GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

An analysis of Phishing and possible mitigation strategies

© SANS Institute 2004, Author retains full rights.

Barney Rudd
June 27, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

With the growth of the internet and e-commerce identity theft has once again become a more significant and potentially large problem for the 21st century. Amongst these types of attacks is "phishing", where online users give away their passwords or credit card details after receiving a convincing but fake email that pretends to be from their bank or e-commerce site. In the last 6 months these scams have risen dramatically and along with it in sophistication. The most targeted being the customers of online banks and e-commerce companies. This paper is an introduction to phishing, and aims to discuss the basics of phishing, what it is, how the scams are run, why they are run and who is behind them. It then looks at the common techniques used by the phishers followed by an analysis of some recent phishing scams. It also will discuss the mitigation of phishing through prevention, detection and response. Finally there is a section on the future of phishing, looking at both sides, the attackers and the defenders.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

What is Phishing?

"Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc."[1] This is a social engineering attack that targets vulnerable online consumers and, depending on the particular scam, uses weaknesses and exploits in email and web browsers.

It is considered a form of spam that results in identity theft. Once the consumer submits his personal details, the identity theft has been successful.

This term was first seen in hacking newsgroups around 1996 when hackers were stealing AOL[2] passwords. It's derived from fishing where a fisherman uses a lure to attract fish in the same way that the attackers use an email to attract online consumers. Finally the 'f'' from fishing has been substituted for with 'ph' to form "phishing". This is in recognition of the original hacking method phreaking[3].

Who Performs Phishing?

Initially most of the Phishing scams were run by novices[29]. But in the last few months there has been a shift towards scams run by organised criminals[29.] In the UK they are particularly concerned with Eastern European crime syndicates and they made a number of arrests of Eastern Europeans operating within the UK[6]. The organised crime groups have recruited highly skilled programmers to help them exploit their scams[6]. The Philippines, china, South Korea and Russia have been linked back to fraudsters[1].

Why do people 'phish'?

Phishing is profitable. The Anti-phishing Workgroup states that 5% of attacks result in identity theft[26]. A Gartner survey of 5000 estimated the damage from Phishing in 2003 cost US Banks and credit card companies $1.2 billion in 2003[3]. Actual losses are much lower, monetary values of losses are difficult to obtain but Paypals loss rate from fraud is 0.33%[2°]. Australian banks have recently put aside $2 million to cover losses from phishing[1]. British banks estimated they lost £1 million through phishing scams[2].

---

[1] Anti-Phishing Workgroup. http://www.antiphishing.org

[2] AOL - America Online. A very large ISP which offered very cheap deals to access the Internet. As such, many of its users were not very security aware or Internet literate, and they fell for most of the scams and problems which occurred over the years.

[3] "phreaking" is where a hacker would take over someone else's phone line and use it for their own use, including hacking into other computers.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Phishing scams are easy to mount. A web server, a bulk mailing tool, a form e-mail and a database of e-mails would be enough to mount a phishing scam.

Prosecution of Phishing scams is difficult. To date prosecutions of Phishing scams has been limited. The major prosecutions to date have involved only one jurisdictional area or the local part of a scam operated from overseas. The difficulty lies in the borderless nature and anonymity of the internet. The people behind the scams and the ghosted web servers are quite often located overseas. Without legal treaties and common law it's difficult to prosecute.

Finally the security at the banks and e-commerce sites is generally too hard to break into, as the link from customer to bank is usually a 128 bit encrypted SSL link. This leaves the consumers, who may be vulnerable to a smartly crafted social engineering attack such as phishing.

Which companies are targeted?

The main targets are financial institutions and e-commerce companies, particularly online banks. The top four targets according to the Anti-Phishing Work Group in April 2004 were Citibank, eBay, PayPal and US Bank. The table below shows a breakdown of unique Phishing scams reported in the last 6 months.

Figure 1 Unique phishing attacks for last six months from the Anti-Phishing Work Group

How do the scams work?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The resources needed for a Phishing scam are a bulk mailing tool, a form e-mail, a ghost website, and a database of email addresses.

First, the ghost is setup and then the bulk e-mails are sent. The email is branded to look like it's from the particular financial institution or e-commerce site and the 'from' address is spoofed to appear from that domain. It usually includes an URL, which appears to be linking back to the appropriate site, however the actual link points to the ghosted website. The email is designed to provoke an immediate reaction and for example might mention something about a non existent transfer, or fees which will be charged without an immediate reply, etc.

The ghost website usually will have some form of address bar spoofing to mask the real address. That is, the user is fooled into thinking that they are at the legitimate site of the bank or e-commerce site. If the user is fooled they click on the link and then submit their pin code or credit card details and may be presented with a message, or may be forwarded to a page on the authentic website.

The phishers must then retrieve the stolen information; this could be by anonymous login or email, although this is only speculation.
Once the phisher has the information they then try to get the money or goods using the stolen identities. Quite often a local operation is setup to siphon the money out of the country using valid bank accounts[13].Recently 12 people of eastern European nationalities were arrested in England for laundering money from a phishing scam[13].

Where do the phishers get their email addresses from?

Phishing is considered part of spamming and as such they would use similar resources. There is evidence to suggest that phishers are swapping databases and techniques [23].

Phishing techniques

<u>The email:</u> The email is designed to provoke an immediate reaction from the victim. Common themes are confirmation of a transfer, account verification, or "congratulations, you have won a prize!". The emails are usually long and sent in html format. The long emails are meant as a deterrent if someone wants to verify the source code. For the ordinary internet user it's not that quick to find the actual link amongst a jumble of html. Good phishing scams will also make an attempt at branding, which means putting in the company logos and formatting. Occasionally the scammer uses a form inside an email, but most commonly the email contains a link pointing to the spoofed website.
The visible link usually shows a valid address of the company website. The actual link can only be seen within the html source code of the email. Finally the phisher spoofs the 'From' field so that it appears to come from the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

authentic business site. A convincing email would be one that uses branding and uses good grammar.

The ghost website: Is usually a copy and paste version of the login page from the authentic website. Phishers use either a hijacked PC, hacked web domain or a similar domain name to host the website. The domain name looks similar to the actual site. An example is "www.paypa1.com", which was used instead of "www.paypal.com"[22]. Quite often the spoofed website is located offshore because it's more difficult to shutdown[17]. The phishers needs a method to collect all the stolen data; they could do this via anonymous login or email. However this is just speculation.

Hiding or spoofing the address bar: To make the spoofed site look more authentic an attempt is made to change or cover the address bar in the web browser to make it look like the authentic URL. Both the Opera and Microsoft IE web browsers have patched vulnerabilities that allowed their address bars to be spoofed[20]. Phishers have used this Microsoft vulnerability in numerous phishing scams[20]. In March the technique using JavaScript to show a fake address bar was published, it appears that this particular technique was first used in February[21]. The spoofed website detects the browser type and runs a browser specific JavaScript that suppresses the real address bar and displays an fake address bar with an address from the authentic site. Another technique is to add a sub domain so that the page appears to be for the real site. For example "http://www.realbank.com.au.fakedomain.com/.".

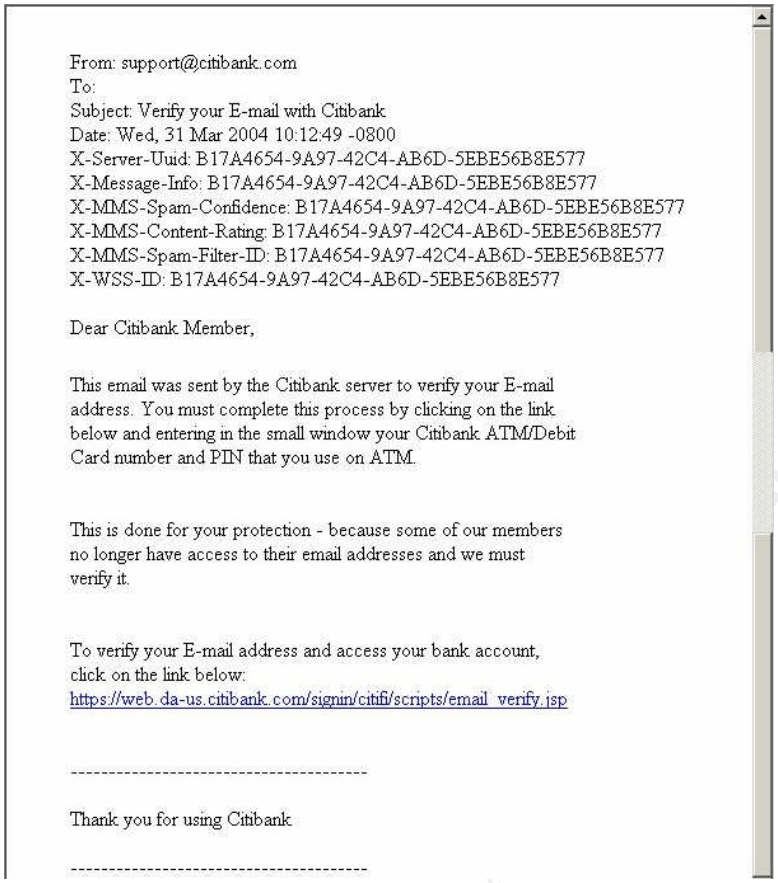
Popup windows: Instead of hiding or spoofing the address bar some phishing scams use a popup window to authenticate and the real website in the background. The user enters his password or credit card details into the form. This can appear to be authentic as some banks use similar popup windows to authenticate. The only difference is that the spoofed web page doesn't contain the SSL padlock.

Use of Malware: Phishers are now starting to use some malware like Trojans and viruses in their scams.

Examples of scams

1) Citibank – 31st March 2004: This is one of a new breed of scams that uses JavaScript and frames to draw a window that suppresses the real address bar instead displays a fake address bar that shows a secure address of Citibank[15]. The aim of the scam is to harvest Citibank card numbers and their pins[15]. It appears this scam will work for Internet Explorer and Netscape browsers[15].

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



From: support@citibank.com
To:
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800
X-Server-Uuid: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-Message-Info: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Confidence: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Content-Rating: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Filter-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577
X-WSS-ID: B17A4654-9A97-42C4-AB6D-5EBE56B8E577

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

---

Thank you for using Citibank

Figure 2 - Spoofed email http:/www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm

The e-mail asks the user to verify their email address by clicking on the link. The link appears to be a valid Citibank site but in fact it's a bogus site (http://69.56.202.82/~citisecu/scripts/email_verify.htm) [15]. Some signs that give away this fake email as are that there is no branding (Citibank logo) and the use of poor grammar.

Figure 3 - URL redirect http:/www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm

As the web browser is redirected it briefly shows the real address bar before the JavaScript suppresses and adds the fake address bar[15]. This would be a sign of the scam for an alert user.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

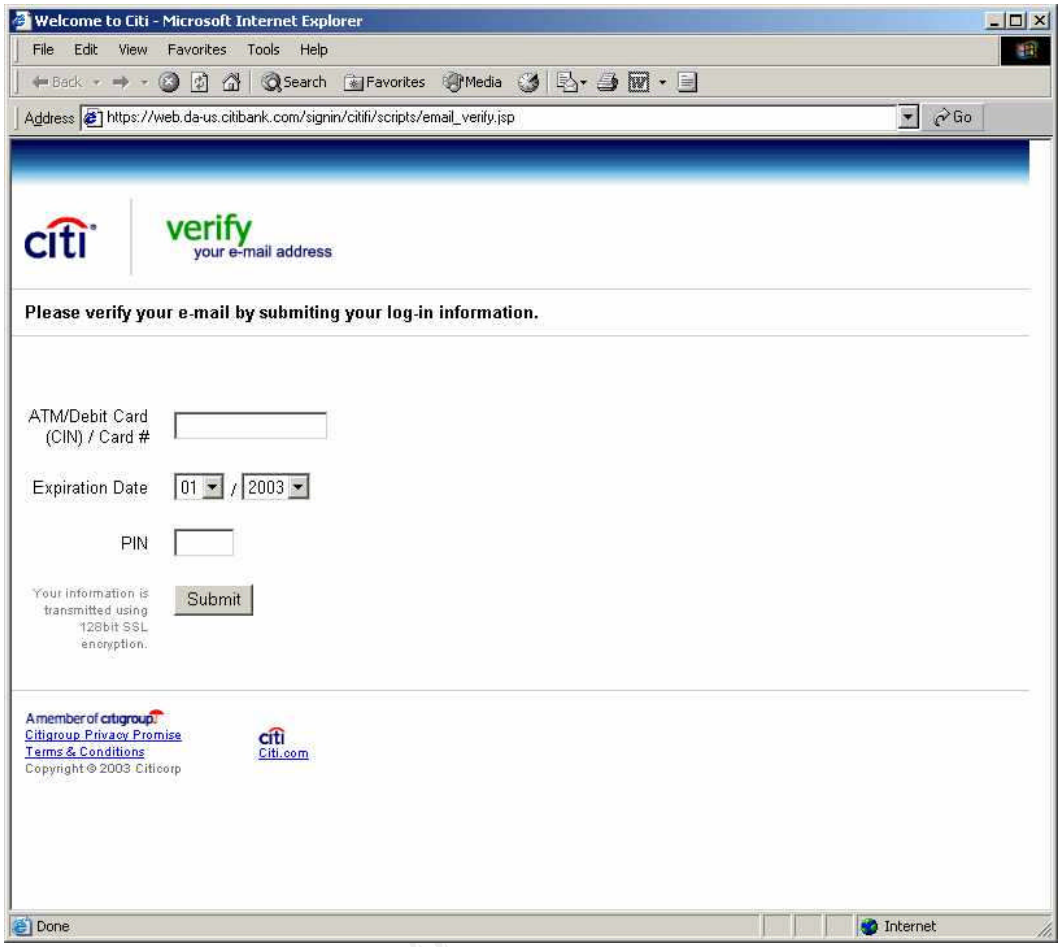


Figure 4 - Citibank_ghost_site - http:/www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm

The page is branded to look like the Citibank site, the address bar is fake. It is active java script and the real address bar is suppressed[15]. The user is then asked to submit his card details and pin[15]. Signs that give away this scam are that there is no SSL padlock but the address bar shows an https address, also if the user types another URL the title (Welcome to Citi), the browser does not redirect to the new URL[15]. This also raises another security because the fake address bar remains installed[15]. It could be possible to track the sites visited and possibly a man-in-the-middle-attack[21]. Another aspect that makes this scam more convincing is that right-clicking and viewing the source shows the html without the JavaScript, viewing the source through the menu will however show the JavaScript[15].

What happens after the user submits their personal details is unavailable, possibly they would be redirected to an authentic page on Citibank or to a page showing authentication failure. However this is only speculation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Example 2 E-gold 4 June 2004: E-gold is an e-commerce currency site. In this example the phisher has bought a similar domain egolds.org (a fake site) to the actual domain e-gold.com (the authentic site) [33]. The aim of the scam is to steal the user's E-gold username and passphrase[33].

The email is branded like it's from e-gold and the 'from' field is spoofed to appear to be from the e-gold.com domain. The visible link just shows 'Click Here'[33]. Interestingly the email from address changes in different emails to avoid the spam filters[33].

e-gold

Dear E-gold member,

As a part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

This email was sent by the E-gold server to verify your e-mail address. You must complete this process by clicking on the link below and logging in to your E-gold account. This is done for your protection, because some of our members no longer have access to their email addresses.

This is required for us to continue to offer you a safe and risk free environment to send and receive money online and maintain the experience.

As outlined in our User Agreement, E-gold will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Click Here

Thank You,
Accounts Management

Thank you for using E-gold!

Do not reply to this automatic email.

Figure 5- spoofed email - http://www.antiphishing.org/phishing_archive/06-04-04_e-gold_(Please_Verify_Your_Account).html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

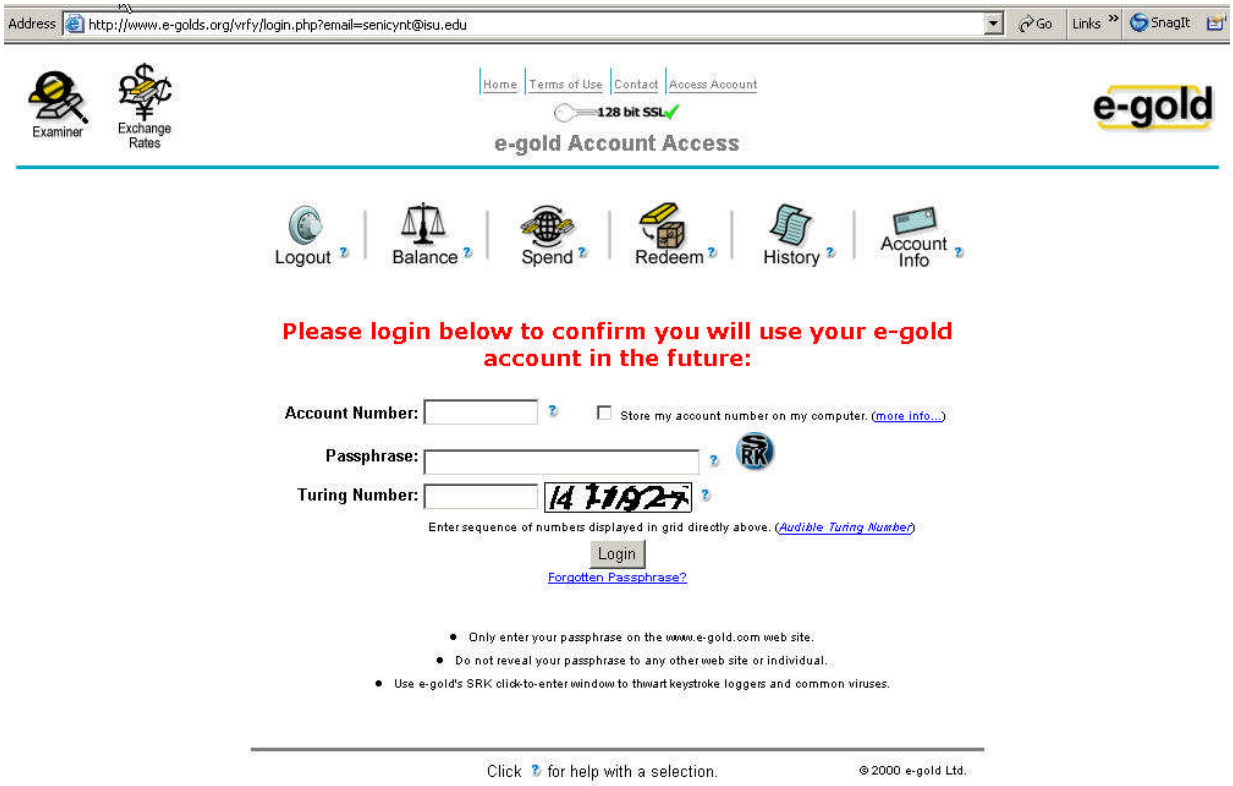


Figure 6 ghost website - http://www.antiphishing.org/phishing_archive/06-04-04_e-gold_(Please_Verify_Your_Account).html

The ghost website contains an identical authentication page to the actual E-gold site except the difference in the URL as discussed above. If the user was alert they would notice that there is no SSL padlock even though this is clearly documented in the authentication page[33]. The ghost website was still active several weeks after the scam was reported, even though the site is hosted within the United States. A ghosted website can be taken down between nineteen hours to six and a half days depending where the hosted site is, if it's overseas then it take s much longer[17]. E-gold has implemented some anti-fraud features; they include detecting IP address range changes, browser changes and e-mailing of a one-time pin. This link has more details http://www.e-gold.com/accsent.html.

Risks

The major risks associated with phishing, apart from the theft of identity, could be loss of consumer confidence in email, online banking and e-commerce. If phishing becomes a persistent problem then consumers may lose trust in e-commerce and online banking. This may slow down the adoption of e-commerce and online banking and in a worst case scenario they could go back to traditional methods of buying and banking, the E-commerce sites and banks could lose an economical and efficient way of doing business.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

E-commerce sites and financial institutions are losing email as a valuable and cheap communication tool

Firms also face the threat of loss of brand identity, as they are falsely represented by fraudsters pretending to send emails and hosting their websites. This is probably the biggest factor that will force e-commerce sites and financial institutions into using stronger two-factor authentication.

Finally phishing represents an easy money tool for organised crime.

Prevention

Consumers: The first step urged by security analysts, e-commerce, online banking and law enforcement is that the consumer should take proper precautions and to treat their online identities like they would their own wallets. If everyone did this then the number of successful phishing scams would dramatically reduce. E-commerce and banking sites now have a section on their web page devoted to security including precautions that their customers should take and the latest security alerts affecting them. For example the US Banks Email fraud page: http://www.usbank.com/cgi_w/cfm/promo/personal/fraud_email_info_and_help.cfm.The following list has been compiled from consumer awareness sites and banking sites and lists most of the common recommendations:

- check online accounts regularly to make sure they are correct
- apply latest security patches for operating system and browsers
- use anti-virus software and a personal firewall
- consider an antispam tool or an ISP that offers spam blocking services.
- use anti-phishing tool bar (see current solutions section)
- do not click on links within the email, open the web browser and type in the address.
- Do not fill out forms that appear in the email.
- Always make sure that a secure site is used when entering credit card or bank details.
- Be suspicious of urgent emails received asking to verify account details.
- Report suspicious activities to relevant website and or phishing tracking group like Anti-Phishing Work Group.

The media also has given big coverage to phishing scams. Nearly every article contains information to consumers about avoiding getting caught.

Financial and e-commerce sites: Implementation of 2nd factor authentication by all the banks would be a solution to phishing[9]. A quick look at the major banks websites in Australia and America reveals that they haven't implemented 2nd factor authentication and this probably holds for a lot of other countries. This could be a device that generates a pin or just a simple scratch card (this is particularly prevalent in Scandinavian countries[11]).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

E-commerce companies don't have the same options as the banks for two factor authentication as people usually have only one bank but could buy from several different e-commerce sites[11]. Imagine if a person was using ten different e-commerce sites[11]. E-bay for example enforces stronger passwords[11], but it does not use any further form of authentication.

The financial institutions are using velocity and IP address analysis to detect phishers cashing in on stolen data[1]. Some banks are already using e-mail authentication to sign their emails including JP Morgan Chase & Co and Bank of America Securities[10].

Detection and reporting of phishing

When a new phishing scam surfaces it is important to detect the scam as quickly as possible. This way the investigation can be started sooner and the scam shutdown quicker. Phishing scams can be reported through consumer alerts or real-time detection. The process usually involves the consumer reporting to the institution involved and then the institution reporting to the relevant authorities. There are also some groups that do semi independent analysis.

Consumer reporting: With the rapid increase in phishing scams the online companies and authorities have had to streamline reporting to ensure that phishing scams are easy to report and that there is minimum amount of time between a scan surfacing and being investigated. Time is critical because the ghosted sites are only online for a few days. Most financial institutions and e-commerce companies have published easy to access information on their websites on how to report a phishing scam. For example the US Bank website has a link "Email fraud and Online Security" on its front page which points to a page that explaining how to report phishing. It then gives an email address (fraud_help@usbank.com) to forward suspect emails to. Citibank (who have been the most targeted company in May) [in] particular have a list of recent scams with a link to each one[5]. Meaning that a reported phishing scam is immediately categorized as unique or known, speeding up the reporting process. In most case the reporting involves forwarding the email or suspect link.

The banks have streamlined their reporting[5] now and at some banks their call centres report new phishing scams directly to their IT staff.

Consumer reporting to independent groups: As well as reporting directly to the website involved there are some specialist sites that track and analyse the phishing scams. The most prominent is 'The anti-phishing workgroup' (APWG) who are an industry association made up of groups from various sectors including banking, E-commerce retailers, law-enforcement and service providers. They are looking at solving the problem of phishing and perform a wide range of tasks, such as analysis of attacks, tracking of scams and a monthly report which is used as a source for a lot of articles on

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

phishing. Once a suspect email has been reported they analyse the email and ghost website. This information is then passed onto the relevant authorities where appropriate[5]. A lot of the statistics for phishing quoted in the media are sourced from reports that this group produces.

There are other sites where phishing scams can be reported. Amongst these sites are "http://www.codephish.com" and "http://www.millersmiles.co.uk". They do detailed analysis of phishing scams that they receive.

Financial and online retailer reporting: Once the financial institutions and online retailers are aware of a new phishing scam it is reported to the law enforcement officials. In Australia a process is currently being setup where financial institutions can report phishing scams to the Australian High Tech Crime Centre (AHTCC - a group under state and federal Police control that investigates computer related crime) and to the Australian Computer Emergency Response Team for Australia (AusCERT) [27].

Near Real-time detection: A recent development and an area of more development has been the near real-time detection of phishing scams. This is a more proactive approach which involves searching for ghost sites, doing trademark searches and scanning emails. The advantage being that the ghost website and the scam can be shutdown much quicker than a scam that is reported by an online consumer. It is done in partnership with solutions provider and financial institutions, online retailers or ISPs. Real-time detection is also discussed later in the current solutions section.

Response and investigation

Once the alert has been raised there are various avenues that can be investigated, such as getting the appropriate authorities to shut down the fraudulent website, tracing the source of the emails, tracking the funds that the phishers steal and prosecuting the people perpetrating the scam. The main parties involved in the response and investigation are the financial institutions or online retailers that have been targeted in the scam, and the law enforcement officials.

Groups involved: The groups most involved would be the law enforcement agencies, the organisation reporting the phishing scam (for example Citibank). There would also be some involvement from the ISP where the ghost website is being hosted in cancelling the domain name and shutting down the website. In Australia a taskforce has been setup to combat phishing involving AHTCC, AusCERT and the finance sector[28]. This involves sending security staff from the banks to work alongside the staff at the AHTCC, assisting in investigations[28]. The cooperation will give law enforcement better access to financial data during fraud investigations[28]. Up until now there has been limited financial data that the banks would give law enforcement officials during a fraud investigation[28].

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Tracking and shutting down the scams: First thing looked at will be the email. From this the useful information is the email headers and the link to the ghost website. Examining the email headers will lead back to the network where the email was sent. But the most important thing is to find out where the website is being hosted to get it shutdown. A quick search of DNS records will reveal who is responsible for the domain. Then you have to convince them to shutdown the site, which may not be easy if they are located in another country. Depending on which country they are in, then you may have to speak the local language[1]. There are offshore hosting companies that are making a business form phishers and spammers because they will keep the ghost website even after they have been discovered[29]. To shutdown the fraudulent site requires different actions depending on the method used by the phishers. If the page is sitting on a hacked web server then only the page should be taken down, whereas if it's a similar domain name then the whole computer should be taken down.

The G8 24/7 network has recently been set up to help where computer crime crosses more than one jurisdiction (i.e. offshore). It currently has 37 members and they share evidence and cooperate in computer crime investigations[6]. An example of this cooperation was when 13 people were arrested in England from a phishing operation. Agencies from Australia, America, Canada and England were involved.

Prosecution: There have only been several prosecutions from phishing scams. In a recent prosecution scam a man in USA was sentenced to 46 months prison after defrauding $50000 from AOL and PayPal[29]. But prosecution is difficult because it can involve multi-jurisdictions. In the UK there was a scam which was spread across 5 nations, with website hosting, payment, DNS registration, server location and address all in different companies[30].

The setup of high tech crime centres, such as AHTCC in Australia, and the G8 24/7 global network should facilitate prosecution. Prosecution of criminals for mounting phishing scams from other countries will remain difficult because complex legal treaties need to be in place between countries.

Current Solutions Available - Pros and Cons

Current solutions that aid against phishing can be consumer based or network based, this sections examines some of the solutions that are available. Network based solutions concentrate at detecting and stopping the phishing attacks in real-time or near real-time, there is also a component that looks at digital signing of emails. Consumer based solutions are centred on making the customer aware of possible scams, making sure information about current phishing scams is readily available.

Both Earthlink (an ISP) and E-bay have produced browser toolbars that offer anti-phishing alerts. The Earthlink toolbar warns when a browser goes onto a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

suspected fraudulent website, while the E-bay toolbar pops out a warning when the authentic E-bay site is entered.

Digital Envoy has produced a consumer based tool that checks the origin of the email and inspects the embedded URL's for validity[1].

Tumbleweed (a secure internet messaging solutions provider) has a gateway product that digitally signs e-mail. This would sign outbound e-mail on a domain level. The recipients at the other end would see a blue ribbon or equivalent to signify a digitally signed email. The advantage of this solution would be that there is no further complication to end users.

Some companies offer services that aim at detecting in near real-time the phishing scams. Solutions include doing trademark searches, monitor DNS registrations, and monitor text on front pages to checked for ghosted websites. MessageLabs, Symantec and Solutionary offer managed mail services which scan emails looking for viruses, spam and phishing[1]. These types of services are located in the network and once in place can scan and filter suspect emails. They also act as an early warning system. MasterCard announced that it is forming a partnership NameProtect, a company that specialises in brand protection.

RSA and Vasco offer two factor authentication devices which are in use on a number of banking sites. Two factor authentication is based on "something you know" like a pin code and "something you have" like an ATM card. The user enters his pincode into the device and the device generates a one time password. The bank can also generate that same password and authenticate the user. Scandinavian banks also offer a scratch card that contains one time pins[11]. The advantage of such schemes is that stealing the password is useless.

Passmark offer a solution that adds a step in the authentication process and is targeted for e-commerce companies. It involves sending a unique image only known to the user from the website to the user thereby the user is sure he's connected to the authentic site. This solution is implemented on the website side of the network. The problem with website authentication at the moment is that the user presents his credentials to the website, but the website doesn't present any to the user although it's possible to verify via the SSL certificate. This solution goes someway towards rectifying this imbalance. Currently there is no news of any adoption of this product.

The Future

In this part the focus will be on the future direction phishing scams might take and responses to these directions on the parts of the consumer, technology, and law enforcement.

<u>Consumer</u>: With all the media attention the awareness about phishing scams consumers should become more internet savvy. Although as consumers

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

become more aware then the attacks are likely to become more sophisticated as well.

Technology: Firstly the phishers may become more opportunistic. Phishers produced a scam in June that sent out an email supposedly from Westpac asking for donations for the New Zealand Paralympics team[23]. Westpac are the legitimate sponsors and posted a link on their website for the appeal. This shows that no site will be immune to phishing scams and also raises new attack vector because the bogus website contains a blank page with JavaScript that tries to install a key logger through an old Microsoft exploit[23]. As new vulnerabilities appear then phishers will try and exploit these.

The phishers may also look at diversionary tactics to buy time, to hide their tracks, to avoid prosecution and to make the most possible of their scam. They are already doing this with emails, by regularly changing the 'from' email address so that they don't get caught in spam filters.

Another article speculated that DNS spoofing and DNS cache poisoning might be slotted into the attack[12]

In response to the possible future developments in phishing, banks may be forced into issuing two-factor authentication devices to customers despite the costs associated. HSBC in Australia has announced it is moving to two-factor authentication and issuing devices[15]. The negative thing about this type of device is that the user must have it with them to use their account. Microsoft has implemented RSA two-factor tokens in the latest XP Service Pack which means the rollout of 2 factor authentication could be simpler[32]. Finally some analysis was done on the future when and if 2 factor authentication is widespread and this report was predicting man in the middle attacks[7].

Such devices are impractical for e-commerce companies as a user would be forced to have one device for each website. More common may be solutions like that provided by Passmark mentioned above. Another concept which may hit the market in two to three years is single sign-on where a user would sign on once and be authenticated to several sites.

The other major development is going to be in stopping e-mail spoofing, the source of most phishing and spam emails, using some form of digital signing similar to the web. There are several solutions in the pipeline, what is important is that there is minimal or no consumer impact. Mentioned above Tumbleweed Communications already have a digital signing solution ready to go to market. Other approaches that are being trialled currently include Microsoft's Caller-ID, the Sender Policy Framework (SPF), and Yahoo! DomainKeys proposals[10]. The Internet engineering Task Force (IETF) have also published an IETF draft to stop source address spoofing[19].

Another area that will become more prominent is the near real-time detection of phishing scams using email scanning and filtering, trademark searches, monitoring of DNS registrations, scanning of front pages. This was also discussed in the current solutions section above.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

These solutions may take six to twelve months before these security measures can be implemented[20].

Law Enforcement: Law enforcement officials will get more organised in evidence sharing and cooperation in investigations this was apparent in the example where 13 eastern Europeans were arrested in Britain mentioned above. The more countries within the G8 24/7 network the more effective it will be in stopping phishing. This will mean that it will be easier and quicker to shutdown fraudulent websites and there will be more chance of prosecution.

In the longer term countries will setup legal treaties that will allow easier prosecution and extradition for cyber crimes where they are committed in multiple jurisdictions[8].

Strong cooperation will also be needed between private sector and the law enforcement agencies to help with investigations and prosecution like in Australia where an Anti-phishing task force has been setup.

Conclusion

Over the past 6 months phishing has made a dramatic rise all over the world and the scams are becoming more sophisticated and sneaky. People are falling for the scams and the phishers are making easy money.

Most current websites don't have enough two-factor security as yet. There are immediate short term solutions ready for rollout and there are also medium term to long term solutions involving signing emails and single sign-on solutions.

This increase in attacks affects the online confidence of consumers and attacks credibility of banks and e-commerce sites. It also removes a valuable and cheap communications tool in email. The industry is also worried about losing brand identity, with people impersonating their sites.

The good news is that consumers are more aware of the danger and more prepared to repel these attacks. This is due to dissemination of information about phishing through the media and websites.

The solution to phishing involves several fronts; the consumer, the financial institution or e-commerce sites, the technology and effective law enforcement.

The technical solutions are working towards stopping email spoofing and implementing two-factor authentication. The implementation of these solutions will most likely dramatically reduce phishing.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

1. Krebsbach, Karen. “Goin’Phishing”. 04 April 2004.
URL: http://www.onlinesecurity.com/links/links925.php (20 June 2004)

2. Leydon, John. “Phishing scams cost UK banks £1m+”. 26 April 2004. URL: http://www.theregister.co.uk/2004/04/26/phishing_scams/ (19 June 2004)

3. Kirwan , Mary. “Phishing for gold — don't take the bait”. 14 May 2004. URL: http://www.globetechnology.com/servlet/story/RTGAM.20040513.gtkirwanmay13/BNStory/Technology/ (19 June 2004)

4. Roberts, Paul. “More Scam Artists Go Phishing”. 31 May 2004 URL: http://www.pcworld.com/news/article/0,aid,116330,00.asp (19 June 2004)

5. Anti-Phishing Workgroup. Phishing Attack trends Report May 2004. May 2004. URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf (16-Jun-04)

6. Deats, Mick. “This is a stick-up!”. May 25, 2004. URL: http://www.theage.com.au/articles/2004/05/24/1085359551469.html (18 June 2004)

7. Tuliani, Jonathan. “The Future of Phishing”. 2004. URL: http://www.cryptomathic.com/pdf/The%20Future%20of%20Phishing.pdf (25 June 2004)

8. Williams, Phil. “Organized Crime and Cybercrime: Synergies, Trends, and Responses”. 2001-2002. URL: http://www.iwar.org.uk/ecoespionage/resources/transnational-crime/gj07.htm (31 May 2004).

9. Colley, Andrew. “ABA: Online bank fraud losses not a "material" concern”. 11 March 2004. URL: http://www.zdnet.com.au/news/security/0,2000061744,39116536,00.htm (17 June 2004)

10. Tumbleweed Communications. “Tumbleweed Announces Availability of Email Authentication Engine To Stop Spoofing, Spam and Phishing”. 24 March 2004. URL: http://www.tumbleweed.com/company/press_releases/2004/2004-03-24.html (17 June 2004)

11. Jesdanun, Anick. “Simple passwords no longer suffice”. 1 June 2004. URL: http://cnews.canoe.ca/CNEWS/TechNews/Internet/2004/05/28/477072.html (17 June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

12. Blass, Steve. “Phishing just the start?”. 7 June 2004. URL: http://www.nwfusion.com/columnists/2004/0607internet.html (17 June 2004)

13. Leyden, John .“UK police arrest 12 phishing mule suspects”. 5th May 2004. URL: http://www.theregister.co.uk/2004/05/05/phishing_mules_arrested/ (17 June 2004)

14. Poulsen, Kevin. “Prison time for unlucky phisher “. 21 Jan 2004. URL: http://www.securityfocus.com/news/7871 (17 June 2004)

15 Anti-Phishing Working Group. “Citibank - "Verify your E-mail with Citibank"”. 31 Mar. 2004. URL: http://www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm (16 Jun. 04)

16. Anti-phishing Workgroup. “Consumer Advice: How to Avoid Phishing Scams”. URL: http://www.antiphishing.org/consumer_recs.htm (31 May 2004).

17 Berlind, David. “Phishing: Spam that can’t be ignored” . 7 Jan 2004. URL: http://techupdate.zdnet.com/techupdate/stories/main/Phishing_Spam_that_cant_be_ignored.html (26 June 2004)

18. Colley, Andrew. “AusCERT: AFP looks to French connection to arrest phishing scam “. 7 April 2004. URL: http://www.zdnet.com.au/news/security/0,2000061744,39144081,00.htm (17 June 2004)

19. “Email Spoofing Targeted in IETF Draft on MTA Authentication Records in DNS”.2 June 2004. URL: http://xml.coverpages.org/ni2004-06-02-a.html (25 June 2004)

20. Barrett, Jennifer. “Phishing Fall-out”. 15 April 2004. URL: http://www.internetnews.com/dev-news/article.php/3362991 (17June 2004)

21. Anti-Phishing Working Group. “APWG THREAT ADVISORY ALERT” . 31 Mar. 2004. URL: http://www.antiphishing.org/news/03-31-04_Alert-FakeAddressBar.html (16 Jun. 04)

22. Bray, Paul. “How to sell - A pretty kettle of phish”. 1 June 2004. URL: http://www.computeractive.co.uk/Features/1155507 (16 Jun. 04)

23. Saarinen, Juha. “Net fraudsters target Paralympics donations”. 03 June 04. URL: http://www.computerweekly.com/articles/article.asp?liArticleID=131003&liFlavourID=1&sp=1 (16 Jun. 04)

23 Kerner, Sean, Michael. “Who's Taking the Bait? 'Phishing' Skyrockets”. 22 April 2004. URL: http://www.insideid.com/idtheft/article.php/3347341 (26 June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

24. Naraine, Ryan. "Opera Patches URL-Spoofing Flaw". 3 June 2004. URL: http://www.internetnews.com/dev-news/article.php/3362991 (16 Jun. 04)

25. Secure Science Corporation. "Banking Scam Revealed". 13 November 2003. URL: http://www.securityfocus.com/infocus/1745 (16 June 2004).

26. Anti-phishing Workgroup. "What is Phishing". URL: http://www.antiphishing.org/ (28 May 2004)

27.Willams, Daryl and Ellison, Chris. "Catching the phishers: Government/banking taskforce targets online fraudsters". 20 May 2004. URL: "http://www.iwar.org.uk/news-archive/2004/05-20.htm" (24 June 2004).

28. Bajkowski, Julian. "Banks' phishing cops get hi-tech crime schooling". 21 May 2004. URL: http://www.computerworld.idg.com.au/index.php/id;935592981;relcomp;1 l (25 June 2004)

29. Roberts, Paul. "Phishing scourge prompts calls for change". 21 May 2004. URL: http://www.thestandard.com/article.php?story=2004052105220142 (24 June 2004).

30. Warner, Matthew. "Internet crime". May 2004. URL: http://www.accaglobal.com/publications/fsr/70/1142155 (25 June 2004)

31. Robert, Paul. "MasterCard program combats phishing, black market". 22 June 2004. URL: http://www.thestandard.com/article.php?story=20040622164031501 (25 June 2004)

32. Colley, Andrew. "Banks dismissive of 'phishing' losses". 11 March 200.4. URL: http://news.zdnet.co.uk/internet/security/0,39020375,39148259,00.htm (28 June 2004)

33. Anti-Phishing Working Group. "e-gold - 'Please Verify Your Account'". 04 June 2004. URL: http://www.antiphishing.org/phishing_archive/06-04-04_e-gold_(Please_Verify_Your_Account).html (28 June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 23rd, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

Community SANS Virginia Beach SEC401*	Virginia Beach, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS