Global Information Assurance Certification Paper

Internet Fraud
- An Overview -

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Leo de Geus
21 February 2005

SANS Conference: Amsterdam September 2004

Paper Abstract
This paper gives a high level overview of Internet fraud, types of fraud, the consequences when becoming a victim of Internet fraud, techniques and tools used by scammers and detection / prevention measures for users and businesses.

Table of Contents

List of Figures

1. Abstract

This paper describes one of the biggest threats of the Internet at this moment, electronic or Internet scams. Fraud is one of the oldest crimes on earth. Over the years people have become more skilful in performing all kinds of fraud for own financial profit. Today, the Internet provides the scammer a very easy and save way to perform electronic scam. Completely save behind his* computer, he can use all kinds of electronic techniques and methods to perform his scam activities. Two very important aspects of the Internet are the best friends of the scammer; anonymity and scale of the Internet. He can do his job without a name or with a spoofed name, without being detected. Next to this he has an enormous group of potential victims for free to perform his scam. These two issues combined give the scammer incredible possibilities to con unsuspecting Internet users and steal their identity and/or money.

This document gives an overview of electronic scam performed via the Internet and with the use of e-mail. Several aspects on electronic scams are described including their relationships with each other. The most important electronic scams and dissemination methods are described. Next to this an important section will be detection and prevention of becoming a victim of electronic scams. Although this document does not cover every aspect and type of electronic scam it gives an overview of the most important, most frequently used and most dangerous electronic scams circulating on the Internet. The reader of this document should be warned going on the Internet doing his business. The threat of being stolen of his money and/or identity is high. However with some simple precautions and common sense the risk can be minimized.

* For document layout purposes the male format is used when referring to the scammer, victim or any other person in this document.

2. Introduction

Crimes like fraud or scam have always been around since the beginning of days. During the evolution of the Internet organized crime became aware of the enormous and unlimited possibilities of the Internet to extend their criminal activities. Cyber crime was born! Standard fraud activities (e.g. mislead people to give their personal information) could now be performed electronically via the Internet or e-mail which is a lot easier, faster, more efficient and with less risk to be discovered.

Cyber crime statistics seem to explode last few years. According to an article for the BBC New World Edition [1], Cyber Crime was booming in 2004. During 2004 almost every security threat has grown dramatically. The number of known viruses has exceeded the 100,000 barrier and the number of new viruses grew by more then 50%. The same trend is shown with phishing attempts which have grown more then 30% in the last year. Lycos Europe detected a 500% increase in the number of phishing e-mails. The third big issue in 2004 was the increase of the number of so-called "bot computers". The number of "bot computers" rose from 2,000 to 30,000 per day according to anti-virus vendor Symantec. A large number of "bot computers" together form a "bot net" or a "zombie network", which can be used as a gigantic remotely controlled e-mail "system" to send large numbers of spam e-mail messages. Spam was one of the biggest problems in 2004. About 70% of all e-mail messages were defined as junk e-mail or spam.

When does this trend stop? When will these security threats decrease? Not in 2005 according to Roger Thompson, director of content research security management at Computer Associates Inc. In an article for eWEEK Enterprise News & Reviews [2], he states that "Spy-ware will replace the mass-mailing worm as the biggest nuisance – and security threat – facing businesses in 2005". Mass-mailers were a big problem, still are and will be in 2005, however they can be stopped now. This in contrast to spy-ware which is a real threat for individuals and businesses because it presents a legitimate threat because of the way malicious code can be executed on infected systems and its consequences.

Time to panic? Answer: YES and NO. YES, if you stay passive and do not take precautions and implement the basic security detection and prevention measures (e.g. anti-virus programs, performing regular software updates and installation of a firewall), while surfing the Internet and reading e-mail. YES, if you do not use your common sense while clicking on a link in an e-mail message send to you asking for your login credentials to verify your account. YES, if you do not have a healthy dose of distrust in the (unknown) party with whom you are doing business with over the Internet or e-mail. NO, if you DO the things just mentioned. NO, if you read on and learn more about electronic scams, techniques used by cyber criminals to perform their evil scamming

activities and detection and prevention methods. After reading this document you will have a better understanding of the threats you are facing and how to fight them.

3. Types of Electronic Scam

There are many types of electronic scam. This section reviews the most common scams at the moment on the Internet. These types of scam are almost daily business for the regular Internet and e-mail user.

3.1 E-mail Scams

E-mail is the basis for most types of scams. Almost every Internet user has one or more e-mail addresses. For scammers this is heaven on earth, millions and millions of potential victims (normal users as well as businesses) can be approached for free. Besides this the sender address of the e-mail can be spoofed so this gives the scammer anonymity. Like the beginning of this paper stated, the extremely large number of unsuspecting potential victims and the anonymity provides the scammer powerful means of performing his job. The content of the e-mails can be anything to mislead people who open and read it. The next paragraphs describe some of the most common e-mail scam types on the Internet today. There are of course many more types of scam via e-mail however the principle is always the same. Furthermore, some types overlap with other types or combinations of types are used for one scam action. For example, the phishing scam in combination with fake websites can be used to steal credit card numbers but also to steal a person's social security number to take over his identity.

3.2 On-Line Identity Theft

On-line identity theft is one of the scariest scams at the moment. Could you imagine that someone takes over your identity? He is using your identity, your personal information such as your name, credit card number, social security number, drivers license, etc, without your permission. In fact he has stolen your life! The most likely scenario is that the scammer will use his new identity, YOUR identity, to steal money from you or perform any other illegal actions under your name. Do you think this is not going to happen to you? Watch the drama movie "Identity Theft", directed by Robert Dornhelm, made in 2004, starring: Kimberly Williams-Paisley and Annabella Sciorra [3]. This movie is based on a true story so yes, it can happen to you.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years including their hard-earned money and savings, cleaning up the mess on-line identity thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit [4].

Who are those people who perform this scam? GOVCERT.NL organized an international symposium on 19 August 2004, Den Haag, the Netherlands. One of the speakers, people from the Australian CERT (AusCERT), gave the following graphical representation of on-line identity theft scammers.

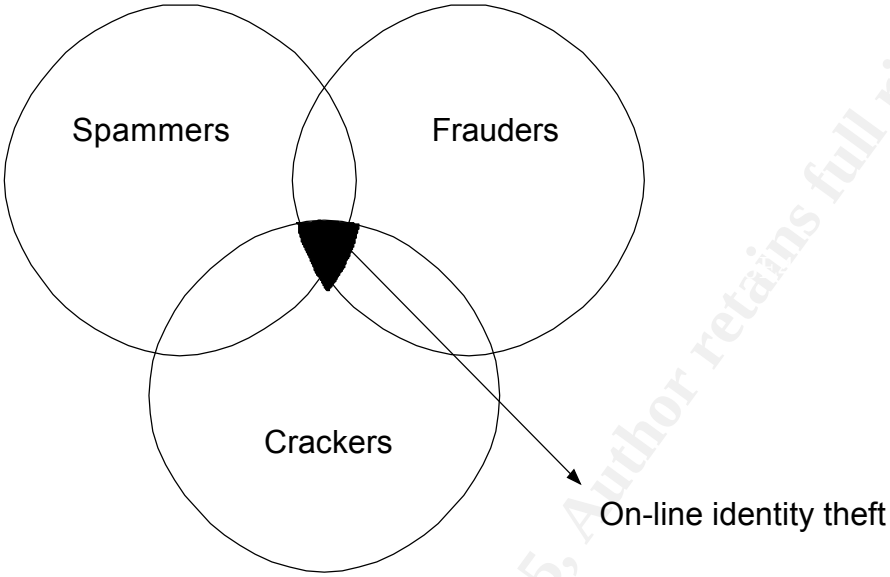

Figure 1, On-line identity theft revealed

As you can see there are three cyber crime groups who work together to perform the on-line identity theft scam. Spammers take care for the collection of e-mail addresses. Crackers enable the technical possibility to send the messages to unsuspecting potential victims while the frauders or scammers determine the scam scenario and content of the e-mails and handle the results of the scam.

AusCERT thinks that organized crime, active in the real world, is exploiting the electronic opportunities of the Internet. They co-operate with individuals or small groups of crackers and/or spammers. This is in accordance with the story of Phil Williams of the CERT Coordination Center [5].

GOVCERT.NL is the Computer Emergency Response Team of the Dutch government [6]. AusCERT is the Australian Computer Emergency Response Team for Australia and a leading CERT in the Asia/Pacific region [7].

3.3 Phishing

What is Phishing? Phishing is used by scammers to steal confidential personal data from people like login names (user IDs) and passwords, credit card numbers, social security numbers, etc. Spoofed e-mail messages in combination with fake websites are used by scammers to deceive people. Phishing scammers hijack trusted and well-known brand names like banks,

credit card companies, online retailers and so on [8].

How does the phishing scam work? In fact scammers make a copy of the official website of the trusted party including all text, logo's and lay-out. This fake website is then hosted on a web server determined by the scammer. Next step for the scammer is to send a large number of phishing e-mails to potential victims. These e-mails contain an official "look-and-feel" message from the trusted company. The message often contains a request to the recipient to provide his personal information for checking or support reasons. The unsuspecting user is requested to click on the URL (that is in fact the Internet address of the fake website) in the message to go to the website where login credentials like user ID, password, credit card number, can be submitted. After providing this information normally a message appears that the website has some problems at the moment and the user is asked to try again later.

What's the true story here? The user is now a victim of the phishing scam. He went to a fake website, which looks like the trusted one, and provided his personal data to the scammers. His name, credit card number and valid thru date are now saved into a database on the web server owned by the scammer. This information can be used to steal money from the user. The scammer can also sell this information to criminal organizations.

An example of phishing is shown on the next few pages [9]. A phishing e-mail is received from the TCF Bank with subject: "TCF express checking card alert". The sender is spoofed and the phish message or question is to verify your TCF account otherwise the service for the account will be stopped. There is also a nice logo of the TCF bank in the e-mail. The goal is to get the victims credit card information.

Figure 2, The phish e-mail

After clicking the link the following screen appears.

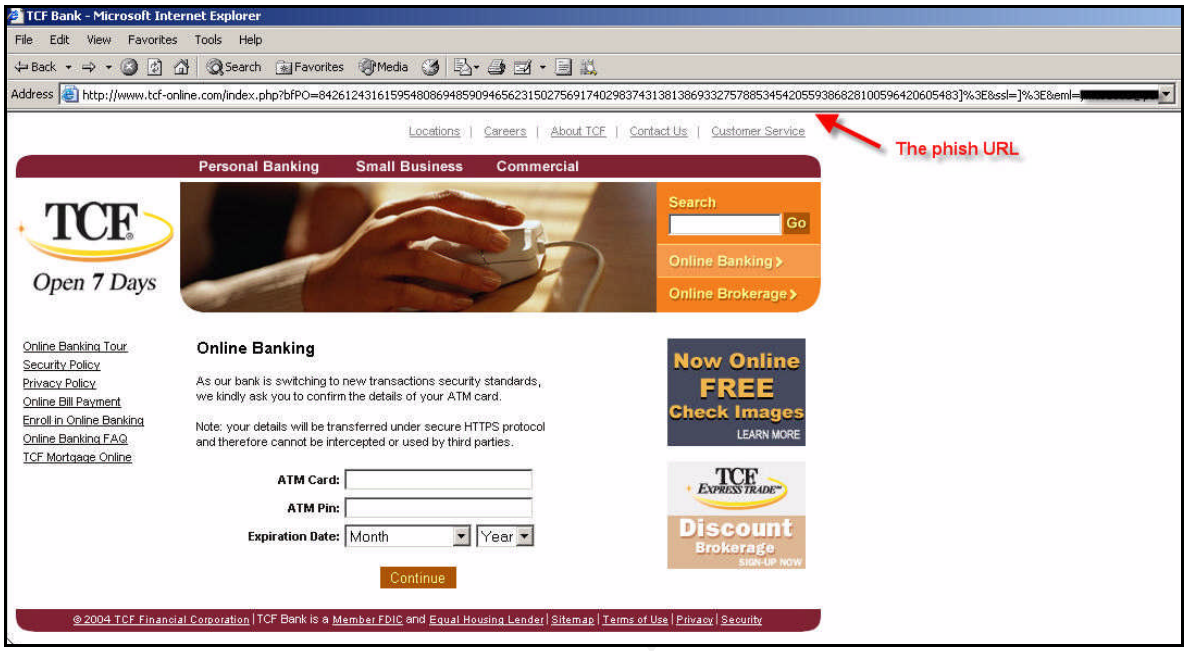

Figure 3, The fake website

There are some weak points in the e-mail as well as the fake website, but it is close enough to trick some users. After submitting the requested information the following reply screen appears.

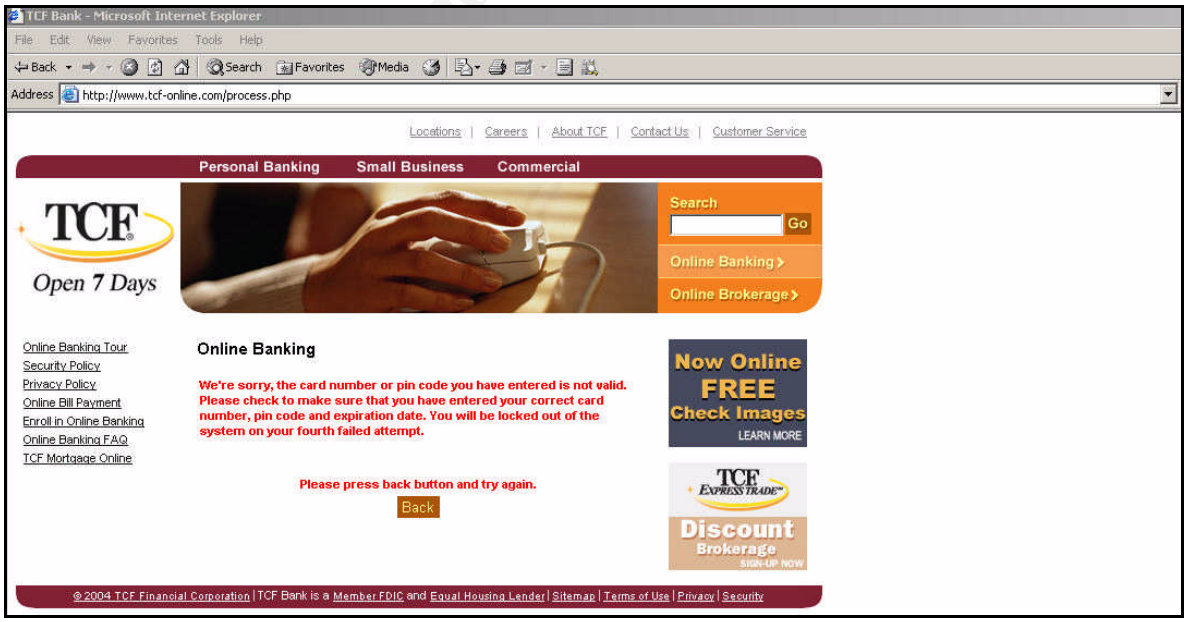

Figure 4, The reply screen

A bogus message appears requesting the user to check their submitted data again. But harm has already been done. After checking the source location (IP address of the server hosting the fake website), it appears to be located in USA, California.

As you can see in the original website below almost everything (logo's, text, pictures) is the same as in the fake one. Weak points are the URL and the fact that you do not need to login in the fake website. However if you are a new TCF bank customer or you did not ever login before you could easily be tricked.

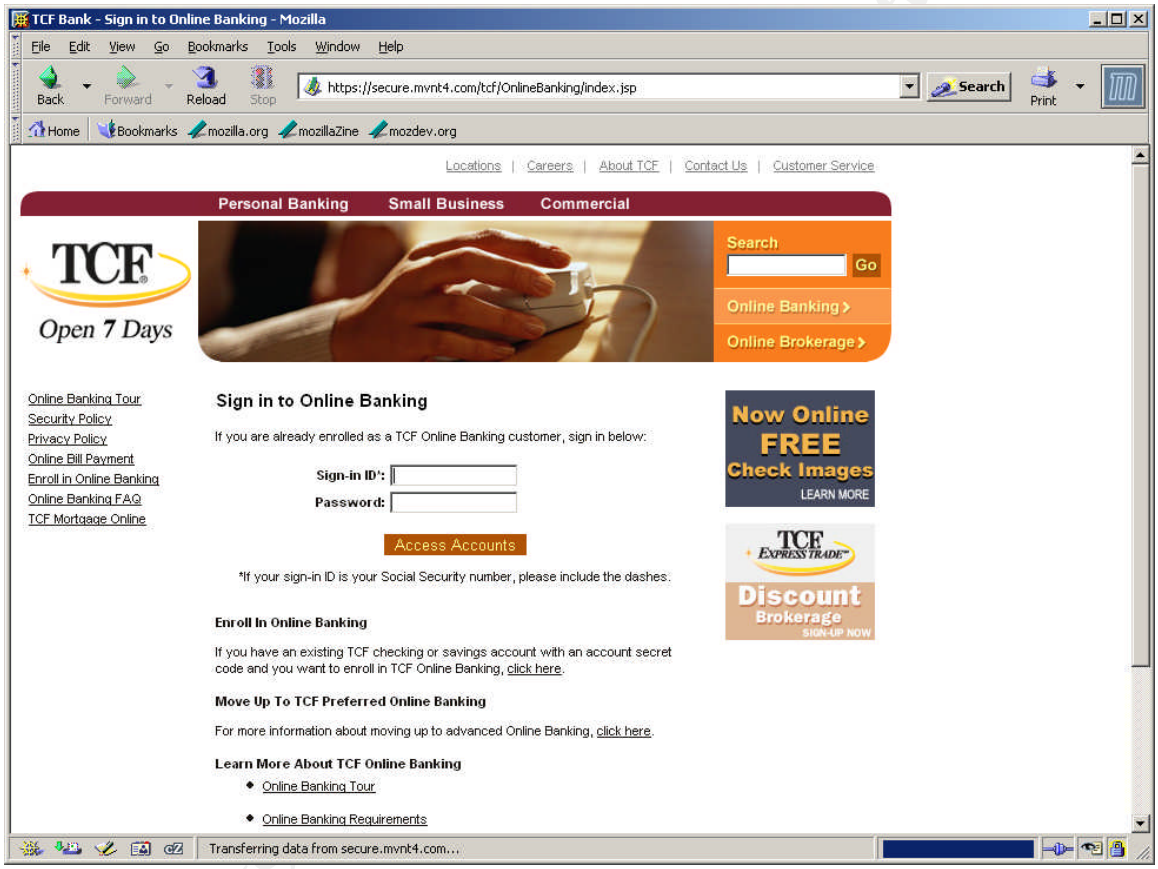

Figure 5, The original website

Phishing is one of the fastest growing threats at the moment on the Internet and is likely to grow significantly in the next few years. According to the monthly Phishing Activity Trend Report of December 2004 from the Anti-Phishing Working Group (APWG) [10], the number of active phishing sites reported in December was 1707. The average monthly growth rate in phishing sites from July through December was 24%. In line with the increasing number of reported active phishing sites is the increasing number of reported unique phishing attacks. In December 9,019 new and unique phishing e-mail messages were reported to the APWG. This is an average monthly growth rate of 38% since July (2,625).

The graph below shows an alarming growing rate of the number of reported active phishing sites from September through December 2004.

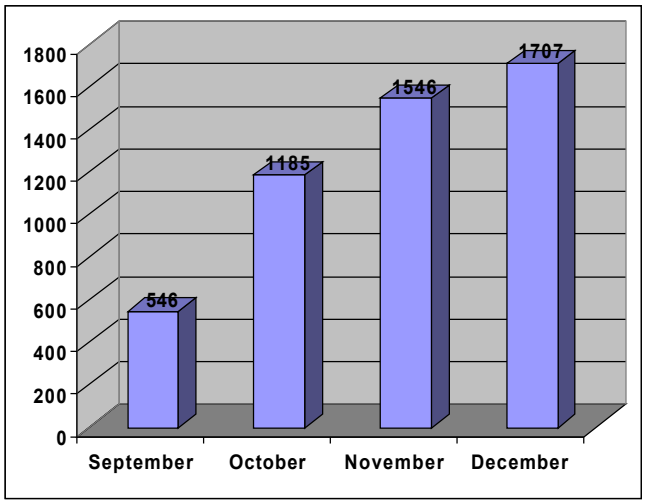

Figure 6, Active reported phishing sites, September – December 2004

3.4 Nigerian Scams or 419 Scams

Nigerian scam is also called “Advance Fee Fraud” or 419 scam (Four-One-Nine). 419 is referring to the Internationalizing Nigerian Criminal Code, Chapter 38 Section '419' [11].

How does this scam work? The potential victim receives an unsolicited fax, letter or e-mail message containing a business offer. The business offer mostly concerns some issue within the Nigerian or another African nation and is always about a large sum of money (mostly millions of dollars) that is the property of the sender. However because of certain reasons the money cannot be obtained by the sender without the help of the person (victim) who receives the message. There are various types of this scam but the core message in all scams is the same.

The story continues as follows. You are being asked to send a small amount of money in advance (Advance Fee), to resolve some problems. When these “problems” are solved the millions can be obtained. It is also possible the scammer asks you to send some personal information like your bank account number, a copy of your signature or your passport. You can even be asked to come over to Nigeria or another African country to discuss the matter personally.

Suppose you fall for this scam and you transfer some money to the person. Soon you will be approached again because there were some unexpected problems and you will be asked for some more money to resolve these problems. This can go on for weeks or months until you run out of money or you stop sending money because you don’t trust it anymore. Unfortunately it is too

late to get your money back. The scammers have vanished with your money [12].

The 419 scam has been around here for decades. Already in the early 1920's people were conned with this type of scam. Potential victims (businessmen, rich people) were approached by a person, the scammer, who tried to get a prisoner out of jail but needed the help (money) of the potential victim to do so. The wealthy family of the prisoner would reward him for his help in this situation. When the victim offered his help and money, it seemed that the release of the prisoner was not that easy. The victim was asked to help again because the attempt to escape did not succeed. And so on, and so on. This scam is called "The Spanish Prisoner" con [13].

The danger of the 419 scam is not only the loss of money. As said before you can also be asked to send some confidential, personal information like your bank account number and passport. With this information the scammer can steal your identity and perform crimes using your name and identity. See paragraph 3.2 for more information about identity theft. You can also be asked to come over to Nigeria to discuss the matter personally. Can you imagine yourself being in a strange African country, doing business with strange people who even bribe the custom officials to get you into the country without passing Customs? In this case you are an illegal person in the country. You can be threatened, kidnapped or even murdered if you do not pay them money [14].

Nigerian scam is evolving fast. Not only the number of Nigerian scam attempts is growing. Also certain situations happening in the world (disasters) are a drive for Nigerian scammers to do their job. At this moment there are Nigerian scam e-mails around about the Asian / Pacific Tsunami disaster. Recipients of the e-mail are asked to send money for the victims of the Tsunami disaster. Of course the money does not go to the victims…

There are many forms of Nigerian scam. Examples of Nigerian scam can be found on various Internet websites. The 419 Coalition provides some examples of Nigerian scam letters [15], and a huge database with Nigerian e-mails which have been submitted by Internet users is provided by www.quatloos.com [16]. But there are many more websites with examples of Nigerian scams. On the next page you will see an example of a Nigerian scam e-mail message received by the author of this paper.

Nigerian scam message example

Dr. Terry Wires
Tel: 27-73-308-9676
Fax: 27-11-507-5168

STRICTLY CONFIDENTIAL

Attention: ***PRESIDENT/CEO***

With respect and humility, we are writing this letter to solicit for your assistance; though it looks strange hence we don't know each other. My name is Dr. Terry Wires one of the Accountant under the Ministry of finance Republic of South Africa. We wish to express our willingness to transfer an overdue contract sum of ***US$11M*** *to your company's account, through the Reserve Bank of South Africa.*

SUBJECT: After due consideration, we have fully agreed to privately contact you for this transaction. We are intending to retire from government services to private business we decided to contact you for an urgent business proposal. We have decided to deal with a neutral person like you because of the nature of the transaction as I will equally be happy to arrange with you on terms of trade and possible transfer of the funds needed for the investment into your company's account or personal account.

The Ministry of Natural Resources incurred these funds as a kick back lifting of gold product. This was a ground plot by some of the key staffs of this ministry for their selfish interest. It was so unfortunate that they were removed from office resulting from the change of Government and policies, which did not favor their continuous stay in the office. This money ***$11M (ELEVEN MILLION US DOLLAR)*** *is now floating in the Ministry of Finance as a redundant fund waiting to be claimed. Because of our new Government policy on Civil Servants, we are not allowed to own a company or operate a foreign bank account. Hence my soliciting for your assistance to enable us receives this fund into your company's account or personal account.*

To enable us start the process and remittance of this funds into your bank account successfully within 10 banking days, we need the following information from you;

Beneficiary full names.
Beneficiary address.
Private telephone & fax number.
Your bank particulars including your bank name, address and your account number.

Note that as soon as we receive this information it will be forwarded to the appropriate quarters for final processing and approvals. With the modalities we have worked out, it makes it possible for you to act as a contractor who worked under my ministry and now waiting to receive his payment and when satisfied by the agencies your bank account will be credited within 48 banking hours. This transfer is 100% risk free and hitch-free having done all the underground works locally for the smooth transfer of the funds into your bank account within the shortest period. We advised that you should keep this transaction a top secret and rest all correspondence to fax, and phone only, because we are occupying a sensitive position in the government circle and also this is once in a lifetime opportunity.

Finally, we want you to assure us that you will work on our instruction and our own share of the money will be safe. You will be rewarded with ***25%*** *of the total sum for your honest assistance and co-operation,* ***5%*** *for any expenses that may come up during the transfer while* ***70%*** *remain for me and my colleagues involved in this transaction.*

Contact me by return call/fax for any question and further discussion.

Awaiting your immediate response.

Regards,
Dr. Terry Wires.

***NOTE:** Please do not reply to this email address, Contact me by call/fax.*

3.5 Lottery Scams

Lottery scams are in fact a type of 419 scams. Lottery scams typically start with an e-mail message to an unsuspecting potential victim stating that the recipient has won a foreign lottery. The recipients e-mail address has been chosen through an automated ballot process and won the first price in the lottery, often millions of dollars. To claim the price the recipient must take contact with the lottery agent and provide some personal information including a copy of his passport and drivers license to verify his identity. At this point the scammer has enough information to take over the victims identity. Next to this the victim will receive an e-mail with a few options how to collect his winnings. No matter what option he chooses, an advance fee for taxes, insurance or legal issues, has to be paid upfront before the winnings can be collected [17]. Consequences? The money is gone and even worse, your identity has been stolen.

"Lottery scams are increasing at an alarming rate", according to FraudWatch International. In April 2004, FraudWatch International received more then 1000 variations of lottery scams. At this moment the website contains a list of more then 400 known lottery scam operatives with a huge number of example e-mails [18].

Below you see an example of a lottery scam e-mail message which has been received by the author of this paper.

Lottery scam message example

EMAIL LOTTERY ROLLOUT INTERNATIONAL

Ref. Number: 034/834/1853
Batch Number: 4427-4184-MN 82

Sir/Madam
We are pleased to inform you about the result of the Loteria EuroBote Winners International programs held on the 28th December 2004. Your e-mail address attached to ticket number 004098045- with serial number 3282-912 drew lucky numbers 5-18-01-43-00-25 which consequently won in the 1st category, you have therefore been approved for a lump sum pay out of â,¬1,000,000.00 (One Million United Euros)

CONGRATULATIONS!!!
Due to the mix up of some numbers and names we ask that you keep your winning information confidential until your claims has been processed and your money Remitted to you. This is part of our security protocol
to avoid double claiming and unwarranted abuse of this program by some participants.

All participants were selected through a computer ballot system drawn from over 30,000 company and 40,000,000 individual email addresses and names from all over the world. This promotional program takes place every three years. This lottery was promoted by the software corporation to compensate some few individuals with website and email addresses, we hope that with part of your winning you will take part in our next year EUROPE 60 million international lottery. To file for your claim, please contact our
EUROPEAN FIDUCIAL AGENT: MR.MARTINS ALBERTO of EUROBOTES LOTTERY AGENCY S.A
TEL: 0034-618-157-904
Email:eurobotes@netscape.net.

Remember, all winning must be claimed not later than 26th of February 2005.After this date all unclaimed funds will be included in the next stake. Please note in order to avoid unnecessary delays and complications
please remember to quote your reference number and batch numbers in all correspondence. Furthermore, should there be any change of address do inform our agent as soon as possible.

Congratulations once more from our members of staff and thank you for being part of our promotional program.

Note: Anybody under the age of 18 is automatically disqualified.

Sincerely yours,
Mrs. Anne Jose.
(Lottery Coordinator)

3.6 Other Types of Frauds and Scams

Next to the major types of Internet fraud like phishing and Nigerian scams, there are a lot of other types of Internet scams which work basically the same. Unsuspicious people receive an e-mail with a "too-good-to-be-true" offer in it. A lot of money can be earned but there are a few preconditions. Personal information of the recipient is needed and in most cases also some money in advance. In this chapter a few other types of scams are described and explained. A pretty large list of Internet scams can be found on [19].

3.6.1 On-Line Auction Scams

On-line auctions are very popular lately. People buy all kinds of stuff from other people they do not know. The Internet is a very good place to offer products because a very large group of potential buyers can be reached very easily. Buyers do not need to come over to an auction premises but stay at home and buy the product on-line. Photo's and a description of the product are provided so the buyer knows what he is buying. There is only one disadvantage in this process and that is payment. Buyers do need to send their money to the seller of the product. Buyers do not know the sellers so there is a risk that the seller has bad intentions. Problems during this process are mostly late delivery of the product but also:

- Receiving products different than those promised
- Receiving damaged products
- Receiving nothing at all

Sellers also encounter problems in the on-line auction process. Buyers who do pay too late, not pay at all or change their minds [20].

3.6.2 Job (Employment) Scam

Job or employment scams are circulating over the Internet in various types. From relatively simple Work-At-Home scams [21] to very complicated Payment Transfer scams [22]. In fact all scams work basically the same. Often job sites like CareerBuilder.com or Monster.com are used by the con artists to place a

job advertisement.

The contact scenario between scammer and job seeker is as follows.

1) A job seeker responds on the advertisement and contacts the scammer.
2) The scammer contacts the job seeker based on a resume that has been posted on the job site by the job seeker.

After some contacts and perhaps some interviews by phone or in person, the job seeker is offered a job. The proposals are often very reliable because existing company information and logo's are used in the communication towards the job seeker. In most cases personal and confidential information is requested by the scammer. Social security numbers, drivers license or personal bank account numbers for direct deposit must be provided by the job seeker. This information can be used to steal money from the victim and/or his identity.

In the case of the payment transfer scam job seekers are offered a job as a financial accountant. Victims can be asked to transfer or forward money via their personal bank account, PayPal account or in person via Western Union, to another bank account provided by the scammer. This bank account number is often overseas. The scammer deposits the money on the personal bank account of the victim. Usually this amount is under $10,000 because these transfers are subject to less scrutiny from banks than amounts over $10,000. A small percentage of the money, usually 5%, is the payment for the services the victim has provided. In fact the money which needs to be transferred is often stolen money from other victims or money from stolen credit card numbers. This is the basics of money laundry and, as you may guess, the victim is committing a severe crime (theft) at the moment he performs the job because he has taken and transferred stolen money.

3.6.3 Page-Jacking and Mouse-Trapping

Page-Jacking and Mouse-Trapping are more sophisticated scam techniques used by scammers to divert unsuspecting Internet users from their intended web destination (page-jacking) to other sites, crafted by the scammer. When the victim of page-jacking redirects to the other site, he is unable to leave the site because their browsers back, forward and close buttons are not working anymore (mouse-trapping). These sites are often pornographic sites [23].

To perform this scam the scammer crafts several websites with porn advertisements in it (click through banner ads) and loads these pages into his web server. Also these websites contain scripts which disable the viewer's browser's back, close and forward buttons. Next, the scammer copies the HTML source code from other legitimate websites (of course without permission of the owner of the website) and adds the redirection script to the HTML source code. The redirection script contains the URL of one of the websites from the scammer containing the porn advertisements. The page jacked websites containing the redirection scripts are loaded into the scammers web server. The

last thing the scammer does is to use search engines to index the page jacked websites.

Now, how does this work? An unsuspecting victim searches on certain keywords using a search engine. He will probably find the page-jacked website and clicks on the URL listed in the search result. When clicking on this URL the victim thinks he visits the legitimate site, however, he is redirected to the scammer's site with the pornographic advertisements. At that moment the victims browser is affected by the mouse-trapping scripts so he cannot leave the site anymore or is redirected again to other porn sites [24].

The scammer makes money since they are paid for each visitor of the porn sites the victims are redirected to. Besides this, scammers also may get money because of the increase of advertisement revenue and/or increase in network traffic to the porn sites. Although this scam is not directly a financial issue for the victim, it is really annoying and another more important issue, children can be exposed to unwanted pornographic material.

3.6.4 Advance Fee Loans

Like the name already mentions, people receive a proposal for a loan or credit card from a certain (financial) company. It does not matter what the credit history of the victim is, he can receive the loan without any further questions. However a small advance fee is requested to obtain the loan. After payment of the advance fee the victim will not get his loan. The company makes up a story that the transaction was unsuccessful or the company will disappear completely [25].

3.6.5 International Modem Dialing

Although broadband connections are becoming more and more common nowadays, there are still a lot of people who use dial-in connections to the Internet. That's where this scam is being performed. Some sites, often pornographic sites, use international dialing to trick Internet users into paying large amounts of money for viewing the content of the website. The sites have large ads which say that the content is free of charge and the victim is requested to download a dialer program to view the content. Once downloaded and installed, the dialer program starts dialing to an international long distance number. The victim will get connection however the site maybe very slow or the dialer runs in the background without being detected or the sound of the dialing program maybe turned of so the victim does not hear the dialing tones. This may go on for the complete Internet session of the victim which could be hours resulting in a huge telephone bill [26].

3.6.6 Skimming

Although not really an Internet scam, skimming is a type of electronic fraud which is growing rapidly last few years. However it is worthwhile to mention here because this is a real-life threat for everyone. Skimming usually is performed at cash machines (ATMs) and is based on two techniques. First a skimming device is placed on top of the PIN pad. The skimming device looks exactly the

same as the PIN pad so the victim does not get suspicious.

The skimming device contains some simple electronic equipment which is enabled to scan and copy the magnetic strip on the (credit) card of the victim. The second technique is the theft of the PIN code belonging to the victims (credit) card. Therefore the skimming device may contain some electronics which records the code or a miniature camera is placed somewhere on top of the cash machine which records the PIN code typed by the victim [27].

There are also portable skimming devices which can read the victims card details and PIN code. Take the example of waiters in restaurants. While paying for his dinner the customer gives his credit card to the waiter. The waiter swipes the card through the skimming device and all relevant information is being scanned and copied [28].

Skimming is dangerous not only because of the loss of money and creation of fake cards but this could also be the beginning of identity theft.

4. Techniques and Tools used by Scammers

The scammer uses several techniques to perform his act. The Internet provides the scammer a number of (electronic) techniques and tools which can be used to con unsuspecting people using the services of the Internet (e.g. e-mail, surfing web-sites). In this chapter a number of techniques are described and explained which form the basis for the scams described in the previous chapter.

4.1 E-mail and the Internet

Most of the explained scams use e-mail and/or the Internet as underlying technique to trick people who use e-mail and the Internet. While in the past letters or fax messages were used, nowadays the electronic ways of communication offers great advantages. With e-mail it is possible to send large amounts of messages (bulk e-mails) with relatively low or even no costs at all. Besides this, e-mails can easily be spoofed. The sender safeguards his anonymity. The Internet is the perfect "cyber" world for scammers to perform their acts. The Internet provides anonymity, large groups of unsuspected potential victims and a lot of technical ways to support them in their evil intentions.

The next paragraphs describe some methods and techniques related to e-mail and the Internet.

4.2 Spam

A very short but easy to understand definition of spam in a general sense is: any e-mail you do not want to receive (e.g. advertisements, newsletters or questionnaires). However this definition does not cover the real meaning of spam where the Internet community is referring to. The most concerning or dangerous form of spam is the illegal spam. The definition of illegal spam is the attempt to deceive people (Internet users) by falsification of seller identity or e-mail address, and use of other trickery (defrauding), in the hope of gaining monetary advantage (stealing) from the e-mail recipient and other parties [29].

There are of course many definitions of spam however in a general sense its all about the same: unwanted e-mails, deception of the recipient, false sender identity and fraudulent purposes. Scammers send spam in order to sell products and services or to promote an e-mail scam.

The more polite name of spam is Unsolicited Commercial E-mail (UCE). More names of spam are: junk e-mail, Unsolicited Bulk Mail (UBM), Excessive Multi-Posting (EMP), spam mail, bulk e-mail.

An example of a typical spam message received by the author of this paper is shown below.

SAVE OVER 50% ON PRESCRIPTION DRUGS

With our On-Line Pharmacy you can:

1. Order name brand prescription drugs right from home (not the cheap European versions on sites offer)
2. Get it shipped same day to your door step
3. Never have to worry about getting a doctor to write the prescription again
4. Save hundreds of dollars over your local pharmacy

If all this sounds good to you then you need to Click Here for more about what we offer. We carry everything from Soma, Valium, Xanax, and Viagra. So go to our site to see how much we can save you today.

4.2.1 How does the Spammer obtain E-mail Addresses?

The spammer wants to collect as many e-mail addresses as possible and he does not matter where the addresses come from or who owns the e-mail address. He wants to fully automate this collecting process to save time and energy. There are a number of ways to collect e-mail addresses.

- Extracting e-mail addresses from various (public) sources such as websites, chat boxes, newsgroups, mailing lists, guestbook's, bulletin boards, e-mail databases (e.g. www.addresses.com), and so on.
- Use so-called "spam-robots" or "spam-bots", also known as e-mail grabbers, extractors, harvesters, etc. These specially crafted programs or automated scripts work like search engines. They scan the Internet page-by-page, site after site, collecting e-mail addresses, searching for text strings like "@", "mailto:" etc. It's easy to collect all the addresses in this way because each e-mail address has one standard form: xxx@yyy.zzz [30].
- Spammers can use an even simpler method to obtain e-mail addresses by just buying e-mail addresses from a company who is selling his mailing lists to third parties, spammers included.

After collection of the e-mail addresses the spammer will sort them en save them in a database for further use. On his turn he can also sell them to other spammers to make more money.

4.2.2 How does the Spammer send the E-mails?

The spammer can use several methods to send bulk-mail to their potential victims.

- Use bulk-mail software for automated sending of large amount of messages. There are numerous software tools and packages to send bulk-mail. Just search on "send bulk-mail" on www.google.com and you see countless of hits pointing to e-mail software packages doing the job for you. Using this software, spammers can easily send an almost unlimited number of e-mails to their victims. Some products offer the option of sending e-mail without the use of the ISPs e-mail servers so the e-mails from the spammer cannot be blocked on the e-mail server of the ISP.
- Spammers can also use open mail relay systems from ISPs. Especially in the early days of the Internet e-mail servers were poorly configured and gave the ability to use the relay function of the e-mail server for systems in another domain then the e-mail server. When the use of the open mail relay was detected and blocked, the spammer just searched for another open mail relay and started again with his spamming activities [31].
- Use zombie networks to send e-mail. See next paragraph for more information about zombie PCs or zombie networks.

4.3 Zombie Networks

Zombie PCs are in fact "hacked" systems of unsuspecting Internet users. The systems can be controlled by the hacker for any purpose like spam runs or Denial-of-Service attacks. If there are more then one zombie PCs working together in a spam run or attack it is called a zombie network. Zombie networks can contain thousands of single systems performing the spam run or Distributed Denial-of-Service attack against well-known websites.

4.3.1 How is a Zombie Network created?

The scammer or hacker who wants to create a zombie network first has to infect a lot of single systems with a computer virus. This computer virus installs a so-called "back door" program on the infected system. This "back door" program leaves an Internet port open on the system so the hacker is able to probe the systems with the open port connected to the Internet. When the hacker finds such a system he can install the "bot" program on the system which is in fact the malicious software where its all about. The system has now become a zombie PC because the hacker can wake the systems from the dead on command. IRC rooms (Internet Relay Chat rooms) are often the central control command rooms from which the zombie PCs are controlled (see figure 7).

According to Viki Navratilova, a systems administrator at the University of Chicago, there is no technical limit to the size of a zombie network or a botnet because bots can be placed on any number of PCs, and chat rooms provide a useful central location from which to control them [32]. In January 2004 zombie networks comprised around 2000 systems while in May in the same year that had risen to more than 60,000, according to the latest research from security firm Symantec. One reason for this is the growing number of broadband Internet connections and because of that, systems which remain connected to the Internet permanently.

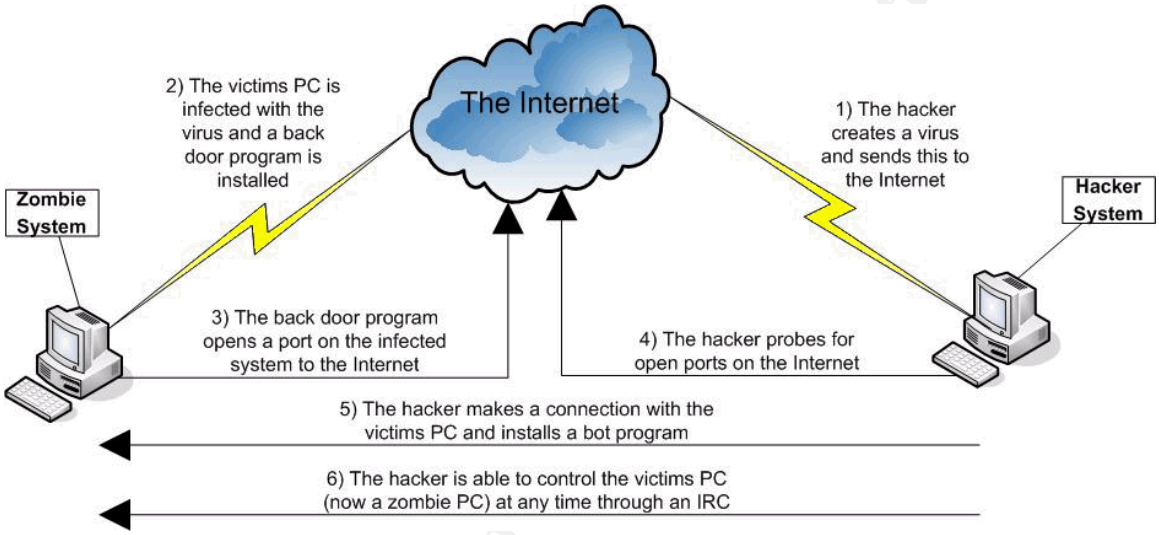

Figure 7, How an innocent PC becomes a zombie PC

4.3.2 Zombie Networks at Work

More than 70% of spam is being sent from zombie networks according to spam expert Steve Linford. In an article for ZDNET he explains some issues around zombie networks and mentions a few staggering numbers. For example, every week more than 100,000 PCs are becoming part of a zombie network without the knowledge of the innocent owner of the system [33].

Zombie networks can also be used for phishing attacks. According to another article on ZDNET [34], phishing attacks are powered by 'just five' zombie networks. Security firm Ciphertrust found out that phishing e-mails were send from groups of 1,000 zombie PCs belonging to one of five zombie networks. They came to this conclusion by analyzing the IP addresses from the sources from which the phishing e-mails were send from.

There are more purposes zombie networks can be used for but sending spam and phishing e-mails and carry out DoS attacks are the most common uses of the zombie networks.

4.3.3 Zombies for Rent?

It is very easy for a spammer to perform his act because hackers are hiring out their zombie networks. According to an article of PCWORLD, British teen hackers are offering their zombie networks for $100 an hour [35]. The spammer does not need to have any technical knowledge about viruses nor how to setup and control the zombie network. Its all done for him.

4.4 Fake Websites

Especially the phishing scam uses fake websites. Official websites from mostly financial institutions are copied in detail by scammers. Text, links, pictures, logo's, almost every detail on the original site is copied to the fake one. Some additional features are added, e.g. scripts or special fields in the fake website that collects the personal information and credit card numbers entered by the victim. These special features are often different from the original site since the original site would never request this kind of information, in this way and not secured, from their customers. Another difference between fake site and original site is the Internet address of the website, the URL (Universal Resource Locator). More information and specific (attack) techniques, also related to fake websites, are explained in the next few paragraphs.

4.5 Attack Scenarios and Techniques

In the following paragraphs a number of attack techniques are explained, which can be used by scammers to con people using the Internet. Some techniques are related to fake websites, others use legitimate websites, but in general all techniques are up for just one thing, theft of valuable information from the victim. It goes too far in this document to describe the techniques in detail so only a general description is given with a reference to an Internet site where more detailed information can be obtained.

4.5.1 Social Engineering

Social Engineering is not a technique in the technical sense but more related to persuade people to give certain information. The scammer uses a spoofed identity and misuses the trust of unsuspecting people they have in a certain company. Besides this there is often a matter of urgency or threat in the request from the scammer to the victim. In most cases the scammer uses the telephone. To get the information (e.g. user IDs and/or passwords), the scammer calls the victim and pretends he is an employee from a certain company (e.g. a financial institution or a bank). There are several requests the scammer can make to the victim. Here are few examples.

- The victims login information is needed to verify the victims account.
- The victims login information is needed because there were some problems with the administration system.
- The victim login information is needed because a former transaction

needs to be corrected.

Social engineering is a very powerful technique if well performed. It requires the power to improvise in unexpected situations and a fast thinking mind. Kevin Mitnick was (and perhaps still is), one of the best social engineering hackers.

4.5.2 URL Obfuscation

The URL of an Internet website comprises of different parts. The most common parts are the hostname and the web page itself. Take the following example URL:

http://www.sans.org/aboutsans.php

- www.sans.org stands for the hostname, namely the SANS organization.
- aboutsans.php is the filename of the web page (the contents) you are actually seeing on your computer screen.

About 99.9% of the URLs on the Internet use this layout [36]. However an URL may contain other parts too. For example an username and password. Besides this it is possible to replace the actual hostname with another notation. The hostname can be noted as an IP address and on its turn, the IP address can also be noted as binary or octal or decimal or hexadecimal numbers. Another possibility is to change the file name of the web site into hexadecimal characters instead of normal readable alphanumeric text. Using several of these possibilities at the same time can make up an URL that looks like an official URL but in fact it is the URL of the fake website [37].

More technical information about the URL can be found in the Request For Comments, number 1738 (RFC 1738) [38].

4.5.3 Page Redirection

Also explained in paragraph 3.6.3, Page-Jacking and Mouse-Trapping, the redirection technique is used to divert unsuspecting people to other websites then they originally intended to go to. An example of a redirection in a phishing scam is a bogus login screen which pops up after clicking a link.

4.5.4 Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a technique used by the scammer to attack Internet users via an e-mail message or via a legitimate website. There are many types of XSS but the most common one is the scenario in which the Internet user visits a legitimate website.

The scammer identifies a vulnerable application on the legitimate website and inserts a malicious script in the vulnerable part of the website. Malicious scripts can be any scripting language, e.g. JavaScript, VBScript, ActiveX, and Flash. When the unsuspecting victim displays the website the malicious script runs and attacks the victims browser. A successful attack can result into anything from cookie theft and account hijacking to theft of user IDs / passwords and change of user settings [39].

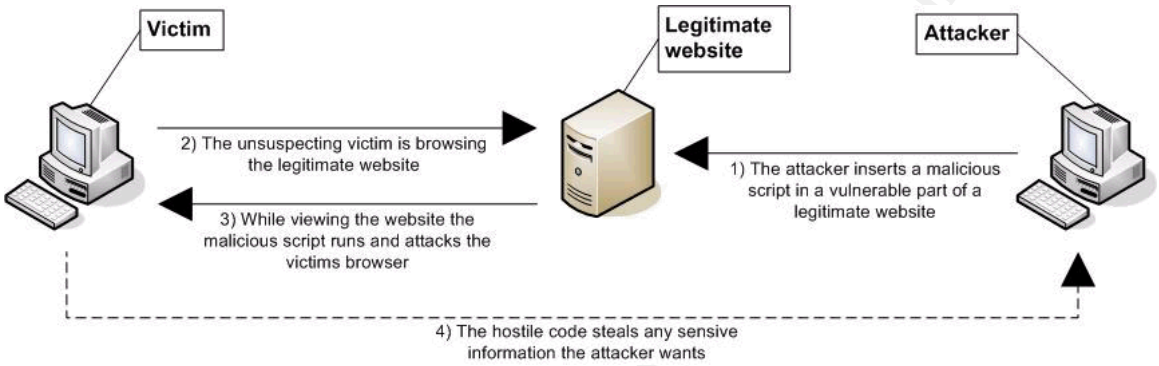

Figure 8, Cross-Site Scripting explained

4.5.5 Visual Spoofing

In a phishing case when URL obfuscation is used in combination with a fake website, people with a little bit of knowledge and suspicion can detect the scam. However Visual Spoofing is a technique which makes it harder to detect the scam. Parts of the browser interface that normally are affected by the scam (e.g. the URL), are now substituted by images. JavaScript links are used to launch a new browser window without the normal elements in it (e.g. address bar, scrollbars, menu bars, etc).

You might have seen this before while browsing on the Internet. Sometimes a popup window appears with an advertisement in it. The popup window only contains the advertisement and nothing else. In the case of visual spoofing the window does not contain an advertisement but an image which looks exactly the same as the address bar and menu bar of your browser. On the next page you see an example of visual spoofing. The address bar and menu bar of your browser are copied and placed into the screen as an image. Below the image the malicious content is presented (e.g. login fields). The fake image contains the URL of the real, trusted site so you do not get suspicious by the URL. Even the golden lock in the bottom of the screen, which represents a secure site, is fake [40]. You can test visual spoofing with your own browser [41].

An example of visual spoofing

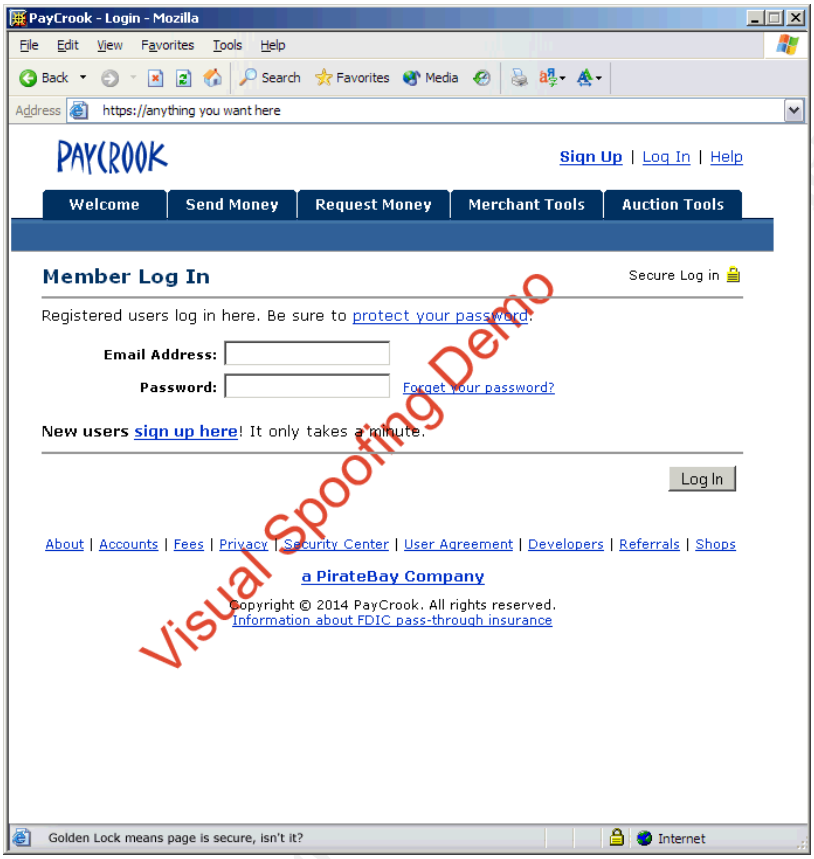

Figure 9, Visual Spoofing example by Don Park

4.5.6 IE IFRAME Buffer Overflow

This technique is a Internet Explorer specific vulnerability which can be exploited by the scammer to execute arbitrary code with the privileges of the user on the system of the user. The user is convinced to view a specially crafted web site or HTML e-mail message containing malicious JavaScript code. When viewing the website, Internet Explorer is affected by the malicious code because of the way IE handles HTML elements such as FRAME and IFRAME. A buffer overflow situation occurs and the attacker may execute arbitrary code [42].

Once the malicious code is executed the attacker may do anything from completely compromise the victims system and steal sensitive information to crash the victims applications. Some variants of the MyDoom worm use this vulnerability to attack systems.

4.5.7 Window Injection

This vulnerability is found in a whole range of different web browsers on multiple platforms. When clicking a link on a trusted website people believe that the content in the new window can be trusted. However if, at the same time, another (malicious) website is open, the content of the just opened (trusted) window may be overwritten with malicious content. This content may comprise login fields for user IDs, passwords and other sensitive information. Usually the login screens of secure sites are like popup screens. There is no address bar, menu bar, etc, so the attacker may overwrite the real login screen with a fake one [43].

4.5.8 Man In The Middle

The Man In the Middle attack (MITM) is also known as "TCP Hijacking" [44]. Like the name of this attack technique says the attacker is logically located between the victim and the legitimate web server the victim is using. If the attack is carried out successfully all network traffic between victim and legitimate server is flowing via the attackers system. The attacker is able to sniff the network traffic for sensitive information such as passwords but at the same time he is also able to change the contents of the network packets and insert malicious code to infect the victims system which makes other attacks possible.

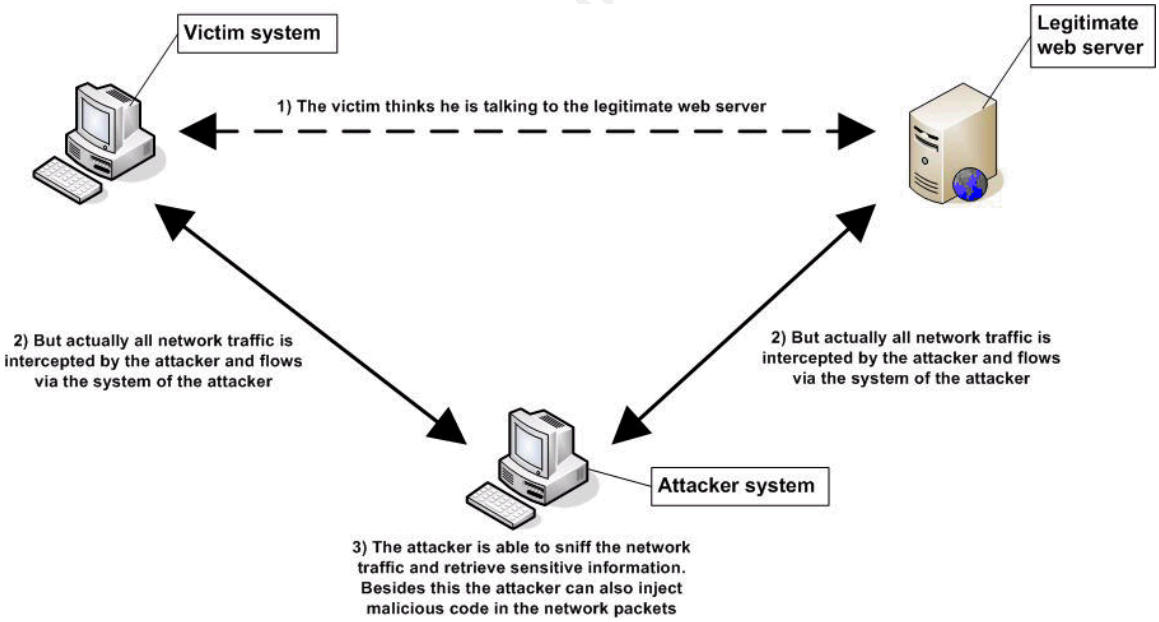

Figure 10, Man In The Middle attack

4.5.9 Trojan Horse Programs

Attackers may convince unsuspecting victims to install malicious software such as Trojan Horses. Victims can be infected by the Trojan by installing a bogus software patch or by reading an e-mail containing a virus. Once the Trojan is installed the attacker has the possibility to monitor the victim system activities. Usually the Trojan opens a back door on the victims system. This enables the attacker to get access to the victims system.

Key Stroke Loggers and Screen Grabbers are the most common Trojan horses on the Internet. Key stroke loggers are logging every key stroke the victim types. All key strokes, which could be sensitive information, are then send to the attacker. Screen grabbers copy the screen content and send it to the attacker. Broadband Internet connections make it even possible to send live streaming video.

4.5.10 Worms

A worm is a sub-class of a virus. Its design is almost similar however, unlike viruses, worms replicate without the knowledge and intervention of the victim. A worm which has infected a system may infect other systems by sending e-mail messages to all e-mail addresses listed in the address book on the victims PC. It is also possible that the worms spreads via the network services of the system (TCP or UDP ports).

Typical characteristics of worms are high consumption of system resources (e.g. memory or CPU load), and network bandwidth causing a huge network load. Web servers, file servers, workstations, all other systems attached to the network are getting slow and even stop responding. Besides this type of damage some worms also have the possibility to tunnel into the victims system and allow attackers to take over your system remotely and control it with administrator rights.

4.5.11 Spy-ware and Ad-ware

Usually ad-ware is that part of a software application which displays advertisements in the program while running. The ads can be viewed through pop-up windows or through a bar that appears on the screen. This is not necessarily a bad thing. The developers of the application try to recover programming development costs and also helps to hold down the cost for the user of the application. Nowadays most ad-ware includes code that tracks the user's personal information or activity on the Internet. This information is passed on to third parties without authorization or knowledge of the user. This is called spy-ware [45].

Spy-ware secretly gathers information about the Internet user without his authorization or knowledge. The user's Internet connection is used to send the collected information, which could be sensitive, to third parties like advertisers or other interested parties. For example the cookie mechanism could be considered a form of spy-ware as the cookie is used for storing information about the Internet behavior of the user. The victims system can be infected with spy-ware by a virus or as the result of installing a new program or software update [46].

Some scary facts on spy-ware are mentioned in [2].

- Spy-ware uses covert techniques to install itself on computers.
- Spy-ware tracks user activity with the purpose to steal passwords, credit card numbers, other sensitive user information and confidential corporate data.
- The best-performing anti-spy-ware scanner application is not capable of detecting all the critical files and registry entries installed by spy-ware.
- No one knows what the malicious programs are capable of doing, except the spy-ware author.
- Spy-ware contains some really smart features which enables reinstallation of spy-ware components after they are removed.

5. Prevention and Detection

It is crucial to have a good Prevention and Detection program for yourself and for your company to prevent becoming a victim of Internet fraud. There are some technical measures which could be taken but you should not rely on these measures only. More important and mandatory is awareness and training. Some scams easily slip through a firewall, e-mail filter or other detection program. If you only rely on these technical measures then you are not suspicious anymore and you could easily become a victim of a scam. This chapter describes some basic technical measures and security awareness measures.

5.1 Technical Measures

For almost every threat, "anti" products have been developed or are developed at this moment. In the next paragraphs the most important "anti" scam measures are describes and explained. You should implement at least the mentioned measures and investigate if you need anything else based on your specific situation, personal and/or business wise.

5.1.1 Anti - "Malicious Software" Measures

Viruses, Worms, Trojans, Spy-ware; these are all malicious software programs which can do harm to your system, your data and in the end to yourself. For all these malicious software there can be taken countermeasures. You should install at least an anti-virus, an anti-Trojan and an anti-spy-ware product on your system. Besides this, you have to make sure that every product is updated regularly with the newest detection rules.

Anti-Virus Products

This is the most basic protection for your system and data. There are multiple vendors which offer good anti-virus software for personal and business use. Products from McAfee (Network Associates), Symantec, Kapersky Labs and Sophos are commercial but good anti-virus software applications. There are personal and business versions available. A free anti-virus product for personal use is Grisoft AVG anti-virus. A list with anti-virus vendors and their website can be found at [47].

Anti-Trojan Products

Just like a marathon specialist would not perform in the Tour-De-France, an anti-virus product is not good in detecting Trojan horses. Therefore you need a separate product for detecting Trojans on your system. Ian Richards from Tech Support Alert [48] searches the Internet for interesting new sources of (security) information and products. He conducts independent tests and presents his testing results on the Internet. He also tested a number of anti-Trojan products [49].

For experienced users he recommends a product called TDS-3 (Trojan Defense Suite) from an Australian company Diamond Computer Systems. For most users a utility called Trojan Hunter is recommended. Trojan Hunter is written by Magnus Mischel and distributed via his company Mischel Internet Security.

Anti-Spy-Ware Products
Anti-spy-ware or anti-ad-ware products are also explained and investigated on the Tech Support Alert site. Products such as Spybot Search and Destroy, Ad-Aware SE and the new (beta) version of the Microsoft's free anti-spy-ware program are highly recommended to detect and protect your system against malicious spy-ware [50].

Anti-Scum-Ware Products
These annoying changes to your Internet Explorer search settings, unwanted popup screens and change of your home page can be fought against by using anti-scum-ware software. Anti-scum-ware does not really scan your system, It is a protective program like an anti-virus program which checks other programs before execution [50]. Good products are SpywareBlaster and SpywareGuard.

Anti-Key Logger Products
Being one of the most dangerous Trojans or spy-ware, key loggers must be stopped. Anti-key logger software prevents that data from key strokes is being captured and send to the Internet. Besides this feature most anti-key logger products have other features such as protection against windows text capturing and clipboard capturing. Furthermore it is important to understand that this kind of software does not need any (signature) updates. Anti-virus products do need updates as new types of viruses are being "born" every day. However anti-key loggers run in background mode and block all programs which capture key strokes. So in fact the malicious key logger program receives no key strokes and the key-log file remains empty. Products are Anti-Keylogger [51] and Advanced Anti Keylogger from company Spydex [52].

5.1.2 Anti-Spam Measures

Because most scams are based on spamming techniques it is very useful to install and configure a so-called spam filter on your e-mail application. Spam filters work as an automated content-based filter. Certain typical information or key words in the e-mail message may be identified as spam. This e-mail can then be filtered and deleted so it will not be received by the recipient. Common spam filter types are Scoring Content-Based Spam Filters and Bayesian Spam Filters.

Scoring Content-Based Spam Filters
This type of spam filter searches for characteristic elements of spam in the messages and assign those elements a certain score. From the individual scores a spam score for the whole message is computed. Based on the score the message is being deleted or send through. This filter works by building a list of characteristic elements provided by a large number of spam AND legitimate messages. The problem with this approach is that the characteristics of legitimate e-mail messages may vary for each person. Besides this the characteristics are static. As soon as the spammer adapts the content of his spam messages to look like legitimate messages, the spam filter needs to be tuned manually [53].

Bayesian Spam Filters
Bayesian spam filters are also scoring content-based but unlike the "simple" content-based filters relying on the input of humans, Bayesian spam filters are self-learning. Instead of using a manually built list of characteristics, the Bayesian spam filters build the list themselves. You start with two types of e-mail messages, a number of messages classified as spam and a number of legitimate messages. The Bayesian filter starts analyzing the messages and looks for the following characteristics:

- Words, word pairs and phrases in the body of the message
- The e-mail headers (e.g. sender information and message paths)
- HTML code (colors)
- Meta information (e.g. where a particular phrase appears)

Based on the results of the analysis the spam filter can do a pretty good job distinguishing spam messages from legitimate messages. New messages are analyzed and checked against the characteristics database. The probability of the complete message being spam is then calculated using the individual characteristics. The Bayesian spam filter uses an auto-adaptive technique to learn from its own decisions but it is also possible that the spam filter learns from user corrections [53].

There are numerous spam filter products. Known products are SpamAssassin, which is a free, open source software product and Brightmail from Internet Security company Symantec. A search on www.google.com gives you more then enough information about spam filter products or just checkout the website of Tech Support Alert [48].

5.1.3 Anti-Phishing Measures

There is still a chance that even the most sophisticated and well-learned spam filters miss a phishing e-mail because some of the phishing attempts are very convincing. In this case you need some extra protection. In an article for PCWORLD, Tom Spring gives an overview of several anti-phishing products on

the market today [54].

In general good anti-phishing protection software relies on a few things.

1) The software collects your personal sensitive data, encrypt it and stores it on the system.
2) It monitors your Internet use, which websites you visit.
3) It monitors the key strokes you type when you are on-line.
4) It relies on a so-called blacklist of known phishing sites that is updated regularly.

These issues together can cause an alert from the anti-phishing software on your screen. Suppose you receive a fake e-mail from your bank and you fall for it. While typing your user ID, the software warns that you are sharing sensitive information with an unknown third party. This could possible be a scam. Besides this, when you visit a website which is on the blacklist, the software also sends a warning by a popup screen. Phish Net, a free product from Webroot Software works like this. Another anti-phishing tool is TrustWatch from GeoTrust which monitors your Internet behavior and warns when you visit a site that is unknown by the software. It also warns while visiting a site that is listed in the blacklist of phishing sites.

There are more anti-phishing products such as ScamBlocker from EarthLink and SpoofStick from CoreStreet. However these products solely rely on blacklists to warn Internet users and these blacklists may not be up-to-date so the user may not be warned when visiting a phishing site that is not yet listed in the blacklist.

5.1.4 Firewalls

It goes to far in this document to describe all aspects around a firewall so only a general description is given. A firewall is a device, hardware or software, running on your system or running on a separate system in your network, which constantly monitors network connections going in or out of your system or network. Based on a predefined set of rules the firewall allows or denies a connection.

A firewall is a MUST HAVE as it can keep attackers out of your system or network. However do not rely on a firewall solely. Security is about defense in depth. Implement more layers of security measures to increase your total security. A firewall is one thing, anti-virus software the second, and so on.

Again there are numerous firewall vendors and products, free and commercial. Known commercial products are Firewall-1 from CheckPoint Software Technologies and Cisco PIX Firewall from Cisco. Almost every Linux distribution has a build-in firewall but there are also Linux distributions that are completely dedicated to the firewall function like Clarkconnect.

Besides these solutions there are also so-called personal firewalls which are software firewalls running on the user's workstation. Examples are the Internet Connection Firewall from Microsoft Corporation and the free, open source firewall ZoneAlarm from Zone Labs.

5.1.5 Software Updates

Next to implementing a firewall and installing anti-virus software, regularly updating your software and operating system is the third most important technical measure you need to carry out. Software is constantly being investigated and reviewed and every day new bugs and vulnerabilities are discovered. In most cases this information is published on the Internet. This to warn people who use the software but also to persuade the vendors and developers of the software to release patches which solve the discovered problems. Unfortunately vulnerabilities in software are also used by scammers or hackers for an evil purpose (e.g. infection of a vulnerable system by viruses that exploit the vulnerability). So in order to avoid attacks on your system using known vulnerabilities it is mandatory to update your software as soon as the software vendor releases (security) patches. It is a good practice to subscribe yourself to a number of security or vulnerability mailing lists, check the Internet for new vulnerabilities daily or purchase a vulnerability warning service from a security vendor. Vulnerability warning services are offered by security companies Secunia or Symantec (DeepSight).

5.2 Security Awareness

Every company should have a Security Awareness training program which is obliged for every employee to follow. Why? Well, because there is always a chance that a scam or other evil e-mail slips through the technical measures. People who think they are 100% save because they have a firewall implemented, anti-virus software installed, perform regular software updates, those people are wrong! So you have to make sure that you invest in the best anti-scam product there is, namely YOURSELF.

Security Awareness Programs are a sort of security training. These trainings learn people about the basics of (computer) security, how they should handle security and how to detect a possible security breach or scam. All aspects described in this document (and more) should be part of this security training. The security awareness programs can be made by the company itself but there are also companies that are specialized in these kind of trainings so you can buy any specific training you want.

5.3 Tips, Rules, Do's and Don'ts

To avoid Internet scams there are a number of basic rules that you MUST comply. It does not matter what kind of scam is presented to you, if you comply to these basic rules you should never become a victim of a scam. In fact there is only one rule which prevents you from becoming a victim:

ALWAYS BE SUSPICIOUS WHEN DOING BUSINESS VIA E-MAIL OR INTERNET AND VERIFY THE IDENTITY OF THE OTHER PARTY FIRST!!!

This is of course a high level rule but if you have a healthy level of suspicion next to all technical measures taken then you should be save. The general rule mentioned above can be divided in more specific rules:

NEVER give your personal information via e-mail or websites UNLESS you are absolutely sure that you deal with a trusted party.
If you deal with a company you have done business before then that company will NEVER ask for the information again because they already have it. If you do business with an unknown company then verify the request for information by calling them on the telephone. Especially banks and financial institutions will NEVER ask you for personal sensitive data via e-mail and they will NEVER threaten you via e-mail if you do not give the information.

NEVER respond on a Nigerian (419) or any other e-mail offer which sounds "too good to be true".
If you fall for these kinds of scam you do not only run the financial risk of loosing a lot of money but also the possibility that your identity is being stolen or even worse, you could be killed. Even if the source looks extremely trusted and you are tempted by the offer, ALWAYS verify the identity of the sender and his good intentions by contacting the sender or company by other means then e-mail. Just grab the telephone or verify the (Internet) address via other sources.

NEVER respond on spam messages.
If you respond on spam messages your e-mail address will probably be listed on a spam list and sold to spammers. You will receive even more spam (including viruses and other malicious software) then before.

NEVER open messages from an unknown sender especially when the e-mail has an attachment in it.
The most basic rule while dealing with e-mail. Most viruses are spreading via e-mail so you should be warned if you receive an e-mail from an unknown source and attachment. DO NOT open it but DELETE it right away. If it was important, and thus legitimate, they will send it again or contact you via another communication way.

ALWAYS be extremely suspicious for fake websites.
When doing business on the Internet check the company website on URL, misspelled words, fake images, security certificates and any other specific malicious characteristics on a fake website. ALWAYS check some respectable Internet sources (e.g. the Anti-Phishing Working Group) for information about the company you want to do business with. If you still have doubts, DO NOT do business with that company.

NEVER provide sensitive information over the telephone UNLESS you are ABSOLUTELY sure about the other persons identity.
Social Engineering is a very effective way to retrieve sensitive information. So start being suspicious if a person you do not know, calls you and starts asking for your user ID, password or any other information which is confidential for you and your company. NEVER give the information UNLESS you are absolutely sure about the identity of the other person. In case of any doubts DO NOT give the information or ask if you can call back (in the mean time you can check if the other person can be trusted).

NEVER install software you do not trust.
This rule is to prevent that malicious software (e.g. back doors, Trojans, spy-ware, etc) is being installed without your knowledge and authorization. ALWAYS check the source from which you got the software. If you have any doubts DO NOT install it.

ALWAYS install, use and update a number of anti-scam products and other technical measures as described in this paper.
Adapt the Defense-in-Depth method. Implement several layers of security in your network or on your system. Every layer adds more security to your system or network.

6. Conclusion

E-mail and the Internet provide the scammer numerous possibilities, tools and techniques to perform his scam. Anonymity and a huge group of potential victims are key words in this story. The dangers for the ignorant and unsuspecting Internet user varies from financial losses, theft of his identity and, in some cases, may even lead to death! Fortunately we can fight against these threats. We have countermeasures, techniques and tools. We can implement software that detects malicious software as viruses, worms and spy-ware. We can install firewalls to check and control our Internet connections and we can perform regular software updates for our applications and operating system to prevent exploitation of vulnerabilities. We can implement spam filters on our mail systems to block spam messages containing scams. Unfortunately this may not be enough security to be 100% save. That's why we have to setup and follow a security awareness program. Get yourself familiar with all security aspects, learn about Nigerian scam, phishing attempts, fake websites and social engineering. And keep learning continuously! And last but not least; You must fall into a personal habit: Be cautious while you are doing business via e-mail and the Internet and remain suspicious until trust of the other party has been proven. Perhaps that is the most effective way to avoid becoming a victim of scam now and in the future. Happy surfing!

7. References

[1] BBC News World Edition, 29 December 2004, Cyber Crime Booms in 2004, by Mark Ward, Technology Correspondent, BBC News Website.
http://news.bbc.co.uk/2/hi/technology/4105007.stm

[2] eWEEK Enterprise News & Reviews, 9 December 2004, Spy-ware: The Next Real Threat, by Ryan Naraine.
http://www.eweek.com/article2/0,1759,1738207,00.asp

[3] Drama movie: **IDENTITY THEFT**. Director: Robert Dornhelm. Starring: Kimberly Williams-Paisley and Annabella Sciorra. Year: 2004.
http://www.lifetimetv.com/movies/info/move3633.html

[4] Federal Trade Commission, Facts for Consumers, February 2005, Take Charge: Fighting Back Against Identity Theft (formerly: "ID Theft: When Bad Things Happen to Your Good Name").
http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

[5] CERT Coordination Center, Carnegie Mellon University, 2002, Organized Crime and Cyber-Crime: Implications for Business, by Phil Williams.
http://www.cert.org/archive/pdf/cybercrime-business.pdf

[6] The Computer Emergency Response Team of the Dutch Government.
http://www.govcert.nl

[7] The Australian Computer Emergency Response Team.
http://www.auscert.org.au

[8] The Anti-Phishing Working Group.
http://www.anti-phishing.org

[9] The Anti-Phishing Working Group Phishing Archive, 14 January 2005, TCF Bank – "TCF express checking card alert".
http://www.antiphishing.org/phishing_archive/01-19-04_TCF/01-19-04_TCF.html

[10] The Anti-Phishing Working Group Phishing Activity Trends Report, December 2004.
http://antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf

[11] The Nigerian Law, Part 6: Offences Relating to Property and Contracts.
http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm

[12] The 419 Coalition Website, The Nigerian Scam Defined.
http://home.rica.net/alphae/419coal/

[13] Snopes.com, 6 September 2003, Nigerian Scam, by Barbara "fraud gods" Mikkelson.
http://www.snopes.com/crime/fraud/nigeria.asp

[14] Quatloos.com, Nigerian 4-1-9 Scam.
http://www.quatloos.com/scams/nigerian.htm

[15] The 419 Coalition Website, Nigerian Scam – Sample 419 Letters.
http://home.rica.net/alphae/419coal/samplesmain.htm

[16] Quatloos.com, Nigerian 4-1-9 Scam Lettery Exhibit.
http://axiusnews.com/scampost/default.asp?offset=0

[17] FraudWatchInternational, Major Internet Frauds – Lottery Scams.
http://www.fraudwatchinternational.com/internetfraud/lottery.htm

[18] FraudWatchInternational, Lottery Scams Emerge as Major Internet Fraud.
http://www.fraudwatchinternational.com/about/040503_lottery.htm

[19] FraudWatchInternational, Frauds & Scams List.
http://www.fraudwatchinternational.com/frauds_and_scams/list.htm

[20] FraudWatchInternational, Major Internet Frauds – Online Auction Fraud.
http://www.fraudwatchinternational.com/internetfraud/auctions.htm

[21] FraudWatchInternational, Work-at-Home Scams.
http://www.fraudwatchinternational.com/frauds_and_scams/work_at_home.htm

[22] World Privacy Forum, A Year in the Life of an Online Job Scam, by Pam Dixon, Principal Investigator.
http://www.worldprivacyforum.org/jobscamreportpt1.html

[23] FraudWatchInternational, Page-Jacking and Mouse-Trapping.
http://www.fraudwatchinternational.com/frauds_and_scams/pagejacking_mousetrapping.htm

[24] Tech Law Journal, How the "Page Jacking" and "Mouse Trapping" Web Scam Works.
http://www.techlawjournal.com/internet/19990924b.htm

[25] FraudWatchInternational, Advance Fee Loans.
http://www.fraudwatchinternational.com/frauds_and_scams/advance_fee.htm

[26] FraudWatchInternational, International Modem Dialing.
http://www.fraudwatchinternational.com/frauds_and_scams/international_modem_dialing.htm

[27] Bankrate.com, 26 March 2003, Skimming the cash out of your account, by Laura Bruce.
http://www.bankrate.com/brm/news/atm/20021004a.asp?prodtype=bank

[28] FraudWatchInternational, Skimming.
http://www.fraudwatchinternational.com/frauds_and_scams/skimming.htm

[29] InfoHQ.com, 17 January 2004, Fighting Back Against Email Spammers, Internet Hackers, and other Web Thieves.
http://www.infohq.com/Computer/Spam/fight-internet-hackers-email-spammers.htm

[30] Hixus Software, Web Design & Development Tools, Spam.
http://hixus.com/modules/page/?artid=7

[31] Anti-Spam-Software.com, The Online Guide to Spam Email, section 11 of 14 – What is an open relay?
http://spam.anti-spam-software.com/relay.htm

[32] NewScientist, 3 November 2004, How zombie networks fuel cyber crime, by Celeste Biever.
http://www.newscientist.com/article.ns?id=dn6616

[33] ZDNet UK, 22 September 2004, Most spam generated by botnets, says expert, by Dan Ilet.
http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm

[34] ZDNet UK, 20 October 2004, Phishing attacks powered by 'just five' zombie networks, by Graeme Wearden.
http://news.zdnet.co.uk/internet/security/0,39020375,39170848,00.htm

[35] PC WORLD, 9 July 2004, Zombie PCs: Silent, Growing Threat, Spam, worms spread malware to build a spam-bot army of unwitting recruits, by Daniel Tynan, Special to PC World.
http://www.pcworld.com/news/article/0,aid,116841,00.asp

[36] N3dst4.com, “URL Obfuscation” and how it works, by Neil de Carteret.
http://www.n3dst4.com/articles/urlobfus

[37] PC-help.org, 13 January 2002, How to Obscure Any URL, How Spammers And Scammers Hide and Confuse.
http://www.pc-help.org/obscure.htm

[38] The Internet RFC/STD/FYI/BCP Archives, RFC 1738 – Uniform Resource Locators (URL).
http://www.faqs.org/rfcs/rfc1738.html

[39] IBM, 1 September 2002, Cross-Site Scripting, Use a custom tag library to encode dynamic content, by Paul S. Lee, I/T Architect, IBM Global Services.
http://www-106.ibm.com/developerworks/security/library/s-csscript/

[40] Netcraft, 15 February 2004, Visual Spoofing Offers new Opportunities fro Phishers, posted by richm.
http://news.netcraft.com/archives/2004/02/15/visual_spoofing_offers_new_opportunities_for_phishers.html

[41] Demonstration of Visual Spoofing Technique, by Don Park.
http://www.docuverse.com/visualspoof/

[42] Microsoft Corporation, Microsoft TechNet, 1 December 2004, Version 1.0, Microsoft Security Bulletin MS04-040, Cumulative Security Update for Internet Explorer (889293).
http://www.microsoft.com/technet/security/bulletin/ms04-040.mspx

[43] AusCERT, Australian Computer Emergency Response Team, 9 December 2004, AL-2004.041 – Window Injection Vulnerability in Multiple Web Browsers.
http://www.auscert.org.au/render.html?it=4602

[44] GIAC.org, GSEC Practical Assignments, 16 February 2001, Man-In-The-Middle Attack, by Bhavin Bharat Bhansali.
http://www.giac.org/practical/gsec/Bhavin_Bhansali_GSEC.pdf

[45] SearchSMB.com, SearchSMB.com Definitions, 9 July 2004, Adware.
http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci521293,00.html

[46] SearchSMB.com, SearchSMB.com Definitions, 5 February 2005, Spyware.
http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00.html

[47] Microsoft Corporation, Microsoft Help and Support, 27 January 2005, Article ID: 49500, Revision 13.1, List of anti-virus software vendors
http://support.microsoft.com/kb/49500

[48] Gizmo Richards’ Tech Support Alert Home Site.
http://www.techsupportalert.com

[49] Tech Support Alert, Anti-Trojan Software Reviews, A survey of the best anti-Trojan programs, by Ian Richards.
http://www.anti-trojan-software-reviews.com/

[50] Tech Support Alert, February 2005, The 16 Best-ever Freeware Utilities, by Ian Richards.
http://www.techsupportalert.com/best_16_free_utilities.htm

[51] Raytown Corporation LLC, Anti-Keyloggers.com.
http://www.anti-keyloggers.com/

[52] Spydex, Inc., Advanced Security Software.
http://www.spydex.com/

[53] ABOUT, Email, What You Need to Know About Bayesian Spam Filtering, by Heinz Tschabitscher.
http://email.about.com/cs/bayesianfilters/a/bayesian_filter.htm

[54] PC WORLD, 20 September 2004, Spam Slayer, New Tools Fight Phishing Scams, Swindlers combine spam with hoax sites to try to rip off your personal data, by Tom Spring, PC World Senior Writer.
http://www.pcworld.com/news/article/0,aid,117790,00.asp