Global Information Assurance Certification Paper

Pierre Zschocke

GSEC - Practical

Index

Abstract
One of the latest Internet security threats that is making the headlines in many countries around the world is concerned with email fraud or phishing as it is now commonly known. This paper will explain what phishing is, what protection measures one can take to avoid becoming a victim and what to do if you have already become a victim. It will also give information on where to find information on commercial solutions for this problem

Caught, Hook, Line and Sinker

Introduction

Every angler dreams of catching that fish of a lifetime; the one that he can boast about to his friends while having a drink at the pub. If the fish is lucky it will be photographed by its capturer and returned to the water. If it is not so lucky it will probably end up in a glass case or on a dinner plate.
You're probably already asking yourself what has angling got to do with a paper about information technology security?
Well, there are other people out there fishing as well and also dreaming about the catch of a lifetime but their form of fishing has much more sinister intentions and the catch is definitely not returned. We are not talking about sitting down at the lakeside on a warm summers evening casting out to the rising fish but we are talking about something that has been making the headlines recently with increasing frequency. We are talking about phishing.

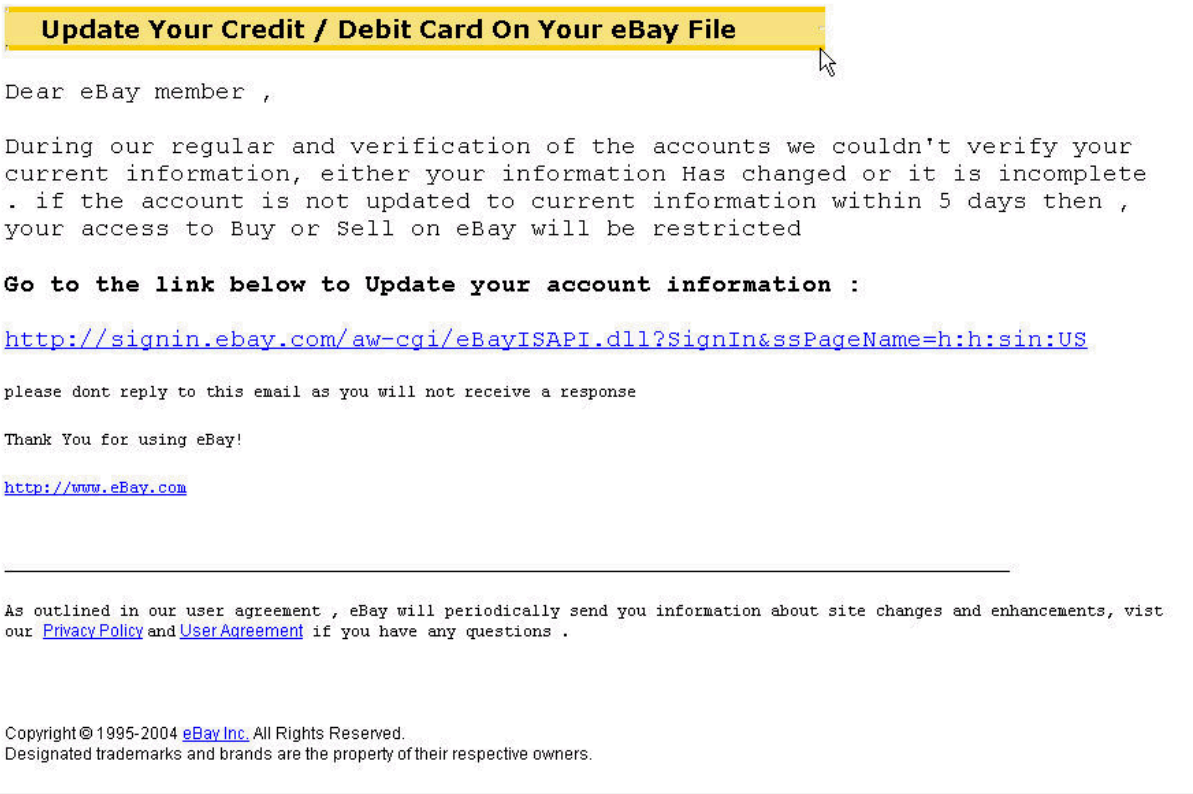
What is phishing?

The word Phishing is the term invented by hackers who have thought up a way of enticing people to share their passwords, financial data or credit-card numbers. As security awareness increases among computer users and more effective software is being used to prevent unauthorized access to private and confidential data the hackers and scammers have to find ever more sophisticated means of obtaining this data. Phishing is the latest method of obtaining this data. The method used is to send a fake email that imitates an email from a legitimate company. Contained in this email is a link to the hackers own website. Once the user has been redirected to the hackers website by clicking on this link, a page is displayed which may or may not be identical to the legitimate company's. He will then be fooled into entering his password or credit-card number and other confidential information that can then be harvested by the hacker. We will have a look at some of these fake emails and web sites and you can judge for yourself whether you would have taken the bait or not.
A recent study by CipherTrust Inc discovered that most of these phishing mails have originated from about 1000 zombie computers. These computers had been compromised by hackers at an earlier stage and are now being used to send spam mails and phishing mails.

Symantec releases an Internet Security Threat Report twice yearly that analyses trends in Internet attacks, malicious code and vulnerabilities. In the latest release from September 2004 one of the predicted top threats to look out for in the coming months will be phishing.

Taking the bait.

Phishing is being reported as a new hacker method but it is really just an improvement of old methods for tricking computer users into divulging confidential information. I remember being caught some years ago as a new computer user while being online. A message, supposedly from my ISP, popped up telling me to enter my password otherwise my modem connection would be lost. So I did just that. Luckily I realised what I had done and managed to change my password before anyone else used my account. Other people are not so lucky and often do not realize that they have been spoofed into giving away their confidential data until their bank account has been plundered or their credit card has been used by someone else.
Lets have a closer look at some of these scams and at some of the characteristics that could help you to avoid being caught out.
The following diagrams are from a fairly recent scam that was bought into circulation on 05 May 2004 and was addressed to Ebay users.



Update Your Credit / Debit Card On Your eBay File

Dear eBay member ,

During our regular and verification of the accounts we couldn't verify your current information, either your information Has changed or it is incomplete . if the account is not updated to current information within 5 days then , your access to Buy or Sell on eBay will be restricted

Go to the link below to Update your account information :

http://signin.ebay.com/aw-cgi/eBayISAPI.dll?SignIn&ssPageName=h:h:sin:US

please dont reply to this email as you will not receive a response

Thank You for using eBay!

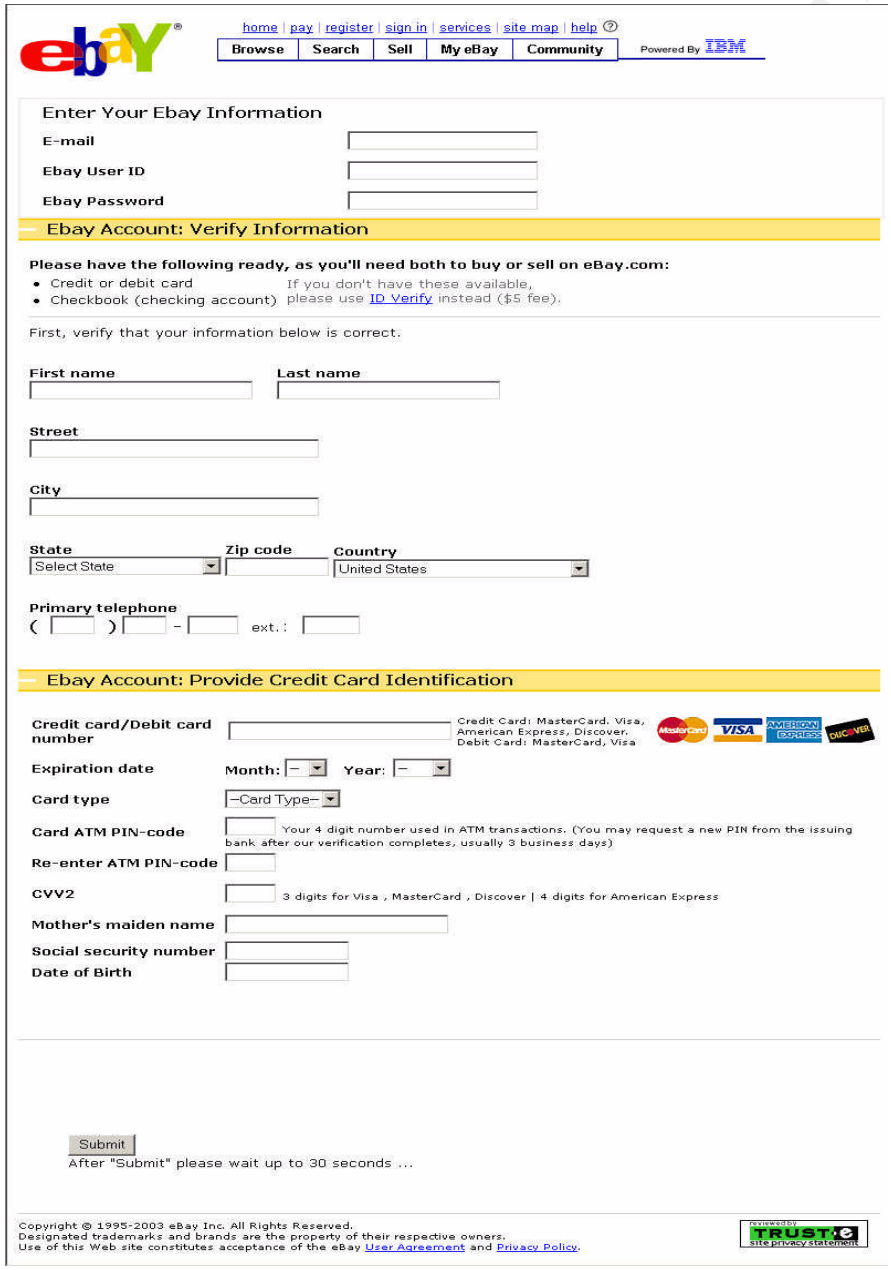
http://www.eBay.com

As outlined in our user agreement , eBay will periodically send you information about site changes and enhancements, vist our Privacy Policy and User Agreement if you have any questions .

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.

This is the original email that users received asking them to update their credit card details. The sender of this mail “support@ebay.com” would at first

sight appear to be genuine. Who really knows whether there is a mailbox at Ebay named support@ebay.com?
One of the first things that would make many people suspicious is the incorrect grammar and spelling but somebody who only glances over the text or whose command of the English language is not particularly good may well oversee this.
The second sign that this mail is not genuine is that the Ebay logo is missing but because of the fact that it is missing means that this clue could easily be overseen.
Of course the visible link in this mail is spoofed and when it is clicked it directs the user to the phishers site where information is asked for.



This page looks absolutely genuine and would fool most people into entering the data that is required.

The only clues that could cause someone to become suspicious is the called URL is not the original Ebay server and that this is not a secure site (not HTTPS:)

This example has a few telltale signs that would cause the aware person to become very suspicious of the senders intentions. But would you have become suspicious if those spelling and grammatical errors had not been there?
With some of these mails it is extremely difficult to determine whether they are genuine or not. Take a quick online test at http://survey.mailfrontier.com/survey/quiztest.html to see whether you would have been fooled by some of these scams.

Dinner plate or back to the water?

What do fraudsters do once they have collected your confidential information? Here is a summary of the frequent ways in which this personal information is used:
Hijacking user accounts
Fraudulent use of credit cards
ATM card duplication
Identity Theft

1. Hijacking bank accounts
If bank account information was provided, it is then possible for the fraudsters to hijack the victim's bank account by changing the access passwords. This effectively locks out the legitimate account holder from their own account. The funds can then be transferred to another account that has been set up using stolen personal information. The cash is then withdrawn from the second account often before the victim realizes that anything is amiss.
The fraudsters may just keep hold of the stolen account information and wait for a time when there is enough money in the account before making their move.

2. ATM card duplication
Some fraudsters have the ability to reproduce ATM cards. With the card information obtained through a phishing scam it is then possible for them plunder the victims account.
3. Fraudulent use of credit cards
With the credit card information that has been obtained it is quite easy for the fraudsters to make unauthorized purchases. This information is also sold to organized fraud rings. If the victim is unaware that their credit card information is in the hands of criminals they will probably only get notice of

this when they receive their next statement or try to purchase something with their card only to find out that their credit limit has been reached.

4. Identity Theft

According to Privacy Rights Clearing House (http://www.privacyrights.org/) there have been 27.3 million Americans victims of identity theft in the last five years. The theft of this information is used to apply for credit cards, make unauthorized purchases, gain access to bank accounts, apply for driving licences or to provide illegal immigrants with an identity. Identity Theft is reported to be the world's fastest growing crime. Identity thieves used to scavenge through rubbish bins looking for personal information that they could use to impersonate someone else. Their life has been made much easier with the use of the Internet and phishing scams.

Detection and Prevention.

While writing this paper an announcement has been issued that America Online is to be the first online service to offer Two-Factor authentication to consumers that will offer a second level of account protection by automatically generating a supplemental password.

The user receives a keychain-sized device after buying this service which creates a unique six-digit numeric code every 60 seconds.
To help protect your screen name with AOL PassCode, you need to secure your screen name to your specific AOL PassCode device. Each AOL PassCode has a unique serial number engraved on its back. This specific AOL PassCode serial number is then associated to a screen name after which the AOL service will know which six-digit number can be entered along with the normal login password, helping to protect the AOL account from unauthorized access. To log into an AOL account, users are prompted for both their normal password and the token code generated by the PassCode device. This means that even if the normal login password has been divulged to someone else it cannot be used unless a correct six-digit code is also entered.

Another announcement that has been made while writing this paper states that Microsoft and Amazon are going on the offensive against these phishing fraudsters that are using false emails and websites. These two companies have filed a federal lawsuit against Canadian company Gold Disk Canada Inc. and three other persons for allegedly sending unsolicited emails using Microsoft's MSN Hotmail services and spoofing, or forging, the name of Amazon.com with the intent of obtaining website passwords and credit card numbers of Amazon customers.
Microsoft and Amazon have worked closely together to identify the offenders and are collaborating to test technical solutions that would make it more difficult to send unwanted messages to consumers.

In the USA professional spammers can receive up to 5 years imprisonment

but the flood of unsolicited emails is still continuing to rise!

These reports show that phishing is a very current problem and that information technology companies are in the process of developing solutions to make life more difficult for online conmen.

How to Avoid Phishing Scams

In a company environment these mails can easily be blocked at the mail gateway by a mail scanner or anti-spam software. Rules can easily be created to block all mails from this sender but this still requires that the System Administrator has already received information about a particular scam and has the necessary information to be able to create such a rule. This is a good reason for the System Administrator to subscribe to an alerting service so that he receives timely information on present threats.
Consumers however may not have this information or the technical capabilities at their disposal to prevent these scam mails getting into their in-boxes and will have to make use of other practices to avoid being caught out.
Even though setting up rules for the perimeter mail gateway to block spam mails is an easy task it is certainly not the most effective method of blocking these spam mails. There are however many other factors involved in a corporate environment that can contribute to these rules not being created and implemented and therefore letting these fraudulent mails through to their potential victims.
Even if a company has subscribed to an alerting service that provides information on phishing scams currently in circulation, this information still has to be filtered from maybe hundreds of other security alerts that a system administrator may receive on a daily basis. As we all know system administrators just do not have the time to react and apply fixes to all security threats that are in circulation.
Phishing mails are spam mails and can be treated as such by blocking these mails at the gateway. As we all know spammers use ever more sophisticated tactics to evade spam filters that means that it is no longer possible to filter all spam by manually creating spam rules for spam filters. This approach would consume an immense amount of time and would not be very effective.

The providers of many antispam solutions advertise that their solutions work out of the box but often these solutions require that the administrator and end users undergo substantial training to provide an effective antispam measure. One of the most effective solutions on the market today is Symantec's Brightmail.
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=642

The backbone of the Brightmail solution is the BLOC (Brightmail Logistics and Operations Centers) that are antispam operations centers based in 3 continents around the world that provide a round-the-clock protection network. These centers provide the real-time tuning of the Brightmails

antispam filters. BLOC technicians monitor and evaluate mail for new variations using sophisticated tools and then issue filters to block similar mails. These updated filters are then continuously delivered to customers sites providing almost real-time filtering rules. BLOC monitors over 2 Million decoy mail accounts that attract tens of millions of junk and spam mails. Symantec Brightmail AntiSpam presently incorporates 17 different antispam filtering technologies and is continually evaluating other new filtering techniques so that it can maintain its present accuracy rate. Currently Brightmail is in the position of delivering only 1 false positive in 1 million messages that is an accuracy rate of 99.9999%.

On the consumer side, there are many solutions to choose from. One of the biggest problems here is that the user has to decide for themselves whether a mail is spam or not. This is really of little use as the phishing mail is designed to dupe someone into believing that it came from a genuine source. It is really up to the user to be aware of the problem and to take other steps that are mentioned in this paper to avoid becoming a victim.

Online banking and e-commerce can generally be considered to be very safe and because of this reason it is difficult if not impossible for hackers to intercept confidential data. However one should still be very careful about what information is given out over the Internet.
This is also the reason why the sophistication and number of phishing scams sent out to consumers is continuing to increase dramatically.
There are a number of recommendations that can be followed to avoid becoming a victim of these scams.

A) Any email that urgently requests personal financial information should be viewed with suspicion. If emails have been digitally signed then it is unlikely to have been spoofed and will have come from a legitimate source.

B) If the email contains a link to a web page then type this link directly in your browser. It could be that the link that can be viewed in the email directs you to different web server.

C) If you are suspicious about any email then contact the company concerned for confirmation.

D) A typical phishing email will include information that asks you to react immediately in the hope that you will act before thinking. Phishing mails normally ask for personal and confidential information about usernames, passwords and credit card numbers.

E) Phisher emails are typically often not personalized, while valid messages from your bank or e-commerce company generally are. If we look at the example phishing mail above we see that the Ebay Logo had not been included in the mail.

F) If you are asked to fill out a form in an email messages that ask for personal financial information ensure that you do this via a secure site.

Check whether it is a secure site by looking at the web address in your browser address bar. It should begin with https://.
You should only communicate information such as credit card numbers or account information on the Internet via a secure website.
There are Web browser tool bars that are freely available that warn you if you are connecting to a known fraudulent website.
A free browser tool bar can be downloaded from: -

http://www.earthlink.net/earthlinktoolbar

G) Log in to your online accounts regularly. You will then soon discover whether your password has been changed or whether money has been withdrawn from your account. Passwords should be changed regularly as a security measure. It could be that someone has already obtained your account login information but has not yet had time to logon to your account. A timely password change could foil the fraudster.

H) Get into the habit of installing security patches. This is not just a good idea to foil phishing attacks but could also foil any other attacks that use vulnerabilities in the operating system or applications. As stated earlier, zombie computers are being used to distribute phishing mails and these machines were probably compromised by not having the latest security patches installed.

I) Contemplate changing your Internet browser. Some scams use vulnerabilities in Microsofts Internet Explorer. As this is the most widespread browser in use it will always be the first on the list to be targeted by phishing scams and other attacks. Hackers and scammers obviously want their attack to have the widest impact and this can only be achieved by targeting vulnerabilities that will be widespread. You should however still regularly apply any applicable patches to whatever browser you are using.

J) Install Anti-Virus software and keep the virus signatures up to date. Regularly complete a manual scan of all your disks.

K) Some exploits actually change the hosts file on Windows systems. This means that even if you have entered the correct Internet site in your browser you will be directed to a fake site. To avoid this, the hosts file should be made read only.

What to do if you become a victim of a phishing scam.

If you have become a victim or have received emails that you believe to be fraudulent then you should report this to the appropriate authorities in your country. They will require a copy of the fraudulent email that will contain information they require to be able to trace the web site and possibly the persons behind the scam.
In the U.S.A. you should report any attempted internet fraud to the FBI (FBI: Internet Fraud Complaint Center) They work on a worldwide basis with other

law enforcement agencies to track down the fraudsters and to close down any fraudulent web sites.
If you have given away any of your personal data concerning your accounts with any financial institution you should immediately inform these institutions to block your accounts to prevent any illegal cash withdrawal.

Summary

Because of the financial loss and loss of consumer trust in using Internet based transaction methods that can be caused by these attacks, a group has been formed that provides useful information about phishing. This group the Anti-Phishing Working Group can be found at http://www.antiphishing.org
This organisation was created with the purpose of eliminating the problem of phishing and email spoofing attacks. They do this by developing and sharing information about the problem and increasing awareness of industry solutions that assist in preventing these attacks. Membership of this group includes qualified financial institutions, corporations, law enforcement agencies, public policy groups and solution vendors.
They publish a monthly Phishing Attacks Trend Report that lists such things as the average monthly growth rate, the number of unique phishing attacks reported, which oorganizations are most targeted and the country hosting the most phishing Web sites.

Due to the fact that some of these phishing e-mails and Web pages look exactly like those of legitimate companies, 5% of the recipients of these e-mails actually enter the data that's requested according to the Anti-Phishing Working Group. An angler reporting a 20:1 ratio between casting a bait and catching a fish would indeed be very pleased with his return rate. A Gartner study released in May reported that approximately 1.8 million consumers had been tricked by phishing mails into divulging personal information within the last year. On average each incident cost the victim $1200.
This problem is not going to go away as long as the fraudsters are getting these return rates and according to the latest Symantec Internet Security Report (http://enterprisesecurity.symantec.com/article.cfm?articleid=4776&EID=0) this threat with be one of the top threats to watch for in the coming months.

Even though this type of scam can be fairly easily avoided it still presents a problem mainly to consumers because of their lack of knowledge about the presence of a particular Internet attack or scam.
While investigating the problem of phishing I have found many tips for preventing and avoiding this scam and a lot of information that was new and helpful to me. One of the methods of prevention is having the knowledge about this type of attack so that one is not fooled into becoming a victim. Having this knowledge is probably the best method of prevention but how can this information be disseminated to everybody that uses a PC for conducting online transactions?

I believe it is the duty of all financial institutions and companies that conduct online trading to inform their customers about these dangers. This is happening to some extent but more often than not this happens after the horse has bolted. There is certainly room for improvement and many more people and companies will become victims of these scams before an efficient solution is found.
Operating system and application security has been increasingly focused on in the past few years by their manufacturers and there has been an improvement in this area but there are still many more software vulnerabilities that have to be fixed before all systems can be considered safe to use in an increasingly dangerous connected world.

References

Privacy Rights Clearing House http://www.privacyrights.org

Anti-Phishing Working Group http://antiphishing.org

Symantec Internet Security Threat Report
http://enterprisesecurity.symantec.com/article.cfm?articleid=4776&EID=0

Symantec Brightmail AntiSpam
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=642

The Internet Fraud Complaint Center (IFCC) http://www.ifccfbi.gov/index.asp

AOL® PassCode
http://help.channels.aol.com/article.adp?catId=6&sCId=415&sSCId=4090&articleId=217623

Microsoft - 5 ways to help protect your identity
http://www.microsoft.com/athome/security/email/phishing.mspx

Gartner: Phishing on the rise in U.S.
http://news.com.com/Gartner+Phishing+on+the+rise+in+U.S./2100-7349_3-5234155.html