every time the page is reloaded. The same approach applies to the cartoon character, which will also randomly display important security messages. This approach is effective to draw the user’s attention and create awareness of important security aspects.
When the mouse hovers over the cartoon strip, an enlarged image will be displayed next to it (see Figure 16). The thumbnail image of the cartoon strip saves space and does not detract attention from other aspects of the site, while user interactivity is encouraged by displaying the larger version.

The rest of the key links featuring in the link bar follow a similar approach described in this section. The technologies used during the development of the design, contents and layouts of the ISAP play an important role in its ease of use and functionality.

8.3. Technologies used to Develop the ISAP

The technologies used to develop the ISAP were the following:

- **Adobe® Dreamweaver® CS3 version 9.0**
  - To construct the initial layout of the Web page and integrate Spry technologies for the collapsible panel.
- **Adobe® Flash® CS3 Professional version 9.0**
  - To create the Flash banner and the 3D carousel.
- **Adobe® Fireworks® CS3 version 9.0**
  - To create and export the graphics needed to display the Web page correctly, such as the background and the icons featuring in the 3D carousel.

**FIGURE 16. Enlarging the ISAP cartoon strips**

- **CorelDRAW® X3 version 13.0**
  - To plan the layout as well as the look and feel of the Web page.
  - To create certain graphics needed to display the Web page correctly, such as the cartoon character.

- **Corel® PHOTO-PAINT® version 13.0**
  - To create certain graphics needed to display the Web page correctly.

- **MySQL 5.0**
  - To store content data of the Web site.
  - To effectively maintain and store content data of the Web site. A database allows for easier maintenance should the content change.

- **Microsoft® Visual Web Developer® 2008 Express Edition version 9.0**
  - To develop the final stages of the Web site.
  - To create the integration between the Web site and the database.
• **Microsoft .NET Framework version 3.5 SP1**
  o To enable the use of Microsoft® Visual Web Developer® 2008 Express Edition as well as the Visual C# language.

The relevant languages used to develop the ISAP:

- Cascading Style Sheets (CSS)
- XML (eXtensive Markup Language)
- HTML (HyperText Markup Language)
- ActionScript 2.0.
- JavaScript
- ASP .NET (Active Server Pages)
- Visual C# Programming Language

The ISAP provides some value to each person reading the contents of the portal from the most basic level to a more detailed level. The technologies used to develop the Web site allow for the creation of the ISAP. Awareness is created through the ISAP to a large audience and community of people, from the average person to the educated business person. This is achieved through a simple, yet impressive look and feel of the portal encouraging user interactivity.

### 8.4. Summary

The relevant technologies used to develop the ISAP, the overview of ISAP functionality as well as the software requirements needed to view the ISAP were discussed. The next chapter summarizes the different security aspects discussed in the dissertation.
Part V

ISAP Discussion and Conclusion

Chapter 9

Conclusion
Part I
Dissertation Outline
Chapter 1: Introduction and Background

Part II
Prologue to the Internet and Internet Transactions
Chapter 2: Computers and the Internet Transactions
Chapter 3: Internet Transactions

Part III
Compromise of Sensitive Information
Chapter 4: Introduction to Online Fraud and Finding Personal Information Techniques
Chapter 5: Modus Operandi (MO) Techniques for Committing Online Fraud
Chapter 6: Preventing MO Subterfuge

Part IV
General Preventative Measures
Chapter 7: Non-technical and Technical Preventative Measures

Part V
ISAP Discussion and Conclusion
Chapter 8: ISAP Overview
Chapter 9: Conclusion
Malware is a serious issue that must be addressed alongside viruses, worms, spam and other threats, but one that many organizations focus on less than they should.

—Osterman Research
Chapter 9
Conclusion

9.0. Overview

Because the Internet is an intangible medium it entails risks to whoever enters it, and more so to the users who are unaware of these risks.

The question is how the issues of risk, identification and trustworthiness can be transferred to cyberspace effectively. Not knowing how the World Wide Web operates in cyberspace causes issues which need to be clarified and addressed. The operation of the World Wide Web in this dissertation have been clarified and addressed, allowing us to understand and perceive the underlying mechanisms of a typical Internet transaction.

Because online institutions neglect to educate the average user, we tend to become a risk to ourselves. We are casually granted online access to online banking accounts without any prior knowledge of the risks involved and what consequences could arise. The continuing technological development of cyberspace raises issues directly related to our privacy, safety and security.

The issues of privacy, safety and security have been addressed and risks have been explained for us to be able to identify an Internet scam and what to do to identify a security risk. The different types of risks illustrated by the fraudsters’ MO give insight into how to better protect our privacy, identities and sensitive information from various Internet schemes.

The problem statement has therefore been addressed as this dissertation promotes user awareness as well as solutions and preventative measures to use the Internet securely. The ISAP and dissertation cover the risks involved in the Internet, but there still remains some opportunity for further research and development in the future.
9.1. **Research and Development Opportunities**

As technology continues to change and develop at a rapid rate, the ISAP may need to be maintained accordingly. Such technology may include:

- Security software packages such as anti-virus programs may need to be developed as they evolve in an attempt to keep up with rapid infections.
- Links and downloads to external sources may need to be reviewed and updated to ensure that each link remains valid.
- New and more effective technologies which may develop in future may be used to keep up to date with maintaining the Web site on a technical level, allowing for (hopefully) quicker and easier access for us.
- A forum could be created to allow victims or users with security concerns to post their opinions and request any assistance. This forum may be used by the community to promote any awareness workshops that may be taking place.
- A blog for each user registered on the system could be formed so that they can express any security concerns, opinions or experiences they may have encountered. The content may need to be reviewed before allowing the post to take place for any content not directly security-related.
- An agent may be developed that searches the Internet for any articles concerning identity fraud and security-related issues.

As criminals continue to reinvent themselves, new Internet schemes and MO develop. The promotion of awareness and countermeasures for each developing risk may need to be updated or added. A more technical approach of the underlying hardware and software mechanisms may be discussed and added into the dissertation or portal for the more technically savvy.
References

Some references listed in this section also apply to the Appendix.


References


Krebs, B. 2006. It’s 10PM. Do you know where your identity is? Popular Mechanics, 01 March, 26 – 33.


References


Tanase, M. 2003. IP spoofing: An introduction. Available from: 

Technews Publishing (Pty) Ltd. 2007. Spyware and viruses - two separate problems requiring separate defences. Available from: 

<http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html> [Accessed: 01 June 2008]


The Mercury. 2008. How to stop e-scammer’s con tricks. Available from: 


Further Reading

Some references listed in this section also apply to the Appendix.


Further Reading


Appendix 1

Part II

Prologue to the Internet and Internet Transactions

Chapter 2

Computers and the Internet

Section 1 – Prologue to the Internet


The abacus was an invention used for computing calculations, about 5000 years ago in Asia Minor. This device was made of sliding beads arranged on a rack and was used by early merchants for trading transactions. The abacus was a part of rare ancient history and is still in use in some countries today. Geographic studies show that the abacus has been examined extensively and various mechanical versions have been developed.


The next great gadget surfaced in France in 1642. A French tax collector’s 18-year-old son, Blaise Pascal (1623-1662), invented a so-called numerical wheel calculator. The brass rectangular box was named after him and
was also called a Pascaline. The Pascaline was to help the inventor’s father with his tasks. It had eight movable dials to add sums up to eight figures long and used a base of 10 to achieve this.

1.3. 1694: Improvement of the Pascaline [Gromov, G. 1995-2003]

Further developments were made in 1694 by creating a Pascaline that could also do multiplication. This was achieved by a German mathematician and philosopher, Gottfried Wilhem von Leibniz (1646-1716).


As research progressed over decades, the more sophisticated early computer was developed in 1822. This piece of machinery performed differential equations and was called the difference engine, designed by a mathematics professor Charles Babbage (1791-1871). The difference engine was a large locomotive-sized steam machine which would automatically calculate mathematical tables. It had a stored program and could print the results automatically. The difference engine held Babbage’s attention for approximately ten years and then he created a new improved analytical engine – the first general-purpose computer.

Introducing the analytical engine for public use could not have been done without the help of Babbage’s assistant, Augusta Ada King, Countess of Lovelace (1815-1842), also the daughter of the English poet Lord Byron. She was one of the few people whose knowledge could help revise plans and organize funds from the British government. Lady Lovelace’s fine understanding of the machine also helped to communicate specifics to the public. By creating instruction routines to be fed into the computer, she became the first female computer programmer.

The first general-purpose computer was intended to execute procedures present in modern-day computers such as sequential control, branching and looping.
The analytical engine was also intended to use loops of Jacquard's punched cards (see Figure 1) to control an automatic calculator, which could make decisions based on the results of previous computations [Maxfield and Montrose Interactive, Inc. 1998a]. The analytical machine was never completed.


Since the US census in 1880 took nearly seven years to count, and owing to the large population growth, an American inventor Herman Hollerith (1860-1929) created a quicker and easier way to compute the census. Hollerith’s idea worked differently from Babbage’s punched card idea. His method used cards to store data information such as census results, which he fed into the machine and the census results were arranged mechanically. It was to become the first really large-scale practical invention of the computer.

A single card could store as many as 80 variables, where one number was represented on a card and combinations of two punches represented one letter.

Census officials compiled the results in six weeks with Hollerith’s machine, compared to the proposed ten years. Punch cards also helped reduce computational errors owing to their storage method for data.

Hollerith’s punch card reader was so successful that he introduced it into the business world, founding Tabulating Machine Company in 1896, later to become International Business Machines (IBM) in 1924 after a series of mergers [Gromov, G. 1995-2003].

In 1928, Hollerith’s company introduced the rectangular hole 80-column format (see Figure 2), almost doubling the amount of data that could be recorded on a card, and by the mid-1930s, IBM was predicting that round-hole cards would soon be things of the past [Jones, D.W. 2006].

FIGURE 2. IBM’s rectangular hole 80-column format punched card I [Maxfield and Montrose Interactive, Inc. 1998]

Until the 1960s, punch cards for data processing had been used in both business and government industries. In the business sector, other companies such as Remington Rand and Burroughs also manufactured the punch cards.


This procedure was developed in 1931 by Vannevar Bush (1890-1974). The machine was awkward as it consisted of hundreds of gears and shafts to represent the various numbers and their associations to one another. The machine could solve complex differential equations like no mathematician was able to do before.

The bulkiness of the differential calculator was eliminated by an approach that was based on the mid-19th century work of George Boole (1815-1864).

An algebraic binary system, known as Boolean Algebra, where any mathematical equation could be stated as true or false, was clarified by and named after Boole. This theory had been applied in much the same way to electronic circuits in the form of either on or off. John V. Atanasoff (b. 1903), a professor at Iowa State College (now called Iowa State University) and his graduate student, Clifford Berry, applied Boole’s theory to create the first all-electronic computer by 1940. Similar advances were made by other scientists since the project had lost its funding and was discontinued.

On the other hand, the all-electronic computer succeeded in 1944 in creating ballistic charts for the US navy. The success was captured by a Harvard engineer working with IBM, namely Howard H. Aiken (1900-1973).

Another computer development called the Electronic Numerical Integrator and Computer (ENIAC) was a massive piece of machinery which consumed enough electrical power (160 kilowatts) to restrain the power in an entire region of Philadelphia, the largest city in Pennsylvania. The project, encouraged by the war, was created by a partnership between the US government and the University of Pennsylvania and consisted of 5 million soldered joints, 70 000 resistors and 18 000 vacuum tubes.


Even more sophisticated and advanced computer designs were implemented in the mid-1940s by John von Neumann (1903-1957), who had joined the University of Pennsylvania team. The conditional control transfer and stored memory functions allowed a computer to be stopped at any point and then resumed. The EDVAC allowed for greater robustness in computer programming. The central processing unit and other concepts initiated by Von Neumann remained within the architecture of computer design for the next 40 years. Owing to the versatility of the central processing unit, all computer functions could be coordinated through a single source.

The computer was an enormous device in the 1950s and occupied a vast amount of space. It used magnetic tape and punch cards to execute commands.


The beginning of all global telecommunications began with the first earth satellite which was launched by the USSR (Union of Soviet Socialist Republics commonly called the Soviet Union or Russia) in 1957 during the Cold War (see Figure 3).

In response to the development of the satellite and to gain an advantage in science technology, the Advanced Research Projects Agency (ARPA) within the Department of Defense (DoD) was established by the US.

![Sputnik satellite](image_url) **FIGURE 3. Sputnik satellite [Strickland, J. 1998-2008]**

The US DoD was to create a network and communications infrastructure so that if one path was destroyed, there would be another alternative route for communication and hence, the ability to survive a nuclear attack. The main challenge was to connect four computers through a network each using different operating systems. Protocols were used to enable different types of computers to communicate flawlessly.

The network was to be called ARPANET and formed the foundation of the way in which the Internet is interlinked and communicates across the globe today.

Computers became smaller and more sophisticated through the invention of the transistor by 1948, which greatly changed the computer’s development. In 1972, Intel introduced the first commercial 8-bit microprocessor, which was able to process 60,000 instructions per second and accessed 16KB of memory - its 200 KHz 8008 chip.


In 1973, different options were analyzed by engineers to connect ARPANET to the PRNET. The PRNET used radio transmitters and receivers to connect computers. Instead of sending data across telephone cables, the computers used radio waves. The objective was for military purposes to ensure security when transferring information over networks.


In 1976 the Apple Computer Company was formed by Steve Wozniak and Steve Jobs. After completing some additional work on a computer circuit board, they called it the Apple I Computer.

In 1977 Bill Gates and Paul Allen officially created Microsoft Company. This partnership was formed a couple of months after Apple reached a high goal with the first computer.

1.15. 1977: Satellite Network (SATNET) [Strickland, J. 1998-2008]

In 1977, the SATNET was connected to the other two networks. The expression “internetting”, or “Internet” for short, was used to classify the connection between multiple networks. Other early computer networks such as USENET, BITNET, CSNET and NSFNET also soon joined.

When the first hard drive hit the market in 1980, this was to mark the growth development of humankind’s artificial memory. The first hard disk was the Winchester 5.25-inch hard disk drive proclaimed by Seagate Technology. It used four platters, held 5MB and cost US$600.

Apple then went public. In 1980, a total of 327 000 personal computers were sold. In 2000 alone, more than 140 million machines were sold.

1.17. 1983: Domain Name Systems (DNS) [Brain, M. 1998-2008]

As the Internet grew, a text file was used by the Network Information Center to map a name to an IP address. In 1983 the Domain Name System (DNS) was created by the University of Wisconsin to automatically link the names to their corresponding IP addresses. Instead of having to remember numbers such as 192.72.39.281, a person may type something like www.uj.ac.za to retrieve the correct Web page. An address such as www.uj.ac.za is also known as a uniform resource locator (URL), while uj.ac.za is known as the domain name.


The World Wide Web (WWW for short) was developed by Tim Berners-Lee in 1990. The system was to simplify navigation on the Internet; a massive interconnection of computer networks.

Government and military employees, graduate students and computer scientists were among the early Internet users. The advent of the WWW allowed colleges, universities and businesses to connect more openly to the Internet.


A non-profit group established in 1992, called the Internet Society, formulates the policies and regulations that define how the Internet should be used. There is a great
need to be able to control and apply laws dealing with misconduct on the Internet. Because people exploit this fact, crimes such as identity theft occur repeatedly.


The first graphical Web browser allowed text, graphics, sounds and other multimedia to be viewed in a single document and was known as Mosaic (see Figure 4). Mosaic was developed in 1993 by Marc Andreessen of the National Centre for Supercomputing Applications (NCSA). The Mosaic development helped revolutionize the Web and demonstrate its potential. It helped shape the WWW into what we know it today.

![Figure 4: Screenshot of the world's first graphical web browser](image)


Through the advent of the satellite which once orbited above the earth’s surface, the Internet has become more complex than ever before. Computers, satellites and mobile devices, amongst other gadgets, are all connected by the internet, which is now a massive network a million times more intricate than the original ARPANET.

Several organizations and committees, such as the Internet Activities Board, Federal Research Coordinating Committee and the Federal Networking Council, have established rules and standards to govern the use of the Internet today as well as ensure that the different types of networks are able to connect flawlessly.

Although these rules have been and are continually implemented, the greatest challenge in the Information Age is managing and controlling the Internet. People
exploit the Internet to their own advantage, leading to various risks. See Chapter 5 for more information about risks.

As satellites play an important role in transmitting data today, the modern computer serves as a tool to enable us to gain access to the Internet. The Internet widely contributed to globalization, resulting in growing pressure to formulate rules and regulations governing the laws of the Internet in the Information Age.
Section 1 – Types of Electronic Payments

1.1. Types of Electronic Payments [Hord, J. 1998-2008] (Chapter 3 (3.1.3) p. 33)

An electronic payment does not involve any kind of paper money or paper cheques to complete a transaction. It may consist of any kind of non-cash transaction which may involve credit and debits cards as well as the Automated Clearing House (ACH) network (a definition is provided in Appendix 2 (1.2)). Direct deposits and debits as well as electronic cheques comprise the ACH system. The different types of electronic payments may fall into three main categories, namely once-off e-payment (customer to merchant), recurring e-payment (customer to merchant) and automatic e-payment (bank to merchant).

1.1.1. Once-off e-payment (customer to merchant)

This occurs when shopping online on an e-commerce Web site where credit card information is entered and the purchase is processed almost instantly. Alternatively, an electronic fund transfer (EFT) can be issued through online banking to secure an order. Another option is to pay by e-cheque, where we (the customer) enter our banking details (such as account number) and the merchant authorizes payment through the
customer’s bank. The customer’s bank initiates the EFT or prints a cheque and mails it to
the merchant.

1.1.2. Recurring e-payment (customer to merchant)

This is commonly initiated by insurance, telephone and loan management companies or
long-term contracts such as fitness centres. A payment schedule is regularly initiated
when automating a direct debit or charge to the credit card.

1.1.3. Automatic e-payment (bank to merchant)

This occurs when our bank allows online Internet banking. When we log in to authorize
the bank to initiate an EFT, money is transferred from our account into the merchant’s
account. We may also choose to pay the bills automatically on the same day of each
month.

1.2. The National Automated Clearing House Association (NACHA) [NACHA. 2008]

A potential source of information is the NACHA, also known as the Electronic Payments
Association.

NACHA is a not-for-profit association that oversees the ACH network, one of the largest
electronic payment networks in the world. More than 18 billion ACH payments were
exchanged in 2007. More information on NACHA can be found at www.nacha.org
[NACHA. 2008].
Section 2 – Are Secure Transactions Really Secured?

2.1. What an SSL Certificate Does Not Do [Newsreader. 2001-2004] [Locke, J. 2004] (Chapter 3 (3.4.2) p. 38)

Similar to a domain name, anyone can get a certificate. Acquiring a certificate is easy and the costs vary depending on the certificate authority (CA). A valid certificate therefore does not guarantee that a Web site is a legitimate one.

The correct Web address in the address bar can be spoofed (more on spoofing in Chapter 5) to display the correct Web address in the address bar, when it is in fact the incorrect Web address leading us to a fraudulent Web site. This is because a certificate does not authenticate the Web site itself, but rather the URL of a matching known certificate. A URL is the address which appears in the browser’s address bar.

2.2. What an SSL Certificate Does Do [Locke, J. 2004] (Chapter 3 (3.4.2) p. 38)

Authentication is the main purpose of an SSL certificate. A CA can be created by anyone but the digitally signed certificate must be built into Internet browsers. The browser should display a warning if it does not recognise the CA. In other cases, a warning should also be issued when the DNS server has been hijacked and is visiting a fraudulent Web site.

The CA validates the certificate to ensure that the Web site is legitimate and is authorized by someone we trust.

2.3. Who Do We Trust? [Locke, J. 2004] (Chapter 3 (3.4.2) p. 38)

Certificates are built into an Internet browser or operating system (such as Windows, or Linux). Companies such as VeriSign, GeoTrust and Thawte have an agreement with the developers of the specific Internet browser to preconfigure their certificates. A warning will be issued if the CA is not preconfigured or recognized by the Internet browser. The “chain of trust” of signing authorities can be viewed when analyzing the details of an SSL
certificate. Details on how to view the validity of a certificate in Mozilla Firefox are explained next.

2.4. Checking a Certificate [Locke, J. 2004] (Chapter 3 (3.4.2) p. 38)

Checking a certificate is useful to determine whether the Web site being viewed is legitimate and not forged by hackers. In Mozilla Firefox, double-click the lock icon in the bottom right-hand corner and a window will be displayed (see Figure 5):

- Under the Security tab in Page Info: the View Certificate button can be clicked to view the certificate (see Figure 6).
  - Under the General tab in Certificate Viewer: contains details about the owner of the certificate, the issuing CA and validity dates. The Internet browser compares the domain name in the URL to the common name (CN) (refer to Figure 7). Check for any strange characters such as “^” or “%” symbols.
  - Under the Details tab in Certificate Viewer: the certificate hierarchy pane displays the “chain of trust”. The first item in the list is the trusted CA preconfigured into the browser. Furthermore, each item in the certificate hierarchy is a certificate. The first one listed is the one to trust. There can be up to four certificates in the chain and each
Appendix 2

certificate has signed the next, validating that it is legitimate. By selecting a particular certificate, more information can be viewed. The last one in the list belongs to the server the user is visiting (refer to Figure 8).

**FIGURE 6.** View Certificate button in Page Info

**FIGURE 7.** Viewing the certificate under the Details tab in Mozilla Firefox

**FIGURE 8.** Viewing certificate information under the General tab
2.5. How Reliable is this System? [Locke, J. 2004] (Chapter 3 (3.4.2) p. 38)

At this point in time, an SSL certificate cannot be forged. However, the easiest way to break the system is through spyware techniques. The Internet browser can be told to trust whatever we are told to trust by installing a malicious certificate from an illegitimate CA. Attackers could hack into a legitimate CA and digitally sign fraudulent certificates. Another possibility is if someone can break the encryption system using a new mathematical technique. If this happens, the entire e-commerce infrastructure would collapse. This is a possibility, but not necessarily a feasible scenario.

2.6. What is SSL? [Garfinkel, S. Spafford, G. 1997: 233] [Locke, J. 2004] [Mencik, S. 1999] [Georgia Institute of Technology. 2002] (Chapter 3 (3.1.3) p. 33, (3.4.2) p. 38, Chapter 7 (7.2.5) p. 131)

SSL is a secure sockets layer between the raw TCP/IP and the application layer. SSL technology is an Internet protocol designed by Netscape Communications Corp. The purpose of SSL was to fragment, encrypt and compress the data to be transmitted. Data on the receiving end is decompressed, decrypted, verified and reassembled to be used with other applications. The intention is to secure the information transmitted via the Internet.

SSL adds numerous features to the clear, anonymous and error-free stream of information transferred via TCP/IP. These features include:

- Using digital signatures enabling the authentication and non-repudiation of the server and client.
- Using encryption to ensure data confidentiality.
- Using message authentication codes to ensure data integrity.
- Authenticating the server at the other end.

When the lock icon appears in the Internet browser, it means the connection is encrypted between the Web server and the client’s Internet browser. Encryption occurs when the data is sent from one computer to another; the data is hidden preventing compromise of information. Encryption is explained in more detail in Chapter 7, section 7.2.8. This technique takes place using SSL technology and is built into modern Internet browsers.
A concept called SSL Hello is when a program which uses SSL attempts a secure connection with a second party and compares which encryption mechanism is the strongest shared between the two of them.

TLS has slight important differences compared to the standard SSL 3.0. Instead of using the MD5 secure keyed message digest function, it uses hash message authentication code (HMAC) and has a slightly different cipher suite from SSL 3.0.

Section 3 – How to Set Up Secure E-commerce Payments for Your Business (Chapter 3 (3.4.2) p. 38)


There are two options when wanting to set up an online payment solution for a small business: Outsourcing the payment solution or doing it in-house.

3.1. Outsourcing the Payment Solution [Hord, J. 1998-2008]

Outsourcing the payment solution means that a processing fee per transaction is charged to the merchant’s account. Well-known third-party services such as PayPal and ProPay provide a convenient all-in-one solution.

When a buyer enters sensitive information onto the merchant’s Web site to complete a purchase, PayPal authorizes the transaction and transfers the funds to the merchant’s account. In this way, we are able to accept credit card details and other forms of electronic payments. Initiating a PayPal solution is discussed in Appendix 2 (4.1) and the following elements are discussed: how PayPal works, signing up for a PayPal account, issuing a purchase using PayPal, advantages and disadvantages of PayPal.

An alternative secure connection solution is to implement one in-house.
3.2. Processing Payments In-house [Hord, J. 1998-2008]

Processing payments in-house means that establishing a secure server is the top priority. Steps the potential online business can take to ensure its reputation and customer's security are as follows:

**Step 1: Establish an SSL Connection**

A secure server is a computer that uses encryption to make it difficult for intruders to intercept confidential information. SSL technology is used to encrypt the data and is done by means of applying for an SSL certificate. The application for an SSL certificate can be done online at [http://www.InstantSSL.com](http://www.InstantSSL.com).

**Step 2: Register with a Digital Authentication Service**

Once you have an SSL certificate, you need to register your site with a digital authentication service. The site receiving your customers' information is validated by use of a digital certificate and ensures that it is the correct one. Digital certificates assure customers that the site is legitimate and that sensitive information is encrypted.

**Step 3: Build or Buy Shopping Software**

Now that you have a secure server, you will need to build or buy shopping software that allows a customer to choose products from your site and add them to a virtual shopping cart. Customers click on a "checkout" link when they are ready to process the order. The link redirects the customer to your secure server, where they enter their credit card information.

**Step 4: Procure Software that Validates Your Customer’s Credit Card Information**

Finally, you need a system to process credit card payments and an Internet merchant account with a bank. Online companies such as VeriSign offer credit card payment processing services. These companies provide you with software that validates your customer's credit card information over your secure server. Some businesses may also opt to accept e-cheques.

PayPal was introduced briefly in Chapter 3, section 3.5.1. How PayPal works is explained in the following sections, beginning with how to sign up for a PayPal account.

4.1.1. Signing up for a PayPal Account

Signing up for a PayPal account is quick and easy – and free. From the PayPal home page, click on Sign Up to create your account (see Figure 9). From there you can choose what account type you would like, from a personal to a premier account. To use PayPal for the occasional transaction a personal account will do. To complete the sign-up process a confirmation e-mail will be sent to your e-mail address with further instructions.

Signing up for a personal PayPal account provides core features only, such as Send Money, Request Money, Auction Tools, Web Site Payments, Money Market, Virtual Debit Card, Account Insurance, E-mail Customer Service.

Supplying PayPal with a confirmed address indicates that you (or other third parties) are less likely to be a scam artist. This can be done by adding a valid credit card to the account. The credit card can be used for PayPal’s Expanded Use Service, allowing you to draw money from the credit card instead of just from a bank account.
PayPal is rich in features such as the PayPal Debit Bar, which is a free service. The PayPal Debit Bar can be used so that you can purchase using the funds in your PayPal account. This can be done when a Web site only accepts credit cards. The PayPal Debit Bar allows you to create a virtual MasterCard number and the funds will be deducted from your PayPal account.

Different packages are offered by PayPal, ranging from the standard package to the premium package. However, the two main account types, Standard and Pro, operate slightly differently:

1. **Standard account:** The customer logs into the PayPal Web site separately to complete his purchase (see Figure 10).
2. **Pro account:** The customer does not leave the merchant’s Web site while the transaction is processed in the background (see Figure 11).
“PayPal has quickly become a global leader in online payment solutions with more than 153 million accounts worldwide. Available in 190 markets and 17 currencies around the world...” [PayPal. 1999-2008].

Although PayPal is well-known as a trusted third party, there are some downsides to using PayPal as a trusted money source to process secure transactions.

PayPal acts as an extra security layer because it provides a service whereby funds remain in the PayPal account until the holder of the funds retrieves or spends them. The merchant does not see the sensitive information, such as credit card details, entered and sent to PayPal. Sensitive information is transferred via a secure SSL connection to PayPal – and stays with PayPal.

Funds can be transferred directly into the merchant’s account if the banking details have been verified.

See Figure 12 for a list of options on how funds can be withdrawn.

![Figure 12. Ways to draw funds from a PayPal account.](image)

### Table: Withdraw Funds

<table>
<thead>
<tr>
<th>Options</th>
<th>Processing Time</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer funds to your bank account</td>
<td>2-4 Business Days</td>
<td>Free!</td>
</tr>
<tr>
<td>Request a check from PayPal</td>
<td>1-2 Weeks</td>
<td>$1.50 USD</td>
</tr>
<tr>
<td>Shop with a PayPal debit card</td>
<td>Instant (once you get a card)</td>
<td>Get cashback!</td>
</tr>
<tr>
<td>Get cash out of an ATM</td>
<td>Instant</td>
<td>$1.00 USD</td>
</tr>
<tr>
<td>Shop online with a PayPal virtual card</td>
<td>Instant</td>
<td>Free!</td>
</tr>
<tr>
<td>Buy from over 40,000 PayPal Shops</td>
<td>Instant</td>
<td>Free!</td>
</tr>
</tbody>
</table>


PayPal makes millions of financial transactions, holds large amounts of money and offers credit and debit cards. It is not regulated, although it acts as a bank. PayPal also does not provide any maintenance and security services that real banks provide. Therefore, PayPal is not a bank but rather a money account.

Rumour has it that PayPal freezes customers’ accounts in order to earn interest on that money for themselves. This means PayPal merchants cannot gain access to their account, add or withdraw any funds. The process to verify the identity of the account holder is tedious and lengthy and in some cases, funds were never returned.
Other charges levied against PayPal include [Grabianowski, E. 1998-2008]:

- Lax security, despite their claims as a secure method of making online transactions.
- A long and confusing terms of service agreement that tricks users into giving up both their right to sue the company and their protections under credit card laws.
- Rude customer service representatives.
- Poor hiring practices that have led to a number of scams committed as "inside jobs".

An outdated but thorough investigation of various complaints can be found at: http://www.wilsonWeb.com/wct5/PayPal_assess.htm.

Another Web site dedicated to the criticism of PayPal’s services is http://www.paypalsucks.com.

For a real-life case study have a look at http://www.paypalsucks.com/paypalfan.shtml (link is subject to change).

Despite these criticisms, PayPal continues to be the most popular money transfer service for online transactions.

4.2. Evolution of E-commerce using Facebook [Allfacebook.com. 2007] (Chapter 3 (3.5.2) p. 39)

4.2.1. Social shopping

Online shopping is turning towards what is called social shopping. Social shopping is based on assisting an interested buyer’s decision with trusted reviews and recommendations on previously bought products and items. These reviews provide value, because the Facebook network provides facilities where we can view what our friend’s bought, and we are more likely to trust the people we know.

Facebook has become the dominant player in social shopping. Advanced e-commerce applications will continue to rise in popularity, owing to the advent of the Facebook payment system.

One would think eBay would launch their own application, which allows us to list items on eBay within the Facebook platform. Buy.com announced a Garage sale application which allows Facebook users to buy and sell items between themselves. Goods can be sold directly from a user’s profile page and Buy.com hopes to attract business away from
eBay. Other similar services include Mosoma, which failed to launch, not obtaining enough users. While Facebook already provides the sufficient marketplace for such transactions, numbers in the masses will need to be reached before this type of marketplace becomes efficient.

### 4.2.2. Facebook: A New Form of Advertising

Applications at this stage are used to place an advert into a user’s profile. This form of advertising may become much more effective than the anonymous flyer advertisements. The Visual Bookshelf and Flixter’s Movies Applications have been successful in increasing sales through users’ profiles. This occurs because people want to boast about their movie and book collections to their friends.
Appendix 3

Part III

Compromise of Sensitive Information

Chapter 4

Introduction to Online Fraud and Finding Personal Information

Section 1 – Privacy Issues and PII Online


Personal information can be accessed from a variety of places, including but not limited to the following:

• Information can be memorized or copied by sales clerks and waiters.
• Formal documents such as financial account statements and other bills are removed from the mailbox before we have a chance to retrieve them.
• Confidential documents are accessed from our employer’s files.
• Confidential hospital records.
• Dumpsters and trash cans, known as "dumpster diving".
• Financial lenders’ files.
• Landlords’ files.
• Online (or offline) databases which may be free.
• Fraudulent (spoofed) Web sites capturing information (more on this topic in Chapter 5).
• A merchant database through computer hacking (this is not as simple as other forms of theft).
• Our personal computer or commercial Web sites by means of malicious software (more on this topic in Chapter 5).
• “Cloned” IRC rooms posting links to illegitimate (spoofed) Web sites to gather sensitive information (more on spoofing in Chapter 5).
• Any information has been gathered through any Internet transaction can be targeted, or sold to information brokers (information brokers are discussed in Chapter 5).
• Skimming machines mostly used in restaurants to capture credit card data (more information on skimming in Chapter 5).
• Part-time employees recruited on a temporary basis, as fewer background checks are done on them.

In addition to the number of places where personal and sensitive information can be gathered about an individual, there are also other public sources of information at anyone’s disposal. These include, but are not limited to:

• **Public records:** Records that are made available for public inspection which many include business records, vehicle information, driver’s licence information, professional certificates, criminal records and any other types of data collected by public entities.

• **Publicly available information:** Includes non-government information which many be accessed in telephone directory entries, newspapers, classified advertisements and reports.

• **Open-source information:** Any information that we may provide about ourselves to journals, magazines, bulletin boards, blogs, reviews and Web sites.

A brief background has been given, considering the different places and public sources from which identity theft may originate. Information found about people can be gathered with the correct tools and skills. A brief outline on how almost anything can be found out about anyone on the Web is provided next.

### 1.2. How to Find and Investigate Anyone Online (Almost) [bizewriter. 2008] (Chapter 4 (4.1.) p. 44)

Before the steps to investigating people online are discussed, a few tools are needed. These tools include, but are not limited to:

• Research time
Appendix 3

- Free people search Web sites
- New e-mail account
- Third-party investigation service (optional)
- Multiple search engines

Once these tools are available, such as the research time, the following steps can be taken:

**Step 1: Keep your identity anonymous:** Create a new e-mail account which cannot be traced back to its creator. Optimally, create an e-mail address which expires within several hours. A temporary e-mail address can be created using Anonymizer’s Nym Software Feature (more information in Chapter 7). Whenever creating an account, keep in mind protecting your own identity.

Also you must remember why you want to investigate a particular person. This helps you to head in the right direction while researching. Online services may require payment to conduct an investigative search. Don’t pay for what you don’t need.

**Step 2: Gather information about the person:** Guessing e-mail addresses, potential nicknames often works well, as well as writing down the person’s activities, hobbies, work and location. Also, think of more informal data such as a person’s interests, family members and friend’s names, potential clubs or organizations, professional data, newspaper clippings and even their pet type and name.

**Step 3: Start searching:** You can find people with identical names, age, address and telephone number on the ZabaSearch Web site (available at [http://www.zabasearch.com/](http://www.zabasearch.com/)). By previewing ZabaSearch’s paid-for people finder service, you may also find relatives and associated names of the person. The Reunion Web site (available at [http://www.reunion.com/](http://www.reunion.com/), the South African version, is available at [http://www.sareunited.com/](http://www.sareunited.com/)) if ZabaSearch does not provide any results. From here, paid research including criminal background checks, home value, small claims and judgments, court records, relatives and neighbours, amongst other things, can be accessed.

**Step 4: Try other Web sites:** Spokeo (available at [http://www.spokeo.com/](http://www.spokeo.com/)), Wink (available at [http://wink.com/](http://wink.com/)) and PiPl (available at [http://pipl.com/](http://pipl.com/)) can be used as search sources. Facebook, Digg, MySpace and Flickr are examples of social networking sites on which users freely distribute personal information. When only a pseudonym is known, a real name may be revealed since
Amazon.com activity is also searched. This is possible when a user leaves account information such as a “wish list” public. Real names of MySpace account holders may also be revealed by PiPi.

NetDetective.com’s service may save time and offers profound information if you wish to investigate people online. Unlimited searches can be conducted over a course of a year in exchange for a modest fee.

Another useful service is the Government Public Records Database of the USA, UK, Canada, Australia and South Africa (available at http://gov-reports.net/), which provides personal records, background checks, criminal records through to military records.

**Step 5: Narrow the search:** When too many false positives occur, add parameters to the Google search such as: site:facebook.com “name/nickname” + “location” + “hobby”. A lead may be found in a hobbyist or other forum, photo collection Web site, job database, or on a blog for starters.

Most investigative search Web sites are populated for the United States only. If a searcher is interested in using numerous search Web sites to locate a person in the States, the following link may be useful: http://lifehacker.com/software/technophilia/where-to-find-public-records-online-280785.php.

1.3. **More on Potential Search Sites [bizewriter. 2008] (Chapter 4 (4.1.) p. 44)**

The Firefox Who Is This Person? Plugin enables us to right-click on a name within any Web site and search the person’s name from any Web site of our choice. Choices include Wink, LinkedIn, Wikipedia, Facebook, Google News, Technorati, Yahoo People Search, Spock, WikiYou, ZoomInfo, MySpace, ZabaSearch, ZoomInfo and other engines from the Who Is This Person? context menu item (see Figure 13).
This Firefox feature is available as a free download from https://addons.mozilla.org/en-US/firefox/search?q=Who+Is+This+Person%3F&cat=all.

The tools and resources to search information about people online have been discussed. When conducting such research, we should be cautious when revealing information about ourselves which may lead to compromise of our own privacy and sensitive data. Some tips and warnings on conducting a more successful search about a person are given in the next section.

1.4. Tips and Warnings [bizewriter. 2008] (Chapter 4 (4.1.) p. 44)

The following tips and warnings could be helpful when doing online research:
• Research the Web site before providing any information such as an e-mail address when signing up. Read the privacy policies, and use different e-mails for personal, business and financial reasons.
• Many Web sites that do investigative searches charge for their services but do not have access to any more information than anyone else.
• Doing a bit of research is recommended before paying for an investigative service. Have a look at third-party sources where the services are reviewed, since many of these Web sites do not provide what they promise.
• Some records such as family court records may be sealed.
• A phone call may often result in paper copies of permanent records if public records are not available for free on the Web.
• The steps and techniques described earlier in this section are legal, free and approved methods to finding someone online. Imagine how much more information a professional hacker is able to find about people online.
• Do not give out any personal information such as telephone numbers, address or credit card information in chat rooms or in newsgroups because the Internet is a public place.
Appendix 4

Part III

Internet Crime Schemes

Chapter 5

Modus Operandi (MO) Techniques for Committing Online Fraud

Section 1 – Credit Card Fraud

1.1. Skimming (Chapter 5 (5.1.1.) p. 53)

The offender steals names and credit/debit card numbers by using a special storage device when processing the card. Anyone who has physical access to the victim’s credit card can swipe away at this information.

Skimming occurs when a fraudster obtains credit card information illegally. This often happens in restaurants where the victim loses sight of the card. The fraudster swipes the credit card through a skimming device which retrieves all electronic data needed from the magnetic stripes found on credit cards for the fraudster to commit illegal activities. The information retained by the device is then downloaded onto a computer and a fraudulent duplicate of the credit card can be manufactured.

Like identity theft, credit card fraud is not new. But the developments in the world of electronic commerce have created opportunities for criminals to use stolen credit card information conveniently, anonymously and globally. In some cases, the fraudster may use this stolen credit card data to order merchandise online. The merchandise bought with fraudulent credit card information is then resold on the Internet.
1.2. How SMS Authorization Works (Chapter 5 (5.1.2.) p. 53)

For additional security purposes Internet banking organizations have integrated the one-time PIN (OTP) into their banking system. The OTP is an alpha-numeric reference number which is sent to our cell phone by SMS. The reference number is valid for a single session. Whether the operation is a once-off-payment or adding/deleting a beneficiary, the OTP must be entered to be able to complete the transaction.

1.3. How the SIM Swap Scam Works (Chapter 5 (5.1.2.) p. 53)

Perpetrators can intercept the SMS authorization utility by using our personal information as well as our cell phone number.

The perpetrator can retrieve our information through phishing, spoofing, malicious software and keystroke logging, which are discussed in the next sections. If the perpetrator acts on this stolen information, he can request a new SIM card from the cellular service provider. A new SIM card is issued to the perpetrator by transferring the SIM card identity and cancelling our old SIM card.

This enables the perpetrator to facade as the legitimate owner of our bank account. All OTPs are sent to the perpetrator’s new SIM card enabling him to complete all online transactions.

Section 2 – Phishing

2.1. People Behind the Phishes [Beal, V. 2006] (Chapter 5 (5.2.1.) p. 56)

At every opportunity, phishing e-mails are sent in the millions by scam artists. A response from only a few recipients with their financial and personal data is needed for their phishing attempt to be successful.
2.2. Web Crawlers (Spiders) (Chapter 5 (5.2.1.) p. 56)

Anyone with an e-mail address is at risk of being phished. Any e-mail address that has been made public on the Internet (posting in forums, newsgroups or Web sites) is more susceptible to phishing, as the e-mail address can be saved by spiders. A spider is a program that is used by search engines to retrieve Web pages. As soon as the program sees a link to another page, it retrieves the Web page responding to that link. Because most Web pages contain links, spiders can start almost anywhere and crawl (search) over the Web (Internet).

Spiders that search the Internet can grab as many e-mail addresses as they can. Millions of valid e-mail addresses can be accessed almost instantly, at no extra cost, proving to be a profitable business for the scammers.

Fraudsters constantly reinvent themselves, which is why it is difficult to stay ahead of their techniques. The best advice is to know what not to do and to stay alert and be aware of these possibilities at all times.
2.3. Spear Phishing [Beal, V. 2006] (Chapter 5 (5.2.1.) p. 56)

Perpetrators alter their attack methods once a small percentage of the population begin to realize what is happening. In spear phishing the focus is on the department of an organization, or a single user. The hacker’s aim is to gain entry into secure networks by sending a fraudulent e-mail which appears to be from a trusted source within that company or department. The e-mail then asks the employee to reveal username and password information, either to update their details or for other reasons.

An alternative spear phishing attack will deploy spyware onto that machine that can steal data when the specified link is clicked on. Spyware and malicious software (malware) is discussed in Chapter 5, section 5.3.1.

2.4. Vishing [Internet Crime Complaint Center (IC3). 2008a] (Chapter 5 (5.2.1.) p. 56)

Different variations of phishing schemes known as “vishing” have been reported to the IC3. This scam is similar to that of phishing but is pronounced with a “V” to indicate voice. Vishing is a phishing scam where a potential victim is instructed to contact their bank by telephone or an automated recording, encouraging them to enter sensitive and personal information. The e-mail contains the telephone number and when the victim phones the number, they are greeted by: “Welcome to the bank of...” and the victim is then conned into entering credentials such as credit card information to resolve a pending security issue.

A new strategy is to send a text message to a cell phone claiming the victim’s online bank account has expired. The victim is then advised that they may renew their online bank account by using the link provided in the text message.
Section 3 – Spoofing

3.1. Types of Spoofing [Wallace, J. 1998-2008] (Chapter 5 (5.2.2.) p. 57)

Spoofing is a broad term used widely in the Internet community. Although spoofing is used mostly in conjunction with phishing, there are various types of spoofing methods from various directions.

3.1.1. Spoofing of File-sharing Networks

Spoofing can also apply to the file-sharing networks used to share music illegally. The Recording Industry Association of America (RIAA) are making the downloading of music
much more difficult by making a song appear to be the original. The aim is to discourage illegal downloads and pay for a legal copy of the song.

### 3.1.2. Login Spoofing

A victim is presented with a login prompt by a malicious program, fraudulent Web site, embedded e-mail or by any other means. This login prompt looks ordinary and asks the victim to enter his username and passwords. Such a login prompt is usually under the control of the attacker.

### 3.1.3. E-mail Address Spoofing

E-mail address spoofing is a problem in our electronic world which persuades innocent victims to believe the perpetrator is someone else whom they trust. By gaining the victim’s confidence, the perpetrator may be able to win over personal information and even money all at the victim’s expense.

### 3.1.4. Web Spoofing

The perpetrator gains control over information and can observe and modify information sent and received from the victim’s computer. The techniques used to achieve this are discussed in 3.2 below.

### 3.1.5. Fraudulent Web sites

These are set up to capture personal and financial information which the legitimate organization, such as a bank, already has. The e-mail may direct the victim to this Web site by requiring them to click on a link and asking them to update their details. Personal data such as passwords, identity, credit card and bank account numbers are then captured by the thieves.

### 3.1.6. URL Spoofing

Another technique, also known as URL spoofing, displays the incorrect URL in the browser’s location bar after the browser has clicked on a link that appears to be legitimate.
3.1.7. IP Spoofing [Tanase, M. 2003]

This is used to impersonate another source, where IP packets are created with fraudulent IP addresses used to conceal the identity of the sender. Defending against IP spoofing is explained in Chapter 6.


The interconnected network works through protocols. An Internet protocol is the basic protocol for communications between different computers and computer networks across the Internet. Each IP packet contains a header which contains an IP address for the source and destination address of the packet. This address is needed for certain things. For example, a receiving computer needs to know the source address to be able to send a response back. An intruder can forge the header of an IP packet. This means that the receiving computer will receive packets from the forged IP source address and
send responses back to that address. In some cases the intruder may redirect responsive packets to his machine through the use of various techniques, such as the man-in-the-middle attack and URL rewriting.

### 3.2.1. Man-in-the-Middle Attack

A man-in-the-middle attack occurs when someone intercepts the messages being passed between two parties. For example, both Sally and Peter think they are communicating with each other but are instead being spoofed. In this way, the intruder gains access to all messages sent between the two parties.

#### 3.2.1.1. SYN Attack Methodology

Messages are intercepted by using the SYN attack methodology. The intruder can send his own packets while the receiving computer thinks it is receiving packets from the sending computer. The intruder guesses the sequence number of the packets received and reconstructs them, which requires the intruder to monitor each packet.

#### 3.2.1.2. Surveillance

As information is directed to and from Web servers, all information typed into forms by the victim is also intercepted by the intruder. This includes any passwords, account or credit card numbers entered. The intruder may passively watch traffic and record all pages and their contents visited by the victim, which is known as surveillance. Surveillance can occur even through a secure connection (SSL), which was mentioned earlier. Making sure the certificate is valid and that there is a padlock in the browser windows does not mean surveillance cannot take place.

Secure connections do not always help. The padlock icon and the ‘s’ following the http indicating a secure connection in the URL will still be there, which, unfortunately, also occurs in a false Web. A false Web occurs when the attacker creates a shadow copy of the original Web. The Internet browser shows that it has a secure connection because it does have one. The browser is told to make a secure connection to the attacker’s server. The secure connection does not point to the place the victim thinks it is. The secure connection indicator only gives the victim a false sense of security.

3.2.1.4. Tampering [Felten, E.W. Blfanz, D. Dean, D. Wallach, D.S. 1997]

Surveillance and a false sense of security are not users’ only concern. A technique known as tampering allows the offender to tamper with and modify the contents sent and received by the victim’s computer and the server being communicated with. The offender is able to change order numbers, product numbers, quantities and the ship-to address. Data returned to the victim can be modified to reflect invalid data and offensive material.

Reinventing the Web also allows the perpetrator to observe and modify whatever information is being viewed, sent and received by the victim. This is done by a technique called URL rewriting.


To start an attack, the attacker must somehow lure the victim into the attacker’s false Web. This can be done through several methods:
1. A link to a false Web could be placed onto a popular Web page.
2. If the victim is using Web-enabled email, the attacker could e-mail the victim a pointer to a false Web.
3. The attacker can deceive that part of the false Web to be indexed by a search engine.

**Step 1:** The attacker’s first trick is to rewrite all of the URLs on some Web page so that they point to the attacker’s server rather than to the original server. The attacker rewrites a URL by adding his own URL to the front of the original URL, for example https://www.attacker.net/https://www.originalserver.net.

**Step 2:** The victim’s browser requests the page from the attacker’s server, since the URL starts with the attacker’s server address. The remaining part of the URL tells the attacker’s server where on the Web to go to get the original document (refer to Figure 14).

**Step 3:** Once the attacker's server has fetched the real document needed to satisfy the request, the attacker rewrites all of the URLs in the document into the same special format by splicing his server address to the front of the original server address. The attacker’s server then provides the rewritten page to the victim’s browser.

**Step 4:** Because all the URLs in the altered page have been modified, the page requested by the victim will again be fetched through the attacker's server. This means that the victim remains trapped in the attacker's false Web, and can follow links forever without leaving it.

### 3.2.2. Spoofed Web Sites Residing in the Cache [MyBB Group. 2006]

Something to be aware of are the spoofed Web sites being stored in the cache. The cache is where the Web browser looks to reload frequently visited sites. A variant to spoofing is using a secretly hidden Trojan horse (more on Trojans in section 5.8.) to manipulate the cache. When we attempt to load a retail, online banking or other legitimate Web site, the Web browser automatically redirects us to a fraudulent Web site.

Spoofed Web pages may reside in the cache on the victim’s computer long after the session has been terminated. This can further lead to the victim viewing false Web pages throughout his browsing experience.
3.2.3. Beware of Filling in Online Forms [Simon, I.M. 2008]

When a victim fills in a form on any Web page contained in a false Web, these details will be sent to the attacker’s server instead of the original server and it will appear as if the transaction has taken place correctly. Form submission is encoded in URLs and the responses are ordinary HyperText Mark-up Language (HTML). Most Web pages are developed through HTML as it is a basic standard and protocol to structure and display text, graphics, multimedia and various links between documents.

This makes spoofing of forms as easy as it is to spoof a URL, as explained earlier. In this way the submitted data is sent to the attacker’s server where the perpetrator is able to modify the contents and send the details to the original server. See surveillance and tampering described earlier in this section.

3.2.4. Beware of Bookmarking Web Pages [Simon, I.M. 2008]

It is not advised to bookmark any random Web pages. When we bookmark or add a Web page to our favourites folder it may become a risk, as the browser will always be directed to the false link, which will enter and re-enter a false Web.

Many Internet protocols which are poorly designed are vulnerable to such spoofing attacks. How Web spoofing works and the basic idea behind Web spoofing techniques have been discussed. Now the reasons why perpetrators send e-mails with spoofed e-mail addresses are given.

3.3. Masterminds behind Spoofed E-mail Addresses [Shinder, D.L. 2005] (Chapter 5 (5.2.2.) p. 57)

Criminals have their reasons for wanting to hide their true identities. It is both convenient and cost-effective to do this through an online facility as there is no physical interaction, and the victim will ideally never see who the real perpetrator is.

When receiving spam or a phishing e-mail it is likely that the return address has been altered. Like ordinary mail received in the post, the sender can write any name and address there. It may even be an address which is valid and belongs to an innocent victim. This is all possible because Simple Mail Transfer Protocol (SMTP) does not require any authentication.
Here are some common reasons why someone would want to spoof their true identity along with the e-mail address [Shinder, D.L. 2005]:

- The e-mail is spam and the sender does not want to be subjected to anti-spam laws.
- The e-mail constitutes a violation of some other law (for example, it is threatening or harassing).
- The e-mail contains a virus or Trojan and the sender believes we are more likely to open it if it appears to be from someone we know.
- The e-mail requests information that we might be willing to give to the person the sender is pretending to be (for example, a sender might pose as our company’s system administrator and ask for our network password), as part of a “social engineering” attack.
- The sender is attempting to cause trouble for someone by pretending to be that person (for example, to make it look as though a political rival or personal enemy said something he did not in an e-mail message).

We may find our computer flooded with e-mails from angry complainants if their address has been used to send spam mail. This could result having our legitimate e-mail addresses banned from many servers. On the other hand, receiving mail from spoofed sources could range in severity.

Spoofing is also used as a network management technique to reduce traffic. For the purposes of this document, this will not be discussed any further.

An introduction to who is behind the spoofed e-mail, spoofing mechanisms and the types of spoofing as well as what spoofing is has been given. Spoofing and its common techniques examined in this section are not the only way in which we can become a victim to surrendering personal data.

**Section 4 – Social Engineering (Chapter 5 (5.2.3.) p. 59)**

**Parcel Courier E-mail Scheme [Internet Crime Complaint Center (IC3). 2008a]**

In this particular scheme, the international shipment providers such as DHL, UPS, FedEx and USPS are involved when the perpetrator e-mails the victim following an online bidding on auction sites. Most of the parcel courier e-mail schemes follow a similar pattern, which is as follows:
1. Shipping information such as the name and address of the buyer is requested by the fraudster.
2. The fraudster informs the buyer of the selected shipment provider, which will keep the item in the buyer’s name and address.
3. The chosen shipment provider ensures that everything is in order by checking the item and purchase documents.
4. The chosen shipment provider verifies the receipt of the item by sending the buyer a delivery notification.
5. The fraudster instructs the buyer to go to an electronic funds transfer medium, such as Western Union, to transfer the funds for the purchase in the fraudster’s name.
6. Once the transfer is complete, the fraudster instructs the buyer to forward the funds transfer identification number to the chosen shipment provider, including the name and address associated with the shipment.
7. The fraudster informs the buyer that the shipment provider will verify payment information and complete the delivery process.
8. Upon completion of inspection and delivery of the item by the receiver, the buyer provides the parcel provider funds transfer information, thus allowing the seller to receive his funds.

Prevention of being a victim to the parcel courier e-mail scheme is discussed in Chapter 6.

Section 5 – Spyware and Malware

5.1. Installation of Unwanted Software/Spyware [Free Computer Technical Support. 2008] (Chapter 5 (5.3.1.1.) p. 63)

Spyware may use up our Internet bandwidth and cause our computer to slow down. Such programs may install additional unwanted software on our computer, add additional unwanted components to our Internet browser, alter our home and/or search page and redirect Web browser activity. A common trick is to automatically install this type of software on our computer when installing a downloaded software program, such as a music file-sharing program which may be freeware or shareware. While the software downloaded does not cause harm to our computer, the bundled spyware does. In some cases, shareware authors have been paid by spyware authors to bundle
spyware with their software. In other cases, desirable free software has been repackaged with installers that add spyware.

It is important to understand what the software will do and to agree to install the software on our computer. Read the privacy statement, disclosures and licence agreements before proceeding with the instalments. Sometimes the terms of installing unwanted spyware programs may be included at the end of these documents. We may have the option of not installing any of these spyware programs.

5.2. Adware in the Spyware Community [Paz, U. 2002] (Chapter 5 (5.3.1.1.) p. 63)

Spyware normally runs in the background of our computer and is often associated with adware. Adware and spyware can have similar characteristics to viruses. During the installation process an independent program is installed called an “adbot”, which maintains advertisements by sending and receiving information from their servers, and is hidden. The types of information delivered to their servers are:

- For how long each advert is shown
- Which Adware hosted the advert
- Whether we clicked on the advert or not

Adware displays advertisements related to what it finds from spying on us. It reports on certain Web sites we visit and provides a specific service in return. It does not operate maliciously the way in which spyware does.

5.3. Spyware Used for Commercial Gain (Chapter 5 (5.3.1.1.) p. 63)

Spyware infections occur mainly for commercial gain. But unlike worms and viruses, spyware does not self-replicate. Instead, it infiltrates computers through software and security vulnerabilities.

Some pop-up ads allow us to choose whether to download a certain software program, such as one that speeds up bandwidth. No matter where we click on the advertisement, even if it is the cancel button, the spyware is automatically downloaded onto our computer. Another aspect of unsuspectingly downloading software is software packages which pose as security packages or a useful software utility such as an Internet Download Accelerator.
5.4. **A User’s Opt-in Approach to Spyware (Chapter 5 (5.3.1.1.) p. 63)**

Software that spies on you and tracks all your activities might not always be bad. We may have opted in to an agreement to allow the party to send advertisements that may interest us. By doing so, the party will track our activities to determine which advertisements to show. Another reason may be to track our browser activity for statistical and research purposes. This process may be hindered owing to suspicions against spyware.

5.5. **Anti-spyware Packages (Chapter 5 (5.3.1.1.) p. 63)**

Anti-spyware programs, which are discussed in Chapter 7, may disable wanted programs. For example, in some cases, downloading software bundled with advertising material cannot be removed without removing the wanted software. This causes issues for the developers of anti-spyware software packages.

The Anti-Spyware Coalition is a group of anti-spyware companies, academics and consumer groups which have published documents addressing the spyware dilemma. These documents address what is and what is not acceptable spyware behaviour.

5.6. **Spyware and Cookies [Herold, R. 2002: 356-358] (Chapter 5 (5.3.1.1.) p. 63)**

Cookies are the small text files used for tracking browsing behaviour, maintaining specific information about users and authentication. Cookies are used for personalization based on a user’s preferences and to determine the contents of a particular user’s shopping basket, for example. Cookies are also used to target advertisements which are applicable to our needs and interests. A Web site can customize the information displayed as we log on to a specific site, when cookies are able to track our usage patterns. For instance, by storing information using cookies and once we enter a username and password on a specific Web site, these do not have to be entered again. This causes security risks when sharing a computer and is not recommended. Cookies are not programs and cannot perform any function determined through any type of instructions, although they have raised some concern about privacy. For this reason, cookies have been mistaken for spyware or viruses. It may be useful to identify what cookies cannot do. Cookies cannot [Herold, R. 2002: 358]:

- Damage or steal information contained on a hard drive
• Destroy the hard drive by means of planting viruses
• Track activities as we follow links from one site to another
• Procure credit card information without our permission
• Travel with us from one computer to another
• Track personal information such as names and addresses unless such information had been provided voluntarily

Modern browsers allow us to disable cookies, disallowing cookies to be stored on a user’s computer. Rejection of such cookies may cause some Web sites to be unusable, such as shopping baskets.

As the spyware epidemic continues to escalate, various attempted techniques and mechanisms have surfaced to neutralize the problem. Programs such as anti-spyware packages, discussed in more detail in Chapter 7, generate the option to remove spyware and cookies that are detected as spyware.

5.7. Spyware – A Security Issue [Technews Publishing (Pty) Ltd. 2007] (Chapter 5 (5.3.1.1.) p. 63)

Spyware is advancing at a rapid rate and becoming more and more complex to identify and combat. Through developed variations of certain spyware programs, this leads to greater numbers of these programs.

Variations of spyware may not be removed and uninstalled easily. In most cases, spyware has the capability to reinstall components, repopulate and impact multiple registry entries, randomize various elements of the program to leave a different footprint, making them more difficult to track, and typically leaves dozens of application files spread across a computer’s hard drive or deep within the hardware. If spyware is not detected and removed, these malicious applications may download additional spyware software, further impacting system performance.

There are spyware programs, such as Look2Me, which installs itself as a Windows critical process that cannot be removed. When attempts are made to remove the spyware, the computer is rebooted and the program reinstalls itself. Look2Me uses Internet Explorer to insert a file into the Windows area that controls the system start-up processes.

The removal of such malicious software programs can be a daunting task and requires highly specialized techniques other than what is provided in the anti-virus software alone.
5.8. Remote Access Trojans (RATs) [Paz, U. 2002] (Chapter 5 (5.3.1.3.) p. 64)

RATs are one of the easiest and most efficient methods to hack into a victim’s computer and gain control. A Trojan horse is a more general term for a RAT, while a backdoor Trojan or backdoor program also refers to a RAT. A user may innocently accept a file transfer, either through IM or by e-mail, which contains a RAT.

RATs differ from viruses: viruses have the ability to self-replicate and distribute themselves, while RATs (sometimes referred to as Remote Admin Trojans) listen for incoming communication once executed on the victim’s computer from a remote program identical to what the intruder uses. The intruder may gain full control over the victim’s computer.

Other types of RATs include worms, which may distribute using their own SMTP engine, or steal passwords, among others. Anti-virus and anti-firewall software programs may be used to counteract and prevent these infections. More information on anti-virus and firewall software applications is provided in Chapter 7.

Section 6 – Key Loggers

6.1. How Key Loggers are Installed [Krebs, B. 2006] (Chapter 5 (5.3.2.2.) p. 66)

Perpetrators need physical access to a computer to be able to install a key logger. The device may be a piece of hardware attached to the keyboard or it may be a cable and will seem as if it is part of the computer equipment.

Another methodology is to send the device in a software form through an e-mail attachment. The key logger is then installed by the software. A key logger may also be seeded by means of an invading virus or piece of malicious software called a worm, which replicates itself across networks. The information recorded is written into a text file and regularly e-mailed to a free, anonymous e-mail account. The attacker then sits and filters through the text looking for credit card numbers and passwords.
6.2. Reasons Why Fraudsters Use Key Logging (Chapter 5 (5.3.2.2.) p. 66)

1. The software version is easily downloadable onto any computer.
2. When a particular bank name is typed in by a user the key logging software immediately begins recording.
3. The software’s files can be accessed remotely and may be accessed by the use of the perpetrator’s password.
4. Key loggers are difficult to detect and to remove.
5. Key loggers may monitor keystrokes in the background. The software downloads information or provides access to our computer without us being able to detect these activities.

6.3. Current Key Logging Software Versions (Chapter 5 (5.3.2.2.) p. 66)

- WINSPY
- FAMILY KEYLOGGER
- ADVANCED KEYLOGGER
- KEYBOARD SPECTATOR

There are many versions of software key loggers. A common area to put key loggers into use is the Garden Route along the coast of South Africa. These are the parts of the country tourists are most likely to use an Internet access point at a public place, such as Internet cafes. Another common strategy related to key logging software is when tourists attempt to access the Internet using a wireless hotspot in a public place.

Section 7 – Wireless Attacks

7.1. Network Security [Spanbauer, S. 2003] (Chapter 5 (5.3.3.) p. 66)

Wireless networks are more prone to intrusion owing to the weak wired equivalent privacy (WEP) encryption mechanism used in most wireless cards and routers. The WEP has since been replaced by a new standard called WPA (wireless protect access) by the Wi-Fi Alliance.
8.1. Other Sharing Risks [Paz, U. 2002] (Chapter 5 (5.3.4.) p. 68)

Other than Trojans, intruders may use the NetBIOS communication standard to hack into a home computer, which is a standard for naming computers in small networks. The communication standards relevant to Microsoft Windows OS are NBT (NetBIOS over TCP/IP), IPX/SPX and NetBEUI.

The NBT (or NetBIOS) acts as a server and is the communication standard used over the Internet. The computer listens for communications using this standard, and reacts to different NBT commands that it may receive from remote applications if it is enabled. The problem comes in when we enable file and printer sharing and do not apply a password. This means any remote computer may gain access to those files and printers. Many technicians are not aware of this fact and leave the backdoor open to unauthenticated threats and intrusions.

9.1. Money Laundering - Most Common 419 Scam (Chapter 5 (5.4.1.) p. 70)

Money laundering refers to illegal financial transactions from an unknown or secret bank account source usually in a foreign country and is related to organized crime. The modus operandi is named for the violation of Section 419 of the Nigerian Criminal Code. The most common approach is to notify a victim of unclaimed funds either by letter, e-mail or fax. The funds are claimed to be worth millions, present in inactive accounts, usually from a deceased estate. The victim is offered the opportunity to help launder these unclaimed funds by Nigerian or foreign government officials.

Payment of taxes and other legal fees are promised to be reimbursed to the victim once the funds are placed overseas.

Once agreed, the victim sends through information such as banking details, blank company letterheads which are duly signed, blank invoices and telephone and fax
numbers in order to use his accounts to facilitate transactions. In many cases, a deposit is required from the victim to reactivate the dormant account. The victim is normally promised a sizable percentage, between 20 and 35% of the money transferred as a commission for the use of the bank account. Money is then paid by the victim in several instalments of increasing amounts, resulting in money lost by the victim.

9.2. Job Scams/Business Opportunities [Internet Crime Complaint Center (IC3). 2008a] (Chapter 5 (5.4.1.) p. 70)

A job scam occurs when counterfeit foreign-based companies pretend to be legitimate recruiters offering attractive work-at-home employment opportunities. These recruitment opportunities involve reselling or reshipping goods to overseas destinations. The victim is usually required to pay money in advance for air travel expenses, such as work visas. Personal data supplied to the illegitimate company may include full name, bank account details, credit card details, PayPal information, driver’s licence, birth date, home address, or any other personal data.

9.2.1. Fraudulent Employee Employment

Employees of such a company are told that their salaries will be paid to them by another United States company that is a creditor of the employer. The employer pretends to not have any banking set up in the United States.

The salary amount paid to the employee is usually significantly more than what is owed. The employee is instructed to deposit the cheque into his own account and pay back the balance through online electronic banking, usually into an Eastern European account. When the cheque is later found to be counterfeit, the victim is held liable to pay that amount back to the bank.

9.2.2. Affiliate Opportunities

Similarly, affiliate opportunities are presented to those interested in selling high-end electronic goods such as plasma screens and home theatre systems at significantly
reduced prices. These opportunities are normally presented by Web-based international companies.

The company claims it holds the stocks in its warehouse, eliminating the storage costs, shipping and handling fees of the affiliate. The affiliate then acts as a middleman between the non-existent company and the potential buyer. The affiliate advertises the item on a well-known Internet auction site and accepts the funds from the customer should a purchase be made. The funds are then paid into the company's account by means of an EFT. The company never delivers the goods, causing the purchaser to take legal action and the affiliate then becomes the victim.

9.3. Lottery Win [Internet Crime Complaint Center (IC3). 2008a] (Chapter 5 (5.4.1.) p. 70)

Contacting victims through randomly generated e-mail addresses, the thief advises the victim that he has won a lottery. Once the victim is persuaded into believing he has won an international lottery, the perpetrator will further persuade the victim to transfer money into an account whatever the reason may be.

Numerous lottery names have been identified by the Internet Crime Complaint Center as being used in this scheme. The e-mail message usually reads similar to the following:

"This is to inform you of the release of money winnings to you. Your email was randomly selected as the winner and therefore you have been approved for a lump sum payout of $500,000.00. To begin your lottery claim, please contact the processing company selected to process your winnings."

The name of the agency, contact (either US, or also at a foreign address), phone number, fax number and e-mail address conclude the e-mail. Usually, an initial fee is required to begin the process and thereafter additional amounts are requested to continue the process.

9.4. Inheritance Payout (Chapter 5 (5.4.1.) p. 70)

The victim is told that a distant relative has passed away. For the victim to get access to the inheritance, money must be paid to the perpetrator to cover all administration fees.

The different aspects to advance fee fraud have been discussed. The naivety and greed of people have become the prime factor contributing to the success of these crimes.
10.1. Romanian Auction Fraud [Internet Crime Complaint Center (IC3). 2008a] (Chapter 5 (5.4.5.) p. 73)

Romanian subjects’ approach to committing online fraud is constantly reinvented through flexibility. The latest trend is in electronic banking systems where the buyer transfers money electronically from his bank into another bank account. These EFTs are routed through large US banks and then to Bucharest, Romania or Riga, Latvia. Romania is infamously associated with auction fraud, as almost every in-demand product is placed on auction sites for purchase.

The Romanian fraudster falsifies his identity, pretending to be a citizen of the United States. He then advises the victim to transfer the money to a European country to a family member, business partner, sick relative or associate. The funds are usually transferred through MoneyGram or Western Union electronic transfer, allowing the victim to transfer half the payment now and half when the item is delivered.

It has been verified by the Internet Crime Complaint Center that the receiver must provide the complete information of the sender and the receiver’s full name and address. These details are needed in order to receive funds using Western Union and can be picked up anywhere in the world. The Money Transfer Control Number (MTCN) or answer to any secret question is not needed, as falsely directed to the victims. The funds sent by wire transfer leaves the victim with few options.

10.2. Phony Escrow Services [Internet Crime Complaint Center (IC3). 2008a] (Chapter 5 (5.4.5.) p. 73)

Fraudulent escrow services Web sites are created (or spoofed) by the perpetrators or compromise legitimate escrow service Web sites. The seller will direct the victim to this Web site and once the funds are transferred to the Web site, the seller discontinues contact.
Section 11 – Identity Theft

11.1. Identity Theft as a Vehicle (Chapter 5 (5.6.1.2.) p. 75)

Identity theft or identity fraud is used as a vehicle to commit other types of fraud schemes. We (the victims) are led to believe that we are signing up for an online job opportunity or providing information to a legitimate and trusted business. This occurs when responding to an e-mail requesting update of billing or membership information. The surrendered information could be used in a number of ways.

11.2. Primary Objectives of Identity Theft [Van Staden, C. 2007] (Chapter 5 (5.6.1.2.) p. 75)

The way in which identity information is used varies depending on the size of threat that can be committed by perpetrators. The details can be used to commit fraud and espionage to kidnapping and extortion. The primary objective of identity theft, in most cases, is to use the information for personal gain.

11.3. Identity Theft Figures Escalate in Numbers (Chapter 5 (5.6.1.2.) p. 75)

An estimated 9 million Americans have their identities stolen each year, as estimated by the Federal Trade Commission (FTC). The figures in South Africa cannot be estimated as they are not made available, although the problem is escalating.

The risk of identity theft materializes through the use of fake bank accounts and/or credit cards. Based on US research, it takes an average of 500 days before the victim becomes aware that their identity has been stolen.

Common methodologies of achieving identity theft involve schemes such as phishing, spoofing, malicious software, key loggers, social engineering, interception of communication and 419 scams.
Appendix 5

Part III
Internet Crime Schemes

Chapter 6
Preventing MO Subterfuge

Section 1 – Credit Card Fraud

1.1. Skimming [Internet Crime Complaint Center (IC3). 2008b] (Chapter 6 (6.1.1.2.) p. 85)

Anyone who has physical access to a credit card can swipe away at this information by using a special storage device when processing the card. Skimming occurs when a fraudster obtains credit card information illegally, and to prevent this from occurring we must do the following:

- Never allow the credit card out of our sight, or allow anyone else to handle the card, such as attendants or waiters, and ensure that the transaction occurs completely in full view.
- When using the credit card, never provide any personal information.
- When using a credit or debit card at an ATM, always ensure that:
  - The card is quickly and easily available when approaching an ATM.
  - The card enters the slot easily. Do not force the card as the ATM may have been tampered with.
Appendix

1. Be wary of people lurking around ATMs and ensure that no hidden cameras are placed above the keypad.
2. Never write the PIN down anywhere, especially not on the card, or reveal the PIN to anyone.
3. Never accept help from strangers at an ATM or use an ATM with a blank screen.
4. Never insert the card or key in the PIN until prompted to do so by the ATM.
5. Ensure that the card transaction limit is as low as possible and do not count cash at an ATM or anywhere in public.
6. Never leave the ATM receipt behind.

1.2. The New Microchip or Smart Card [Watson, L. 2008] (Chapter 6 (6.1.1.2.) p. 85)

Microchip or smart cards will be replacing the conventional magnetic strip cards. This prevents criminals from easily duplicating the information stored on the magnetic strip, although nothing is a guarantee. Fraudsters are always able to overcome security measures in one way or another, as they continue to refine their techniques.

2. Section 2 – Phishing

2.1. How to Spot a Phishing Scam (Chapter 6 (6.2.1.2.) p. 89)

The “from” field can easily be changed to reflect anything that the perpetrator wants it to display and this can be done in a matter of seconds. The attacker gains the victim’s trust and authority and all e-mail sent will be sent straight to the attacker’s inbox. The Sender Policy Framework (SPF) helps to prevent e-mail spoofing. SPF allows software to identify forged e-mail addresses and reject them.

It is easy to spoof e-mail because the SMTP lacks authentication.

This section will consider the warning signs to look out for, misleading links, the status bar and location line, spoofing e-mails, common phishing phrases, what to do if phisher e-mail is received and how to report a phishing e-mail.
2.2. If Phisher e-mail is Received [MSN.co.za. 2008] (Chapter 6 (6.2.1.2.) p. 89)

When an e-mail has been downloaded and appears to be a phishing scam, report it immediately to the company that is being misrepresented. The company may have an e-mail address dedicated to report such abuse. Ensure that the e-mail address is typed.

The phishing scam can also be sent to the appropriate authorities:

1. The FBI through the Internet Fraud Complaint Center at www.fbi.gov which works with law enforcement worldwide to shut down phishing sites and identify perpetrators.
2. The Anti-Phishing Working Group (an e-commerce trade association) at reportphishing@antiphishing.org.

2.2.1. What are the Warning Signs? [MSN.co.za. 2008]

The best protection against any scam, especially the well-known phishing scams, is to display caution at all times. Don’t react immediately and look for the warning signals usually displayed in an e-mail. Although it is very difficult even for experts to distinguish between a phishing scam or the legitimate e-mail, there are five important points to look out for:

- **Legitimate businesses will never ask for personal information in an e-mail.** If the e-mail requests personal information this should send off alarm bells.
- **Displays urgency** and threatens to suspend the account if immediate action is not taken by responding with personal information.
- **Grammatical and spelling errors.**
- **If it sounds too good to be true, it probably is.**

2.2.2. Beware of Misleading Links
It is important to note that the clickable link provided in the e-mail we receive can display anything the perpetrator wants it to display to mislead us. The text clicked is "here", or may also read something similar to "Log in to Yourbank" or "www.yourbank.co.za/secure" to be even more misleading. These are also known as spoofed Web sites, which are covered in Chapter 5, section 5.2.2. Pay careful attention to the bottom left-hand corner (status bar) of the screen which will display the actual name of the server being contacted. Also when we hold our mouse over a link, the status bar will also display where the link points to.

2.2.3. The Status Bar [Anti-Phishing.info. 2008] (Chapter 6 (6.2.2.1.) p. 90)

The status bar is not always reliable when spotting a phishing scam. The attacker may use JavaScript to rewrite what is displayed in the status bar when the link is clicked or when the mouse is hovered over the link. Hence, this makes the con game even more convincing.

2.2.4. The Location Line [Anti-Phishing.info. 2008] (Chapter 6 (6.2.2.1.) p. 90)

The location line (where we type a URL in the browser) will display where the request is being directed to. This URL may change while the page is being loaded, giving an indication that an attack is in progress. This clue can be hidden by the use of JavaScript, which replaces and displays the fake URL (which is the correct URL we expect to see) in the expected place of the location line. URLs can also be typed in normally, as the fake location line can also accept keyboard input and can be rewritten by the JavaScript program before being accessed.

Another source which can be attacked using JavaScript is the menu bar, which is discussed in Chapter 6, section 6.2.2.2.

2.3. Spoofing E-mails (Chapter 6 (6.2.1.2.) p. 89)

Similarly to a spoofed Web site, the e-mail will contain logos, slogans, images and the same look and feel as the original company’s image on the Web and elsewhere.
Additionally, some of these elements may be spotted which do not always appear in every scam:

- Company logos which are not an exact match to the original logo.
- Spelling and grammatical errors.
- The hyperlink contains percentage signs followed by numbers or @ signs.
- Random names or e-mails contained in the e-mail.
- The company mentioned in the e-mail has nothing to do with the e-mail headers.

**Common Phrases [Microsoft. 2008]**

As scam artists become more sophisticated, their phishing e-mail messages and pop-up windows become more sophisticated as well. Some indicators to identify a fraudulent e-mail message may include some common phrases:

- "**Verify your account.**"

When an e-mail is received asking to update credit card information, do not respond as this is a phishing scam. Additionally, businesses should not ask anyone to send passwords, login names or other personal information through e-mail.

- "**If you don’t respond within 48 hours, your account will be closed.**"

Phishing e-mail may be written in an urgent manner, so that a quick response is initiated without thinking. In some cases, this type of mail may claim that the account has been compromised and needs an urgent response.

- "**Dear Valued Customer.**"

Phishing e-mails are normally sent out in bulk and often will not contain the recipient’s first or last name.

- "**Click the link below to gain access to your account.**"

Phishing mail may contain links or forms that need to be filled in. The links normally redirect us to a fraudulent or
spoofed Web site; therefore never click on any link contained within an e-mail. Delete the e-mail also from the deleted items folder to ensure that it is not accidentally clicked on again.

To allow peace of mind and to ensure that our account details are valid, it is recommended that the URL be typed manually into our Internet browser of choice to double check that everything is in order. Alternatively, we may phone our bank to verify that everything is in order.

2.4. If Phisher E-mail is Received [MSN.co.za. 2008] (Chapter 6 (6.2.1.2.) p. 89)

When an e-mail has been downloaded and appears to be a phishing scam, report it immediately to the company that is being misrepresented. The company may have an e-mail address dedicated to report such abuse. Ensure that the e-mail address is typed in manually and not generated from a link.

The phishing scam can also be sent to the appropriate authorities:

1. The FBI through the Internet Fraud Complaint Center at www.fbi.gov which works with law enforcement worldwide to shut down phishing sites and identify perpetrators.
2. The Anti-Phishing Working Group, which is an e-commerce trade association, at reportphishing@antiphishing.org.

Reporting Suspect E-mail with its Original Header [MSN.co.za. 2008]

Technical experts require the header information of an e-mail message. Without it they may be unable to flush out a thief or even track down the investigation. To correctly forward the suspected fraudulent e-mail, follow these simple steps in Microsoft Office Outlook:

1. Without double clicking on the message, right click the message in your inbox.
2. From the context menu choose “Message Options...”.
3. Right click in the Internet Headers panel and choose “Select All” from the context menu.
4. Right click in the Internet Headers box and choose “Copy” from the context menu.
5. Open the phishing e-mail and paste the copied text at the top of the message, and then forward the entire message.

Additional resources regarding phishing are described next.
2.5. Resources [MSN.co.za. 2008] (Chapter 6 (6.2.1.2.) p. 89)

- For the latest phishing schemes and statistics visit the Anti-Phishing Working Group at www.antiphishing.org.
- MSN Online Safety & Security (safety.msn.com) is a good all-around source of information. Additionally, go to safety.msn.com/phishing for more information on phishing.
- Visit the Anti-Phishing Working Group at http://www.antiphishing.org, for more information on phishing and e-mail spoofing.

Section 3 – Spoofing

3.1. Technological Solutions (Chapter 6 (6.2.2.) p. 90)

Spoofing is a technological problem needing a technological solution. Since e-mail uses SMTP, which operates without authentication mechanisms, the obvious solution would be to implement a technique which does require authentication. Mail system administrators will be able to publish Sender Policy Framework (SPF) records for their domains. SPF allows SMTP servers to check the mail headers against the outgoing mail servers in DNS. This allows the owners of domains to determine whether an e-mail address has been spoofed or not.

Mail system administrators will be able to set their domains to allow only authenticated mail to be sent by recipients. The authentication mechanism will be implemented by enabling Simple Authentication Security Layer (SASL)) SMTP by each user.

3.1.1. PGP

Another technique that can be used at our own discretion is PGP. PGP stands for Pretty Good Privacy and provides extra security and authentication, encryption and decryption mechanisms to e-mail messages sent and received between users. A technical discussion on how PGP works is provided in Chapter 7.
3.1.2. Clearing the Cache

Caching occurs when the Web site we are viewing is stored on our computer. Instead of re-requesting the same Web page from the server, there is a stored copy available for quick retrieval purposes. An online banking site should deliver instructions not to cache the information. Internet Explorer ignores these instructions, and to prevent this from occurring, you may need to change the settings:

- Click on Tools > Internet Options > Advanced tab > Do not save encrypted pages to disk
- Click on Tools > Internet Options > Advanced tab > Empty Temporary Internet Files folder when browser is closed

3.2. Defending Against Spoofing Attacks (Chapter 6 (6.2.2.) p. 90)

There are a few precautions that can be taken to limit IP spoofing risks on our network, such as configuring our border router, configuring a firewall, ensuring proper authentication mechanisms and ensuring the integrity of messages.

3.2.1. Configuring Border Router [Tanase, M. 2003]

Configuring the border routers is a good defence mechanism. The router, if configured properly, can prevent an outside attacker from spoofing the address of an internal computer and using the internal computer to carry out the attack. Blocking such incoming packets is known as ingress filtering. Addresses within the internal range of the source should not be accepted, as this is a common technique to get around firewalls. Egress filtering is restricting the source address outside the valid range. This prevents someone on our network from sending spoofed traffic to the Internet. See the cartoon strip below.
3.2.2. Configuring a Firewall

Firewalls can defend against spoof attacks provided they are configured to accept connections from certain IP addresses. Although source IP addresses are unique identifiers, this does not mean they are reliable because an IP address can easily be spoofed. Firewalls are covered in more detail in Chapter 7.

3.2.3. Ensure Proper Authentication Mechanisms [Tanase, M. 2003]

Ensure that proper authentication mechanisms are suitable and all communications are transmitted over a secure channel. Encryption and authentication implementation is included in IPv6 (Internet Protocol version 6, also known as IP next generation), which is designed as an upgrade to the IP. The current version is IPv4 (Internet Protocol version 4). The design of IPv6 allows more data traffic to be transmitted and the number of
hosts (computer with an IP address which contains data and is connected to a TCP/IP network) to be connected to the Internet. At the time of writing, IPv4 was used in conjunction with IPv6 and in the future IPv6 will help to eliminate current spoofing threats.

3.2.4. Ensuring Integrity of Messages [Tanase, M. 2003]

Integrity of information and authentication can be used to ensure that messages are from whom they appear to be. Cryptographic signatures (covered in chapter 7) can be used to ensure the integrity, authenticity and authorization of the messages sent and received to a particular party. An example of cryptographic signatures is PGP.

Warning signs to look out for when involving DHL or UPS as part of a fraud scheme:

- If the DHL or UPS logo is used in any e-mail communication, be wary of the individual, and contact DHL or UPS to confirm the authenticity of e-mail communications.
- DHL and UPS do not collect payment directly from customers.
- Be suspicious if asked to ship packages to an overseas home office and when dealing with individuals in a foreign country.
- Any business associated with DHL or UPS is for shipping costs only and never for other types of fees involving online transactions.
- If money is requested before the goods will be delivered, be cautious and do the necessary research.
- If the individual claims that his country will not allow direct business shipments, this should set off alarm bells.
- Be suspicious if the shipping address belongs to you but the name is not yours. So, do not accept packages that you did not order, meaning they can be refused, or you may contact the company where the package is from.
5.1. Minimizing Risks of Spyware (Chapter 6 (6.3.1.2.) p. 96)

When a large number of spyware programs have infected a Windows computer, a clean reinstalliation is needed in order to rid all the spyware and restore the system’s full capacity. Doing a format procedure every six months is recommended, as other types of spyware can modify system-critical files and procedures, making it difficult to detect and remove completely. Spyware may even prevent anti-spyware or anti-malware programs from being installed, uninstalled or from executing.

Spyware may open doors to further virus infections by disabling firewalls, anti-spyware software and browser security settings. Firewalls, anti-spyware software, anti-virus software and browser security settings are discussed in Chapter 7.

There is no browser on the market that guarantees full security; hence the resulting higher risks of being infected with spyware. Some users opt to use an Internet browser other than Microsoft Internet Explorer because the target market is smaller and less popular. Such Internet browsers include Mozilla Firefox and Opera. By using a different browser as opposed to the most popular ones, a lot can be done to minimize the chances of malware download that may be lurking in almost every Web site or e-mail.

5.2. If Computer is Exposed to Malware [OnGuard Online. 2008a] (Chapter 6 (6.3.1.2.) p. 96)

If the system’s performance has been degraded, such as its speed, then there is a good chance that the computer had been exposed to malware. Keep a look out for unusual behaviour, and if this is the case take the following precautions to reclaim control over personal data:

- Disconnect from the Internet, and stop shopping, banking and other online activities involving passwords or other sensitive information.
At a minimum, the computer should have anti-virus, anti-spyware and firewall software packages installed and these should be active as well as fully updated.

Once all anti-malware packages are confirmed to be fully updated and active, run a full system scan to identify any problems. If any problems are identified, be sure to delete them.

If you think the system may still be infected, try running a different reputable anti-virus or anti-spyware package.

Once all malware had been removed, think about how it can be avoided in the future. There are golden rules to help prevent malware from infecting the system.

---

Section 6 – Key Loggers

6.1. If The System is Infected with Viruses or Trojans [Anti-Phishing Working Group. 2008] (Chapter 6 (6.3.2.) p. 96)

The following safety precautions and checks must be done to ensure system safety:

- Install anti-virus, anti-spyware and personal firewall software (more information on these in Chapter 7).
- Update anti-virus, anti-spyware and personal firewall software.
- Once anti-spyware, anti-virus and firewall packages are fully updated, run a full system scan.
- Ensure that every connection allowed by the firewall is correctly configured.
- If we suspect that our system has been compromised, we need to repair the damage and change all passwords to all accounts in case the current password was sent to the intruder.
- Check all other accounts such as eBay, PayPal, e-mail ISP, online banking account, online trading accounts, Amazon.com and other e-commerce accounts and any other accounts to which we hold a password.

Key loggers may also be found in the form of hardware and physical inspections must be done. The common placement for such a physical device is on the tower where the keyboard input is found. Becoming a victim to key logging strategies can be prevented. The following section provides tips on how this can be done.
6.2. **Tips to Prevent Key Logging (Chapter 6 (6.3.2.) p. 96)**

The following tips will help prevent us from becoming a victim to key logging scams:

- Do not do Internet transactions and online banking through a public terminal, such as Internet cafés.
- If we need to complete a transaction urgently and have no access to a secure computer, we need to change our login details (such as username and password) as soon as we get access to a secure computer. If possible, use the bank’s cell phone services.
- Delete and do not open any e-mails that may come from a source we are not familiar with.
- Ensure that our computer is locked when unattended and is protected with a password at all times.
- Look out for any hardware changes that may have occurred. Some operating systems alert us when such changes take place.
- Always update and install the latest versions of anti-virus, firewall and anti-spyware software packages.
- Immediately change all our passwords and details if we think our details may have been compromised. Contact the bank immediately in case we typed in our credit card details.
- When ending an online banking session or Internet transaction, ensure that we log off every time and close the browser window we were using.

---

**Section 7 – Peer-to-peer File-sharing (Chapter 6 (6.3.4.) p. 97)**

**Avoiding Unrestricted Access to Important Documents**

Some security aspects that must be considered carefully to avoid unrestrained distribution of confidential documents, such as tax returns, e-mail messages, medical records, photos, account statements and other personal documents – along with the files you want to share – are listed below:
• **File-sharing software must be installed carefully.** Any changes made to the file-sharing application’s default settings could allow access to more than just the shared folder.

• **Monitor the system constantly with security software and regular updates.** Some file-sharing applications may install malware and adware that monitors our actions and sends this information to a third party. Ensure that the firewall is always on when connected to the Internet, and all anti-malware programs are continually maintained. Before opening any downloaded files, scan them for malware.

• **Disconnect from the Internet.** Most people who have broadband connections are always connected to the Internet. Moreover, the file-sharing application may constantly be running in the background, even if the window is closed. This allows open access to files by anyone and at any time. Set the preferences or controls in the application to not automatically start up each time the computer boots up.

• **Create separate user accounts.** Set up accounts with limited user rights to prevent other users from downloading and installing malicious software and accessing others’ folders and subfolders. In addition, set up passwords on security software to prevent other users with less privileged rights (other than administrative rights) from disabling or tampering with anti-malware and firewall software, compromising security.

• **Regularly back up sensitive documents.** In case of a computer crash, it is advisable to back up valuable files onto removable storage devices such as CDs or DVDs and keep them in a safe place. All sensitive information stored on the computer or elsewhere must be password protected, and even encrypted to prevent easy access in case a third party gains unauthorized access.

• **Restrict access with a personal firewall.** A personal firewall is useful to prevent and unauthorized, unidentified, external and incoming connections attempting to initiate communication with the server.
Section 8 – Advance Fee Fraud/Nigerian 419 Scams

8.1. Money Laundering [Internet Crime Complaint Center (IC3). 2008b] (Chapter 6 (6.4.1.) p. 101)

Money laundering refers to illegal financial transactions from an unknown or secret bank account source usually in a foreign country and is related to organized crime. The following tips should prevent us from becoming a victim of this type of fraud:

- If the offer or opportunity seems too good to be true, it probably is.
- If e-mails are received asking for personal banking information, do not respond.
- If individuals are representing themselves as foreign government officials, be extra cautious.
- Do extra research when doing business with people in a foreign country.
- When the e-mail talks about large sums, beware, especially when it requests assistance to place that money into overseas bank accounts.
- Keep all account information secret and private at all times.
- When additional fees are needed to further the transaction, this should send off alarm bells.

8.2. Job Scams/Business Opportunities [Oil Offshore Marine] (Chapter 6 (6.4.1.) p. 101)

Before running into a job opportunity which sounds too good to be true, we need to make sure we do a bit of research:

- We should analyze the company name and ask our friends and colleagues if they have heard of it before. Do an online search to see what others say about the company; whether they have been scammed by them or not and/or whether a company by that name even exists.
- Ask the company to provide copies of formal documentation and transcripts, such as a CK certificate and proof of registration as well as VAT numbers.
- If the company asks us to pay for a visa, work permit or air travel, it means there are job scammers behind the scam. The company may at first reply and inform us that there is no fee involved.
Appendix 5

- Check that the domain name matches the name of the company.
- Find out which country that company claims to be operating in. Phone or e-mail the embassy concerned to find out about them.
- Most fraudulent companies offer jobs in areas such as Africa (Nigeria being the most famous case), the Middle East, Asia and even South America, the US or Western Europe. When replying to unsolicited emails or advertisements for work-at-home employment, we need to take extra care, as these job offers are scams.
- When large amounts of earnings or profits are offered, claims that no experience is necessary or claims of product effectiveness should send off alarm bells.
- Do some research before dealing with people from a foreign country.
- When money is required up front for further instructions or products, take extra care. Preferably do not reply to the message or advertisement.

Ensuring that the Job Offer is Genuine [Oil Offshore Marine]

Receiving a job offer we have not applied for and have not been interviewed for clearly indicates a job scam. There are several methods to further ensure whether a job offer is a scam or not.

- Genuine companies will never use free e-mail providers to send an e-mail, such as gmail, hotmail, yahoo etc. We can check this by having a look at the e-mail address the e-mail was sent from.
- If the “from” e-mail address appears to be genuine and matches the domain name, there may be a chance that the company is in (false) existence. Furthermore, the domain address appears to be valid and in working order with an appropriate Web page uploaded. Read the e-mail carefully – if they offer a salary that cannot be refused, or ask for an advance payment via PayPal, cheque, EFT or ask for credit card and/or banking details, we must not send any form of payment or personal information.
- The fraudsters may only ask us for personal information, as mentioned above, after two weeks or even two months of interaction with us by e-mail or other communication media.
- Fraudsters may ask for additional personal information such as medical history, previous employment status, driver’s licence and identity details. We must not disclose any such personal information to anyone we are not familiar with and cannot establish whether they are who they say they are through official means.
If we feel we need to ensure that a company is genuine, we can send an e-mail to info@oil-offshore-marine.com, which will investigate the company for us and is a free service.

8.3. Lottery Win [Internet Crime Complaint Center (IC3). 2008b] (Chapter 6 (6.4.1.) p. 101)

When contacted claiming that we have won the lottery, or some sort of prize, we should be extremely cautious and take the following as guidelines to warn us if we are ever approached with such a claim:

- Be wary of lottery winnings that charge a fee before delivering the prize, if we did not enter a lottery contest, if we receive a telephone call claiming that we are the winner of a lottery or if demands are received to send additional money to qualify for future winnings.
- Do extra research when communicating with people in a foreign country.
- If the winnings seem too good to be true, they probably are.

**Section 9 – Identity Theft**


- We should always ensure we have accurate and complete records. We can resolve our case more efficiently in this way.

- Don’t end any calls until we are certain that we understand everything that we have been told. In case we need more help, we should ask to speak to a supervisor. Write down the names, contact details, what has been told to us by that person and the date and times on which we conversed with that particular person. All contacts we have made on the phone or in person must be followed up in writing. Use certified mail, return receipt requested in order to document what the company or organization received and when.
Appendix 5

- It is important to always prepare a list of questions to ask the representative as well as any information we may have about our identity theft.

- The person that we talk to may not be willing to help or give all the necessary information. This is why we must have a plan before contacting a company.

- Remember that the laws governing our personal access to information provide us with the leverage to demand that the company provide us with any information that relates directly to us and our accounts.

- For any future correspondence, copies of all correspondence or forms sent must be kept.

- Keep the originals of supporting documents like police reports and letters to and from creditors. Send copies only.

- Ensure that we have easy access to our paperwork. It may be feasible to set up a suitable filing system.

- In case problems surface later on, old files must be kept on record even if the case has been resolved.

- Steps must be taken immediately to restore our good name. Such steps include filing a police report, checking credit reports, notifying creditors and disputing any unauthorized transactions.

- The use of companies such as the South African Fraud Prevention Service at www.safps.org.za can help to quickly circulate our details to all the major banks and retailers to try and stop the criminal use of our stolen identity.


The longer the victim’s inaccurate records stay uncorrected, the longer it will take to rectify and resolve the problem. Companies that have opened fraudulent accounts should be contacted immediately by phone and then followed up in writing. Victims of this type of crime should review their financial and credit reports frequently, once every three months in the first year that the theft occurred and once a year thereafter.
The type of theft, problems related to correcting our credit report, whether the thief is caught or not, whether our personal information was sold or passed onto other thieves all play a factor in the time it will take to resolve the effects of identity theft.

Stay alert for other signs of identity theft.


We need to educate our colleagues and devise awareness programmes in our company. We should also educate our friends and family to be aware of identity theft threats and how they materialize (discussed in detail in Chapter 5). Awareness is an effective weapon against many forms of identity theft and make identity thieves’ jobs more difficult.

Be aware of how information is stolen and what we can do to protect ours. We should monitor our personal information to uncover any problems quickly and know what to do when we suspect our identity has been stolen.

Although millions of people’s identities are stolen each year, we can do a great deal to minimize the threats of identity theft and avoid becoming a victim.

Be aware of the DDD (pronounced “triple d”) rule to protect our information and ourselves:

- **DETER**: Protect our data and information from identity thieves.
- **DETECT**: Review all financial statements regularly for any suspicious activity.
- **DEFEND**: React immediately and accordingly if there are any charges which we did not make.

9.4. If Our Information has been Compromised, But Not Yet Misused (Chapter 6 (6.6.1.) p. 106)

Becoming a victim of identity theft can cause enormous inconvenience. This is due to the possibility of having our information misused and the thought of unauthorized access to our financial data. We may have responded to a phishing e-mail (discussed in Chapter 5) or other.
If a company informs us that it experienced a breach and that some of our personal information has been compromised, the company may offer free credit monitoring. It is advisable to accept this offer as credit monitoring from a reputable company can help us quickly detect any misuse of our identity.

Take steps as defined above to respond to and recover from identity theft as soon as we suspect it.

(Chapter 6 (6.6.1.) p. 106)

- Ensure that Web sites are secure prior to submitting our credit card number.
- Do our homework to ensure that the business or Web site is legitimate.
- Attempt to obtain a physical address, rather than a P.O. box or mail drop.
- Never throw away credit card or bank statements in usable form.
- Be aware of missed bills which could indicate that our account has been taken over.
- Be cautious of scams requiring us to provide our personal information.
- Never give our credit card number over the phone unless we make the call.
- Monitor our credit statements monthly for any fraudulent activity.
- Report unauthorized transactions to our bank or credit card company as soon as possible.
- Review a copy of our credit report at least once a year.

The Internet is a public place. Do not give out any personal information such as our telephone numbers, address or credit card information in chat rooms or in newsgroups.
Appendix 6

Part IV

General Preventative Measures

Chapter 7

Tips, Non-technical and Technical Preventative Measures

Section 1 – Non-Technical Preventative Measures

1.1. Methods for Attacking Encrypted Text (Passwords) (Chapter 7 (7.1.1.) p. 118)

This section has been included as it is useful for us to understand why it is important to have and maintain a strong password. By understanding how cyber criminals are able to gain access to our passwords, it will be easier to make more informed decisions before willingly or unwillingly compromising our password (see Table 1).

<table>
<thead>
<tr>
<th>Method</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptanalysis</td>
<td>Practice of attempting to obtain the clear text of a message without authorization. Cryptanalysis techniques require specialized knowledge and skills.</td>
</tr>
</tbody>
</table>
3.4.2 Passwords guess

Highly effective approach. Password may be a dictionary word; otherwise password is something directly related to us. Many specialized dictionaries are available for different areas of interest and different languages. Dictionary attacks are normally software-enabled.

Brute force attack

Attempting to methodically crack all possible sequences of characters in a password.

Scavenge password

Very effective approach. Password (in clear text) may be captured while in transit over the network. Otherwise, password is likely to be written down somewhere physically or in a document/e-mail message if it is not easy to guess.

Extract password

Plain text password may be found in a standard location, such as the system registry. Software-enabled attacks are very simple and practical. Many types of Windows passwords are stored within the registry or other configuration files.

Obtain password

The easiest way to obtain the password is by interview, provided the victim is cooperative. Otherwise, the victim may be tricked into revealing his password, or under extreme circumstances may be forced to reveal the password.

Recover password

If some sort of administrative or password recovery service is available, the system administrator will give the password to use or will reset it. A good systems administrator never reveals the password.

Find plain text

Locate unencrypted copies of desired data on hard drive.

1.2. Tips on Choosing and Memorizing Passwords (Chapter 7 (7.1.1.) p. 118)

Forgotten passwords are common. Weak passwords and using the same password for every Internet service are also very common. There are techniques available to help us remember our chosen password for each service we subscribe to.
1.2.1. Password Technique

When choosing a password at a registration page, choose the word that first comes into mind. For example, when signing up for an online banking account the first thing that may come into mind when having to think of a word is “onlinebanking”. Use this word, but alter it – change the ‘o’ to a 0 (zero). Perhaps change the ‘a’ to a 4 and the ‘e’ to a 3. The letter ‘i’ can also be changed to reflect a 1. The new word will look like this: “0nl1n3b4nk1ng”.

This will make it much more difficult for any perpetrator to randomly guess our passwords.

1.2.2. Benefits of the Password Technique

- We can remember passwords for each and every Web site, without writing them down or trying to remember them.
- The replacement of each chosen letter follows our own conventional method (i.e. ‘e’ will always be a 3).
- With a bit of imagination, chosen passwords can be anything and not directly related to us.
- Passwords will not be easily forgotten if the first thing that comes to mind on a particular Web page is used; it will always be the first thing to come back to mind.

1.2.3. Password Technique Cautions

- It is not advisable to alter too many characters into too many different variations. It may become confusing and more difficult to remember.
- Sometimes altering a password of a minimum of six to eight characters requires the alteration of only one to two characters.

1.2.4. What Not to Do

- Don’t use a password that is the same as your username as this can be easily guessed by fraudsters.
• Don’t select a password that is a dictionary word, as this is susceptible to dictionary attacks.
• Don’t select a password that is directly related to us, such as names, birth dates, etc.

1.2.5. **Recommendation**

• Using a different password for different online services increases privacy and security. If a password is accidentally compromised for one service, it means the fraudster will not be able to use the same password to gain unauthorized access to other confidential and financial accounts.

---

**Section 2 – Technical Preventative Measures**

---

**Section 2 – Anti-virus**

2.1. Anti-virus Performance Comparison [ESET. 1992-2008b] (Chapter 7 (7.2.1.4.) p. 123)

The effectiveness of the anti-virus product and the technology it uses is what stops malware – not brand names. ESET NOD32® Antivirus is effective in its detection, size and speed when compared to other anti-virus products.

Approximately 80% of threats, such as MyDoom, Netsky, Bagle and Mytob, were heuristically discovered by ESET, well before other vendors had issued a definition signature. The “In-the-Wild” Virus Bulletin Tests show the results of the number of missed viruses and their respective vendors (see Figure 15).

In testing done by AV-Comparatives, an independent testing agent, ESET proved to reliably detect viruses producing the least false positives (see Figure 16).
The following chart illustrates that ESET NOD32® Antivirus includes one of the fastest anti-viral scanners in the industry. This means that the product also does not tax resources (see Figure 17).
Based on the statistics, ESET NOD32® was named "Best Antivirus Product" for 2006 and 2007.

### 2.2. Anti-virus Comparison Charts. Which is the Best Anti-virus? [ESET. 1992-2008b] (Chapter 7 (7.2.1.4.) p. 123)

The anti-virus comparison chart outlines the protection as well as performance levels of each of the well-known anti-virus product brands. The comparison chart can be used to conclude which brand will best suit a particular user’s needs. See Table 2.

<table>
<thead>
<tr>
<th>Comprehensive Protection</th>
<th>ESET NOD32® Antivirus</th>
<th>Symantec</th>
<th>McAfee</th>
<th>Trend</th>
<th>Kaspersky</th>
</tr>
</thead>
<tbody>
<tr>
<td>VB100 Awards for detection of all In-the-Wild viruses in the VB test sets without any false-alarms (virusbulletin.com, May 1998 - June 2008)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>44</td>
<td>34</td>
<td>16</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>12/1/0</td>
<td>5/3/5</td>
<td>2/9/2</td>
<td>0/0/3</td>
<td>8/2/3</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix 6

**Advanced+ Awards Tests of proactive and on-demand detection** *(AV-Comparatives.org, May 2005 - May 2008)*

<table>
<thead>
<tr>
<th>Advanced+</th>
<th>Advanced</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed in-the-wild viruses in Virus Bulletin tests between May 1998 and June 2008 <em>(virusbulletin.com)</em></td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>On-Access</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>On-Demand</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Real-time protection against 16 zero-day viruses *(virustotal.com)* | 87% | 7%* | 33% | 0% | 13% |
| Retrospective/Proactive Test by 3-month old signatures *(May 2007)* | 68% | 24%* | 24% | No Data | 9% |

| Performance Scanning throughput of Media files and documents on Windows Server 2003 *(virusbulletin.com, February 2008)* | 46.7 MB/s | 20.5 MB/s | 27 MB/s | No Data | 16.4 MB/s |


---

ESET NOD32 Antivirus or Smart Security is available as a free trial version for 30 days: [http://www.eset.com/download/index.php](http://www.eset.com/download/index.php)

#### 2.3. Useful Links (Chapter 7 (7.2.1.4.) p. 123)

Visit [http://www.av-comparatives.org](http://www.av-comparatives.org) for the latest reports on anti-virus product comparisons.

AVG Anti-Virus and Internet Security’s home page provides links to Virus News, Useful Tools, General Information on Virus and Security Topics and Anti-Virus Software Tests. This information can be accessed from [http://www.grisoft.com/ww.64](http://www.grisoft.com/ww.64).

### Section 3 – Anti-spyware

#### 3.1. When a Spyware Program Installs Itself [Spyware-Free. 2007] (Chapter 7 (7.2.2.) p. 123)

Usually when spyware infects a computer it can be very difficult to detect. Spyware can hide within system-critical processes and leave no on-disk signatures. Some of these infections may even start up in safe mode which enables the anti-spyware program to remove persistent spyware in a more effective manner.

Booting up in safe mode may be a solution to removing persistent spyware resisting attempts to uninstall it. In some cases, when the spyware is removed it can reinstall itself by regenerating another process of itself. Similarly, this process also applies to registry keys installed in the Windows registry system.

There may even be a resistance to well-known anti-spyware programs and spyware programs can prevent them from being installed or operating correctly or can even uninstall it.

#### 3.2. Rogue Software [Computer Cleanup. 2007] (Chapter 7 (7.2.2.) p. 123)

Many Web banner ads advertise or alert us that our computer has been infected with spyware. These advertisements offer the download of an anti-virus or anti-spyware program to clean the infected registry and computer system. A fake anti-spyware program is downloaded to the victim’s computer (sometimes at a purchase price) which
may introduce back doors to accessing our information and further install additional spyware and malicious software on the system. This type of software is called rogue software.

Known offenders include Privacy Defender, Malware Wipe, Pest Trap, SpyAxe, AntiVirus Gold, SpywareStrike, SpyFalcon, WorldAntiSpy, WinFixer, Spy Sheriff, SpyBan, SpyWiper, PAL Spyware Remover, PSGuard, AlfaCleaner, VirusBurst, Trustcleaner Pro and AntispywareSoldier.

3.3. Security Practices [Computer Cleanup. 2007] (Chapter 7 (7.2.2.) p. 123)

In addition to installing and maintaining anti-spyware software programs on a system, there are other useful security practices which can be applied.

Awareness is a key factor when downloading shareware programs. We need to ensure that the programs downloaded are from reputable resources only, which will provide us with some protection against directly harming our computer.

To prevent spyware from entering a system, ISPs may use their network firewalls and Web proxies (a Web proxy is a server installed either locally, or somewhere on a network, used to request a resource on the client’s behalf) to block access to Web sites known to install spyware. This technique is common in colleges and universities.

To prevent computers from connecting to spyware-related Web addresses, some users install a large host file. A host file is a computer file used on networks as a DNS, which maps hostnames to an IP address. However, spyware may bypass this sort of protection by connecting directly to the numeric IP address.
Section 4 – Firewalls

4.1. Inbound vs. Outbound Filtering [SecurityFocus. 2007] (Chapter 7 (7.2.3.3.) p. 126)

There are certain types of malware which anti-virus programs cannot detect. These types of hidden malware nestle into the computer system and establish connections to external sources. These events could lead to the infected computer becoming a “zombie” or “drone” under the control of third-party sources. The firewall blocks and prevents such connections’ access into cyberspace, eliminating the risk of PII leakage. Outbound filtering will notify us of any unknown connections wanting to access the Internet which may constitute spyware. On the other hand, inbound filtering needs to be configured to disallow illegitimate connections from being established on our computer.

4.2. Application Integrity (Chapter 7 (7.2.3.3.) p. 126)

The firewall will, or should, notify and alert us when any major alterations have taken place to an application. Alterations can be due to an upgrade, but can also take place by malicious programs, which could be harmful to our computer.

4.3. Computer Anonymity on the Internet (Chapter 7 (7.2.3.3.) p. 126)

On a typical computer with no firewall, an intruder may be able to find out what operating system we are using, as well as other information such as who our ISP is, and may take the time to find out more information about our computer. If we choose to implement a firewall, any attempts to establish a remote connection with our computer will be void. The intruder will not get a response and this will discourage him from investigating further.

4.4. Firewall Limitations (Chapter 7 (7.2.3.3.) p. 126)
Firewalls are thought of as providing protection against intruders. This statement is quite the contrary to what types of protection the firewall really provides.

Firewalls listen for the types of communications established to and from our computer, which programs are gaining access and the source and destination of the communication. For instance, we can block access to and from an Internet Web browser, although this is not a realistic solution, as this type of communication needs to be allowed in order to browse the Internet. The Web browser may have a security vulnerability through which intruders may gain access to the computer. The firewall will not be able to distinguish between the content of communication and between the intrusion and a legitimate connection to another Web site.

Consequently, the concept of the firewall’s capability to understand specifics about a certain communication is very limited.

In an attempt to mitigate this type of exploitation some firewalls are equipped with Trojan horse and intrusion detection capabilities. These built-in features may be useful, although are normally handled by typical anti-virus programs, which contradicts the perceived definition of a firewall.

4.5. Firewalls: Our Responsibility (Chapter 7 (7.2.3.3.) p. 126)

The purpose of a firewall is not to make informed decisions on our behalf. This means that we cannot merely install a firewall and forget about it. We have to indicate legitimate and illegitimate connections which should or should not be allowed. Sometimes we are not knowledgeable enough to make such decisions and may block access to an important service, such as one provided by the ISP, or may block connections needed for the system to function correctly.

Once the firewall has been installed it may be easier for us to dictate which connections to allow. However, we must gain an understanding of what programs and services should be allowed and when.

4.6. False Statements about Firewalls [Paz, U. 2002] (Chapter 7 (7.2.3.3.) p. 126)

Ten false statements made about firewalls will be presented below, each followed by the more accurate answer:
1. "If you use a broadband Internet connection (such as ADSL or cable), your computer is not safe without a firewall."

The longer a computer is left connected to the Internet at any one time, the more vulnerable it is to non-targeted intrusion attacks. Therefore the chances an intruder will take advantage without our knowledge is greater when we are connected on a broadband connection. The implementation of a firewall can add to the defence of the computer but should not be used as the only defence. Whilst a computer can be safe without a firewall, it can also be potentially unsafe when using a firewall.

2. “If you use a slow dial-up Internet connection, a firewall is not needed.”

The Internet connection speed does not determine whether a firewall is needed or not. Implementing a firewall whether our connection speed is slower or faster provides the same benefits in both instances.

3. “Using a firewall is a must, and is always better than not using one.”

There are known but rare cases where the firewall itself introduces additional security risks owing to security vulnerabilities present in the firewall program. A firewall is not always critical for the security of a computer and a firewall implemented on its own will rarely reduce security levels.

4. "Hardware firewalls are better than personal (software) firewalls."

Both hardware and software firewalls have their advantages and disadvantages and should be evaluated accordingly. The one which suits our needs the most is the one which should be implemented. In some cases, both hardware and software firewalls may be employed for added security levels.

5. "A firewall is more important than an antivirus program."

A home computer’s performance is more likely to be degraded and cause various setbacks through malware infections and intrusions without an updated anti-virus program as opposed to not implementing a firewall.

6. "I've heard that [XXX] is the best firewall."
We need to evaluate what we use the computer for the most and the advantages and disadvantages of each firewall. There is no right or wrong and each firewall is dedicated to different functionalities. There are excellent firewall packages available for free for home use and may be tailored differently for different users.

7. "Personal firewalls which are free for home use cannot be as good as those which cost."

There are better developed firewalls that are just as exceptional when comparing the firewalls which come at a price.

8. "Firewall [XXX] is ineffective, because it causes disconnections from the Internet."

This problem is likely due to misconfigurations in the firewall. Configure the firewall correctly instead of holding the firewall responsible.

9. "Some firewalls give me the details of the attacker, including location and phone number."

Acquiring the exact location and details to trace the attacker needs exceptional expertise. The main purpose of implementing a firewall is to protect our computer from unsolicited connections. The firewall’s logs, at most, provide only the details of the ISP from which the attack originated and identifying the attacker will not help much.

10. "Firewalls are useless because they can be bypassed."

Firewalls can be easily bypassed if a Trojan or similar infection already resides on our computer. Even then, an intruder must first find a way to deposit the virus on the target computer. Additionally, in most cases it is highly unlikely that an intruder will bend over backwards to hack into our home computer. Almost all intrusion attempts use one of two to three methods which are easily blocked by a firewall with a bit of user knowledge. Although there is no generic method for an intruder to bypass a firewall, just because a security system is not fool-proof does not render it useless.

4.7. Hiding the Computer [Paz, U. 2002] (Chapter 7 (7.2.3.3.) p. 126)
Many manufacturers of the personal firewall claim that their firewalls can hide the computer on the Internet from attackers. If the computer does not contain any software or specific services, the computer itself is neither a security nor privacy threat. But when using specific software, the firewall may be configured to allow such a service to be seen by third parties to allow communication (such as a Web browser). This means that the computer may only be partially scanned by attackers, and if they did not search for the specific service available on the computer then they will not see the computer. If the service residing on the computer is a common one, then there is greater chance for the attacker to find the existence of the computer, and decide to scan it further for any further security vulnerabilities.

**Anonymizer** [Garfinkel, S. Spafford, G. 1997: 96 - 97]

Anonymizing Web servers can be used as a solution to protect our privacy. However, if we are concerned about having our PII collected, that is precisely why we would be interesting to monitor.

Anonymizers act as a middleman between us (the user) and the original Web server. The software makes a request for the URL itself, making the destination server believe it is receiving a request from the anonymizing server. Requests are sent back to us in the same way, through the anonymizer software.

The software knows who has connected to it and what pages we have seen, and requires us to put trust in the organization running the service. This may not be the intent, but the possibility does exist.

Anonymizers have trouble with active content such as Java, JavaScript and ActiveX, and should be disabled if we want to truly surf the Web anonymously. This is because Java and ActiveX contain method calls that allow a running program to determine the name of the computer on which it is running. If this information is sent back to the original Web server, then the anonymizer is useless.
Section 6 – Secure and Recommended Internet Browsers

6.1. Stay Secure on the Web with Mozilla Firefox [Mozilla. 2005-2008a, b] (Chapter 7 (7.2.5.) p. 130)

Mozilla Firefox is an open-source development, meaning that the program and its source code are free for download and modification enabling skilled developers from around the world to make their contributions. Contributions from security experts ensure a more secure product with on-demand updates.

6.2. Spyware Protection with Firefox (Chapter 7 (7.2.5.) p. 130)

Our permission is needed before installing, running or downloading any software from a Web site and we will always be notified of what is happening to ensure that we stay in control at all times.

6.3. Phishing Protection with Firefox (Chapter 7 (7.2.5.) p. 130)

Firefox alerts us when we accidentally encounter a phishing (or spoofed) Web site. This feature protects us from phishing attempts to steal our identity and financial information. When Firefox alerts us of a fraudulent Web site, we may opt to be redirected to a search page to find the legitimate Web site we were originally looking for (see Figure 18).

6.3.1. How It Works
A list of known phishing sites is stored within Firefox and is automatically updated and downloaded regularly. We may also choose to have more up-to-date protection through Firefox by opting to check each site visited through an anti-phishing online service such as Google. The address of each Web site visited is sent using a secure SSL connection and no information about the sites we visit is sent when enabling phishing protection in default mode.

**6.3.2. Clearing Private Data in Firefox**

![Clear Private Data](image)

By using the Clear Private Data tool, we can be assured that all private Web browsing data is deleted, irrespective of whether it is a home or public computer (see Figure 19).

**6.3.3. Firefox Automated Updates**

Firefox has a built-in functionality which alerts us of new and available updates in over 40 different languages. The updates are normally small in size (200-700KB), ensuring a quick and easy update process.

**6.4. Web Browser Usage Statistics [Answers.com. 2008] (Chapter 7 (7.2.5.) p. 130)**

Table 3 illustrates the usage statistics distributed amongst the various Internet browsers available on the market.

<table>
<thead>
<tr>
<th>Internet Browser</th>
<th>Usage Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>77.86%</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>14.88%</td>
</tr>
<tr>
<td>Safari</td>
<td>5.07%</td>
</tr>
<tr>
<td>Opera</td>
<td>0.87%</td>
</tr>
<tr>
<td>Netscape</td>
<td>0.72%</td>
</tr>
<tr>
<td>Opera Mini</td>
<td>0.39%</td>
</tr>
<tr>
<td>Other</td>
<td>0.20%</td>
</tr>
</tbody>
</table>
7.1. Phishing Protection with Thunderbird (Chapter 7 (7.2.6.) p. 131)

When we click on a link within an e-mail message, the client will warn us when an attempt is made to redirect us to a URL not specified in the e-mail. Additionally, the client displays a warning when an e-mail may appear to be a phishing attempt to hand over personal information.

7.2. Thunderbird Robust Privacy (Chapter 7 (7.2.6.) p. 131)

Remote images are automatically blocked in e-mails to ensure that our privacy is maintained.

7.3. Cutting Out the Junk (Chapter 7 (7.2.6.) p. 131)

As we mark messages as spam, Thunderbird remembers these markers, enhancing security through its leading-edge junk mail filters. In addition to Thunderbird’s integrated mail filters, it can also use our mail provider’s mail filters to block spam and keep junk mail out of the inbox.

7.4. Open Source Security (Chapter 7 (7.2.6.) p. 131)

Owing to the vast contributions of experienced developers and security experts from all over the world, more security with quick and easy updates as well as the use of third-party scanning allow Thunderbird to further enhance security measures.
7.5. Thunderbird Automated Updates (Chapter 7 (7.2.6.) p. 131)

Firefox has a built-in functionality which alerts us of new and available updates in over 30 different languages. The updates are normally small in size (200-700KB), and check if we are using the latest version, ensuring a quick and easy update process.

Section 8 – Encryption Mechanisms (Chapter 7 (7.2.8.3.) p. 133)

Plug-in Features [Sourceforge.net. 2008]

- Automatically creates a public/private key pair for us upon loading the plugin.
- Automatically transmits our public key to other users.
- Supports 512 - 4096 bit keys.
- Saves keys of known users, and warns us if their public key has changed.
- Embeds all encryption and keys inside HTML, so if the other user does not have the plugin, they will get a message telling them about the plugin, and will not get a screen full of garbage.
- Automatically recognizes if we are chatting with someone who has the plugin.
- Modular and extensible. If we want to define a different type of encryption, we can use this plugin as a wrapper to take care of transporting the encrypted binary over the IM pipe.

Section 9 – Other Encryption Mechanisms and Techniques

9.1. Secure Shell (SSH) [Georgia Institute of Technology. 2002] (Chapter 7 (7.2.9.) p. 134)

SSH is a program which allows us to encrypt data to ensure the integrity and confidentiality of information before sending it over a network. SSH was originally
designed to ensure secure access between two computers over a network or Internet connection. Another factor was to mitigate the risks of the security issues, such as intercepted or stolen data, which exist on the Internet.

For more information on SSH visit www.ssh.com.

9.2. Single Sign-on [Georgia Institute of Technology. 2002] (Chapter 7 (7.2.9.) p. 134)

Single sign-on systems are mostly used in business and possibly university environments where there is more than one system each requiring more than one logon. They solve the problems of each user having to remember multiple passwords for multiple systems.

9.3. Kerberos Authentication (Chapter 7 (7.2.9.) p. 134)

Kerberos is a protocol and the first step toward an effective single sign-on solution. Kerberos provides authentication of secure password storage and encryption, including a centralized management base for changing passwords. A password expiration policy embedded within Kerberos enforces password changes every 90 days. Kerberos also provides an automated account creation for new employees.

9.4. VeriSoft (Chapter 7 (7.2.9.) p. 134)

VeriSoft is a client-server based enterprise single sign-on/network logon solution with robust multifactor authentication capabilities including world-leading support for fingerprint biometrics. Features include secure password management.


9.5. Secure IMAP vs. POP [Georgia Institute of Technology. 2002] (Chapter 7 (7.2.9.) p. 134)

The major difference between IMAP and POP is that when accessing electronic mail, a copy of the message is kept on the server.
9.5.1. POP

POP downloads and retrieves one copy of the original message from the server and the message cannot be retrieved multiple times. A copy of the original message is downloaded to the recipient’s computer and the original message residing on the mail server is deleted.

9.5.2. IMAP vs. Secure IMAP

IMAP is useful when electronic mail needs to be kept in a centralized location, making it accessible from more than one computer and from remote locations when needed.

One major weakness of IMAP is that the messages are transmitted using clear text. Secure IMAP resolves this issue by encrypting the data.

Key goals for IMAP include [University of Washington. 1996-2008]:

- Be fully compatible with Internet messaging standards, e.g. MIME.
- Allow message access and management from more than one computer.
- Allow access without reliance on less efficient file access protocols.
- Provide support for online, offline and disconnected access modes.
- Support for concurrent access to shared mailboxes.
- Client software needs no knowledge about the server’s file store format.

For more information on IMAP, visit http://www.imap.org/.