Phishing for fortune

Dr Marthie Grobler
Defence, Peace, Safety and Security
Council for Scientific and Industrial Research
Pretoria, South Africa
mgrobler1@csir.co.za

Abstract—Phishing is an attempt by a third party to solicit confidential information from an individual, group or organization. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts.

There has been an increase in attack diversity and technical sophistication by people conducting phishing and online financial fraud, making it necessary for Internet users to be aware of new trends. This article presents a holistic view of the cyber criminal attack type *phishing*. It presents a brief history of phishing, explains how phishing works, as well as variations on the attack type and real-life examples.

Keywords—Phishing, man-in-the-middle, cross-site scripting, URL obfuscation, cyber criminal, website, countermeasure

I. Introduction

Where hackers and computer criminals originally attacked computer systems in an attempt to gain fame, their focus gradually started to shift from around 2005 to pursue fortune actively. "Attackers are transitioning from simply looking to make headlines to making money" [1]. One technique to gain access to unsuspecting targets' money is by launching phishing attacks.

Phishing attacks are attempts by third parties to solicit confidential information from an individual, group or organization. These attacks are usually facilitated by mimicking specific, usually well-known brands and aims to elicit financial gain [2]. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts. This criminal mechanism employs social engineering and technical deception to steal unsuspecting targets' identity and financial account credentials. *Social engineering* involves emails professing to be from legitimate businesses, luring targets to fake websites designed to trick targets into divulging financial data. *Technical deception* involves planted crimeware designed to steal or intercept targets' online credentials and to corrupt local navigational infrastructures to misdirect consumers to fake websites [3].

Phishing attacks are similar to pharming attacks. Pharming attacks direct targets to a fake website even if they typed the correct address of the intended website into their browser. Phishing attacks also involve the creation of fake websites, but are generally associated with spam emails encouraging targets to click on links to lure them to the fake site [4]. This article presents a holistic view of the cyber criminal attack type phishing. It presents a brief history of *phishing*, explains how phishing works, as well as variations on the attack type, and real-life examples.

II. History of Phishing

The origin of the word phish is a reference to using email as a proverbial fishing hook to steal passwords. Ph is a common hacker replacement for the letter f, and reminds of the older hacking type, phone *phreaking* (the act of gaining illegal access to resources of telecom networks, usually with the intention of making free long distance phone calls) [5].

The first recorded mention of phishing is on the alt.2600 hacker newsgroup in January 1996 [1]. The term phishing was coined when thieves stole America Online accounts' passwords. After this incident, phishers regularly used email requests to solicit information from their targets. These email requests could be identified by its many spelling, punctuation and grammar errors. By 1997, phish (hacked accounts) were actively being traded between hackers as a form of electronic currency.

In 2003, phishing ploys became more sophisticated. Hackers registered look-alike domain names and created fake valid-looking websites. Phishers started to incorporate stolen logos, proper language use and webpage designs to make their ploys appear legitimate [6].

III. How does phishing work?

Phishing is an online type of fraud, generally performed by tech-savvy con artists and identity thieves. Phishing scams regularly involve spam, fake websites and crimeware to trick targets into divulging sensitive personal information [7]. This information, once captured by the phisher, is used to defraud the targets for personal monetary gain.

Phishers use various techniques to trick users into accessing their fake website. The most common technique is to send an email supposedly from a bank or other reputable institution that may require the target's financial information. The phishing attack is initiated by sending out a wave of spam email, and in some instances, mass mail by traditional postal services. Each email or letter contains a message that appears to come from a well-known and trusted organization. These emails often use legitimate logos, a good business style and spoofed (falsified with the intention to misrepresent) email headers to make it look like it came from a legitimate organization. These letters usually request customers to confirm their user information. When the recipient clicks on the link in the email, they are directed to a fake website and prompted to enter their personal information [8]. The intention of the mail is to evoke an emotional response to a false crisis by using urgent, business-like language. Since the email and corresponding website seem legitimate, up to 10% of recipients are fooled into submitting their data directly to the phishers [7].

Below is an example of a phishing spam email, taken from an actual phishing attack. This message follows the typical formula of official sounding language coupled with an ominous warning that the recipient must act quickly to keep their account active. Every link included in the message points back to the actual eBay website, with the notable exception of the fraudulent and grammatically incorrect invitation to **click here re-enter your account information**. The link for this section takes the user to the bogus sign-in page of *http://signin.ebaay-com.us/* rather than the genuine eBay sign-in page at *http://signin.ebay.com/* [7].

> Subject: Warning ! Credit/Debit card update
>
> Dear Valued Customer
>
> We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
>
> To resolve this problems please click here re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.
>
> For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.
>
> Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.
>
> Regards,
>
> Safeharbor Department eBay,Inc
>
> The eBay team.
>
> This is an automatic message. Please do not reply.
>
> Copyright © 1995-2005 eBay Inc. All Rights Reserved.
>
> Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay

After clicking on the fake link in the phishing email message, targets log into the fake eBay site using their username and password. The phishers do not have access to the legitimate website's login database, and accordingly accepts and saves any login username/password combination offered by the target (it generally does not provide the usual options of resetting a password or emailing a forgotten username or password to the user). The target is then navigated to a page to supposedly update their billing profile. This highly confidential information (ID number, credit card information, home address, driver's license number and mother's maiden name) are either mailed to the phisher, or stored on a server for future fraudulent use. Most phishing attacks last only a few days, with most of the targets responding within the first 24 hours [7].

IV. PHISHING TECHNIQUES

Traditional phishing scams are not cheap. It may cost a few thousand rand to purchase a million name target list and get the website and related scam components set-up, and a few hundred rand to handle the emailing. In addition, there is always the risk of prosecution. However, the benefits and the number of people who are vulnerable to the scams make it worth while for cyber criminals [9]. Due to intense awareness campaigns in the online financial environment, less people fall prey to traditional phishing attacks. Phishers accordingly have to resort to more specialised techniques. There are an ever-increasing number of ways to do this. The next sections explain some of the more popular techniques.

A. Phishing technique 1: Man-in-the-middle (MITM) attacks

MITM attacks places the phisher between the target and the real website, enabling the phisher to proxy, observe and record all HTTP/HTTPS communication between the systems. The target unsuspectingly connects to the phisher's server, thinking it the legitimate site that he/she intended to connect to. The phisher's server makes a concurrent connection to the real site and proxies all communications between the target and the real application server [10]. During the initial MITM attack, the phisher only collects the target's credentials. Fig. 1 shows this MITM attack structure.

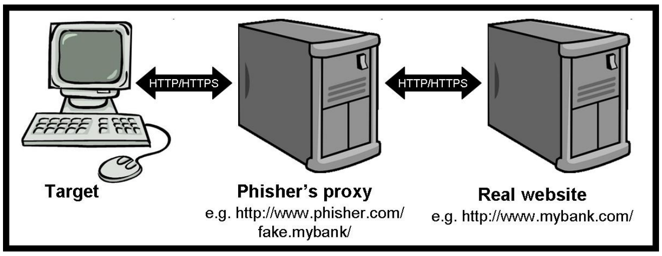


Figure 1. MITM attack structure

For a MITM attack to be successful, the phisher must direct the target to his/her own proxy server instead of the real server. This may be carried out through any of the following methods:

- URL obfuscation - disguise URLs to trick the target into connecting to the phisher's proxy server and not the real server;
- DNS cache poisoning - disrupt normal traffic routing by injecting false IP addresses for domain names;
- Transparent proxy - reroute and intercept outbound HTTP/HTTPS traffic through the phisher's proxy; no configuration changes are required at the target end; and
- Browser proxy configuration - override target's browser setup and proxy configuration options to force all web traffic through the phisher's proxy server [10].

A way to thwart MITM attacks is to encrypt all information before sending it over a network. It is also important to stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences [11].

B. Phishing technique 2: URL obfuscation attacks

Many phishing attacks are reliant on tricking an unsuspecting message recipient to follow a URL to the phisher's fraudulent server. The most common methods of URL obfuscation include [10]:

- Bad domain names - purposeful registration and use of bad domain names. For example, consider the financial institute MyBank with the registered domain mybank.com and associated customer transactional site *http://privatebanking.mybank.com*. The phisher could set up a server using any of the following names to obfuscate the real destination host: *privatebanking.**mybánk**.com*, *mybank.**private banking**.com* or *privatebanking.mybank.com.**ch***.
- Friendly login URLs - web browser implementations allow for complex URLs to include authentication information such as a login name and password. In general the format is *URL://username:password @hostname/path*. Phishers may substitute the username and password fields for details associated with the target organization. Consider the following URL, where *username = mybank.com, password = ebanking* and the *destination host = evilsite.com*. The login URL is thus effectively http://mybank.com:ebanking@evilsite.com/phishing/ fakepage.htm. This friendly login URL can successfully trick many customers into thinking that they are actually visiting the legitimate MyBank page. Because of its success, many current browser versions have dropped support for this URL encoding method.
- Third-party shortened URLs - due to the length and complexity of many URLs, third-party organizations offers free services designed to provide shorter URLs. For example, the online networking site LinkedIn provides members the opportunity to customise and shorten their profile URL. Through a combination of social engineering and deliberately shortened long or incorrect URLs, phishers may use these free services to obfuscate the true destination. Below is an example where phishers customise a long URL to obfuscate the phishing destination.

> Dear valued MyBank customer,
>
> Our automated security systems have indicated that access to your online account was temporarily blocked on Friday 13th September between the hours of 22:32 and 23:46 due to repeated login failures.
>
> Our logs indicate that your account received 2935 authentication failures during this time. It is most probable that your account was subject to malicious attack through automated brute forcing techniques (for more information visit http://support.mybank.com/ definitions/attacks.aspx? type=bruteforce).
>
> While MyBank were able to successfully block this attack, we would recommend that you ensure that your password is sufficiently complex to prevent future attacks. To log in and change your password, please click on the following URL: https://privatebanking.mybank.com/privatebanking/ebankver2/secure/customersupport.aspx?messageID=3324341&Sess=asp04&passwordvalidate=true&changepassword=true. If this URL does not work, please use the following alternative link which will redirect to the full page - http://tinyurl.com/ 4outd.
>
> Best regards,
>
> MyBank Customer Support

- Host name obfuscation - most Internet users are able to navigate to a website with a fully qualified domain name, such as www.google.com. Behind the scenes, the web browser needs to translate this domain name to an IP address, such as 216.239.59.104, through domain name server (DNS) functioning. By navigating to a website using an IP address, it is possible to obfuscate the destination address, and bypass content filtering systems. For example the following URL: *http://mybank.com: ebanking@ evilsite.com/phishing/fakepage.htm* could be entered as: *http://mybank.com:ebanking@210.134.161.35/ login.htm.*

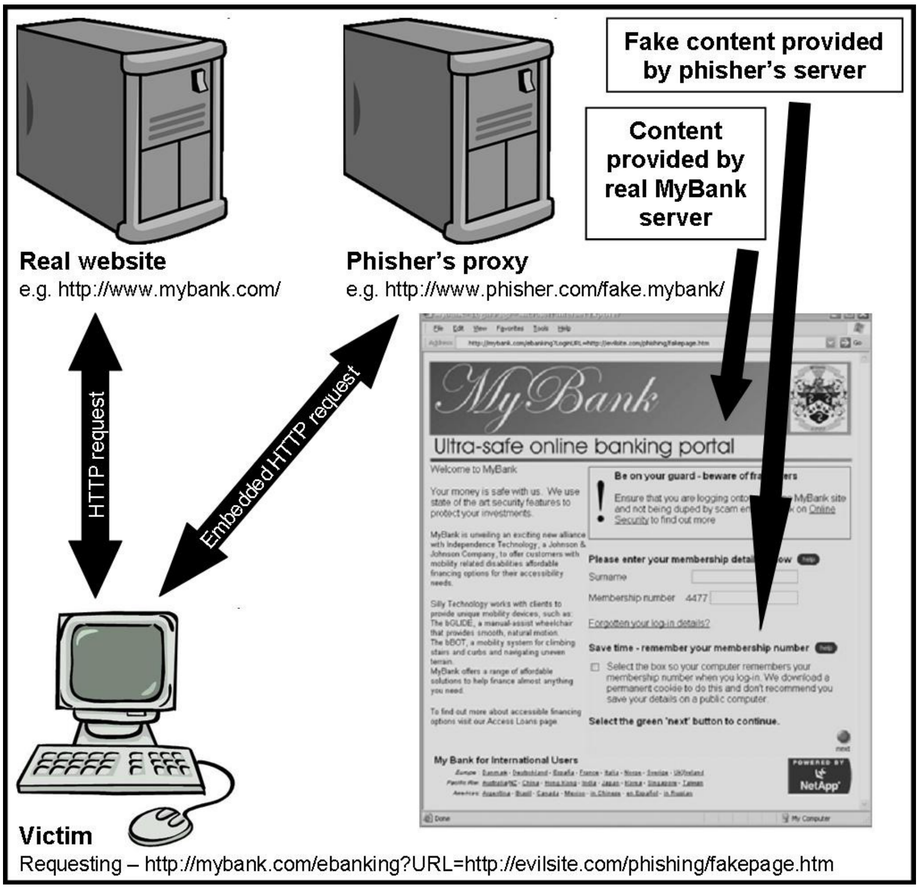
Some techniques to counter URL obfuscation attacks include two-factor authentication and one-time passwords when conducting online commerce or banking, and specially designed web browser toolbars. These toolbars are unfortunately only effectively in identifying phishing sites that have been previously observed and reported.

C. *Phishing technique 3: Cross-site scripting attacks*

Cross-site scripting attacks make use of customised URL or code injections into a valid web application or imbedded data field. Three URL formatted attacks are common:

- Full HTML substitution - http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
- Inline embedding of scripting content - http://mybank.com/ebanking?page=1&client=<SCRIPT>evilcode
- Forcing the page to load external scripting code – http://mybank.com/ebanking?page=1&response=evilsite.com%21evilcode.js&go=2

Fig. 2 illustrates a full HTML substitution. The customer has received the following URL via a phishers' email: http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm. Although the customer is directed and connected to the real MyBank web application, the ebanking component accepts an arbitrary URL insertion.



Fake content provided by phisher's server
Content provided by real MyBank server
Real website
e.g. http://www.mybank.com/
Phisher's proxy
e.g. http://www.phisher.com/fake.mybank/
HTTP request
Embedded HTTP request
Victim
Requesting – http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
File Edit View Favorites Tools Help
Address
MyBank
Ultra-safe online banking portal
help
next
POWERED BY NetApp
Done
My Computer

Welcome to MyBank

Your money is safe with us. We use state of the art security features to protect your investments.

MyBank is unveiling an exciting new alliance with Independence Technology, a Johnson & Johnson Company, to offer customers with mobility related disabilities affordable financing options for their accessibility needs.

Silly Technology works with clients to provide unique mobility devices, such as: The bGLIDE, a manual-assist wheelchair that provides smooth, natural motion. The bBOT, a mobility system for climbing stairs and curbs and navigating uneven terrain. MyBank offers a range of affordable solutions to help finance almost anything you need.

To find out more about accessible financing options visit our Access Loans page

Be on your guard - beware of fra[illegible]ers

Ensure that you are logging onto [illegible] MyBank site and not being duped by scam e[illegible] k on Online Security to find out more

Please enter your membership detai[illegible]ow

Surname

Membership number 4477

Forgotten your log-in details?

Save time - remember your membership number

□ Select the box so your computer remembers your membership number when you log-in. We download a permanent cookie to do this and don't recommend you save your details on a public computer.

Select the green 'next' button to continue.

My Bank for International Users

Figure 2. Cross-site scripting attacks

Accordingly, the application does not provide the legitimate MyBank authentication form embedded within the page, but references the phisher's authentication form on an external server (http://evilsite.com/phishing/fakepage.htm). The customer has no way of knowing that the authentication page is not legitimate [10].

Cross-site scripting attacks are difficult to counter. The best way is to be vigilant whenever busy on the Internet. In addition, the same countermeasure than for URL obfuscation attacks apply.

D. *Phishing technique 4: Capturing customer data*

Phishers can use key loggers and screen grabbers to capture and observe confidential customer data as it is entered into a web application.

- Key loggers – hardware devices or small software applications that capture all key presses by the target, used in particular when entering authentication information into web application login pages. With these credentials, the phisher can misuse the target's account for their own purposes at a later time.
- Screen grabbers - sophisticated applications designed to take a screen shot of data entered into a web application. This application bypasses some of the more secure financial applications with features build-in to prevent against standard key logging attacks. Generally, only the relevant observational area is required (i.e. a small section of the web page instead of the entire screen) and the phisher's software will only record this data, keeping the upload data capture small and quick to transfer to their server [10].

Software key loggers and screen grabbers can be distributed through malware and Trojans, or located in the operating system kernel or grabber-based web form submissions. Hardware devices can be attached to computers only when the cyber criminals have physical access to the computer, and the computer user is either not present or not paying attention.

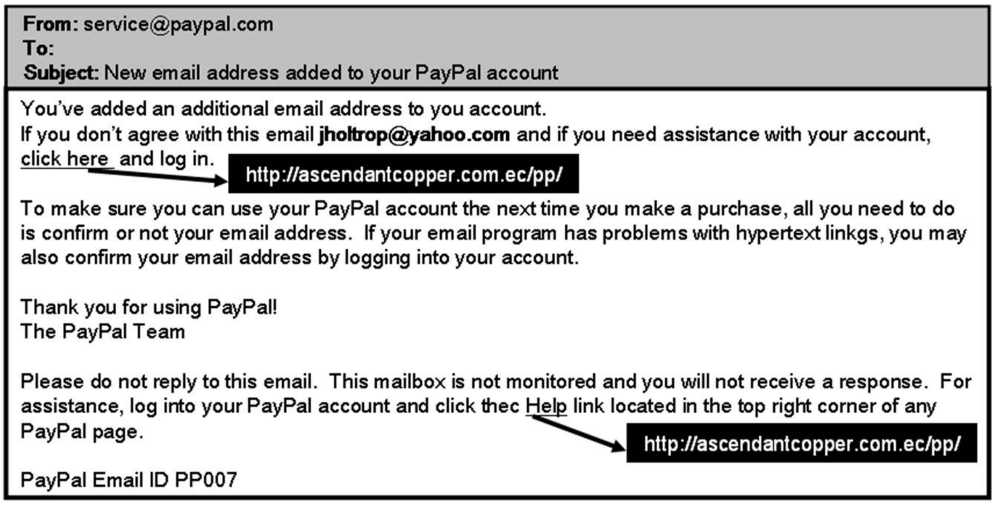
Countermeasures for phishers capturing user data include up-to-date anti-spyware and firewalls, regularly checking for unknown hardware devices attached to the computer, one-time passwords for online commerce and banking, and using on-screen keyboards rather than physical keyboards. Drastic measures include an alternative keyboard layout, customised with products such as the Microsoft Keyboard Layout Creator – this technique will not prevent the capturing of data, but the data will be unintelligible.

V. EXAMPLES OF PHISHING ATTACKS

Phishing is not restricted to email alone. Phishers also use exploited websites, instant messaging, peer-to-peer networks and search engines to direct targets to fraudulent websites that may contain malicious code.

Attacks also target businesses, sending phishes to employees who may click on links or respond to messages, assuming that their IT departments are protecting them from such unsafe activities. "A … study [of] 1,200 users, 400 each in the U.S., Germany, and Japan, [reported that] 39 percent of enterprise workers believe that their company's IT department would keep them safe from viruses, worms, spyware, spam, and phishing and pharming attacks. That confidence, whether on the mark or misplaced, leads workers to do risky, even stupid, things at work, such as opening questionable e-mail messages or clicking on unknown Web site links." [6]. Examples and variations of the traditional phishing scams:

- eBay's widespread popularity and universal appeal has made it one of the most phished brands on the Internet. Hackers set up a fake eBay website on the server, with a login page convincingly similar to the genuine eBay version. The fake eBay website was taken down before any targets visited the site and fell prey to the scam [7].
- Phishers can also exploit inherent website design flaws to make their attacks more convincing. For example, a flaw in the IRS (Internal Revenue Service) website allowed phishers to spoof their phishing email's originating URL to be the IRS' website [7].
- Targeted email phishing is called spear phishing - phishers send spoofed emails to employees within a specific organization, appearing to be come from a colleague. Spear phishing attacks are very difficult to spot and the success rate is known to be high. A separate tactic, called whaling, involves targeted attacks on senior executives and other high-ranking people within an organization [12].
- China's cyber threat response group has warned local Skype users about phishing scams being carried out through the chat feature. Many Skype users in China have recently received fake messages saying they had won a prize, directing them to a fake look-alike version of Skype's website to claim it. Skype is an ideal phishing target since many user accounts have payment information linked to them [13].
- PayPal is the most targeted for phishing attacks in 2009. Fig. 3 and Fig. 4 shows variations of a PayPal phishing attack. Fig. 3 shows a poorly constructed attack, featuring no logo and no user specific details.



From: service@paypal.com
To:
Subject: New email address added to your PayPal account

You've added an additional email address to you account.
If you don't agree with this email **jholtrop@yahoo.com** and if you need assistance with your account, click here and log in.

http://ascendantcopper.com.ec/pp/

To make sure you can use your PayPal account the next time you make a purchase, all you need to do is confirm or not your email address. If your email program has problems with hypertext linkgs, you may also confirm your email address by logging into your account.

Thank you for using PayPal!
The PayPal Team

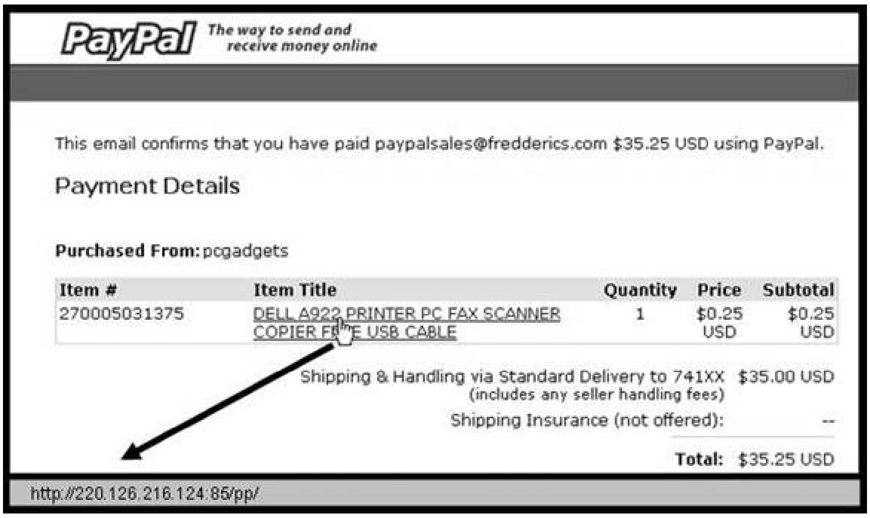
Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log into your PayPal account and click thec Help link located in the top right corner of any PayPal page.

http://ascendantcopper.com.ec/pp/

PayPal Email ID PP007

Figure 3. PayPal phishing email example #1

- Fig. 4 informs the potential target of a payment made by them. Though the email is nicely formatted and looks quite like a legitimate PayPal email, there are no specific details identifying the recipient. The URL points to an IP address and not to the PayPal website.



PayPal The way to send and receive money online

This email confirms that you have paid paypalsales@fredderics.com $35.25 USD using PayPal.

Payment Details

Purchased From: pcgadgets

Item #	Item Title	Quantity	Price	Subtotal
270005031375	DELL A922 PRINTER PC FAX SCANNER COPIER FREE USB CABLE	1	$0.25 USD	$0.25 USD

Shipping & Handling via Standard Delivery to 741XX (includes any seller handling fees) $35.00 USD

Shipping Insurance (not offered): --

Total: $35.25 USD

http://220.126.216.124:85/pp/

Figure 4. PayPal phishing email example #2

- Phishing pop-ups are fake requests for personal information, normally used in browsers that enable tabs and pop-up windows. The user has a number of different websites open in different tabs or windows. A pop-up box opens, supposedly originating from one of the legitimate websites open in a tab or window. This pop-up asks the target to enter their password and credit card information, "for verification purposes" [14]. If the target complies, he/she are not only a target of phishing, but also of social engineering.
- After 2005, phishers started to use crimeware in conjunction with their fake websites by exploiting common browser vulnerabilities to infect target machines. This crimeware enables phishers to steal a target's identity, without having the target physically entering personal information – the Trojan or spyware placed onto the machine would capture this information the next time a legitimate website is visited [7].
- Receiving a letter from a national bank card carrier stating that your existing card has been compromised, including a new card. The recipient has to phone a 0860 number to activate the replacement. Activation requires knowledge of the old card number, expiry date and the four-digit check code - everything a phisher needs to empty the account [9].

VI. PHISHING TRENDS

Reports issued by international IT security service and technology vendors confirm a marked increase in specific security risks such as phishing. Up to 50% of all spam and phishing attacks are initiated by people [15]. The APWG's (Anti-Phishing Working Group) most recent data reported that the number of unique phishing-oriented websites had surged to nearly 50,000 in June, the largest number since April 2007 and the second-highest total since it started keeping records [16].

According to the X-Force report, however, there is a slight phishing decrease in the first half of 2009 due to the shift away from financial targets. During 2008, phishing volume was on average 0.5% of the overall spam volume. In the first half of 2009, this figure decreased dramatically to only 0.1% [17]. Fig. 5 shows the countries with the most phishing URLs.

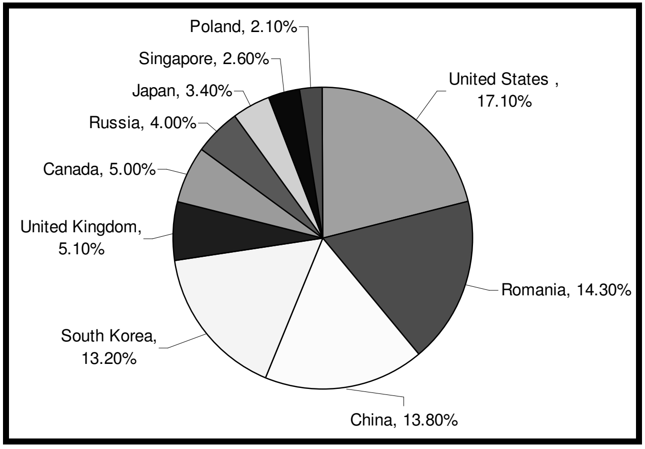


Figure 5. Top 10 countries with the most phishing URLs in 2009 [17]

Although it is accepted that phishing attacks are decreasing due to an upsurge in Trojan attacks [18], the APWG reported that the number of unique phishing websites detected in June 2009 rose to 49,084, the second-highest number recorded since APWG began reporting this measurement [19].

Fig. 6 shows the percentage and distribution of phishing attacks around the world, for 2009 [19]. The main areas of attacks are North America, Canada and China. Africa is largely excluded from these statistics due to the current slow Internet access. This, however, may change soon when the broadband access project for Africa is completed.

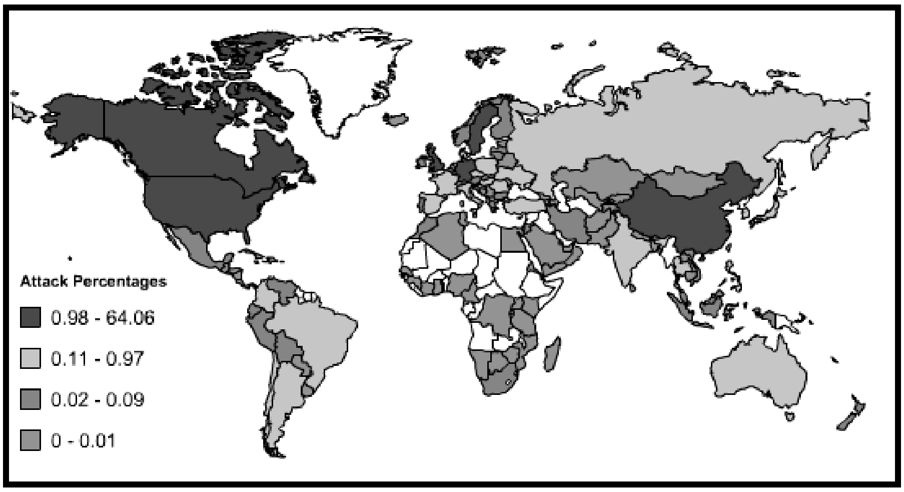


Figure 6. Global phishing attack distribution for 2009

Symantec observed 25% of phishing URLs to be generated using phishing toolkits [20]. Typosquatting, also referred to as URL high jacking, relies on targets making typographical or spelling errors when entering a website address. An example of typosquatting is the US White House site (whitehouse.gov), parodied at whitehouse.org (a pornographic magazine). Typosquatting constitutes 1% of all phishing sites.

Free web hosting is the easiest and most cost effective way to create phishing URLs. This type of attack requires relative levels of technical acuity, but the cost involved is a lot less. Free web hosting accounts for 9% of all phishing sites.

Using IP address domains, instead of domain name addresses (host name obfuscating) accounts for 7% of all phishing sites. The remainder of the phishing sites (58%) is unique domains paid for by the phishers. Phishing toolkits continued to professionalize fraud attacks. Fig. 7 shows the categorisation of phishing sites in 2009.

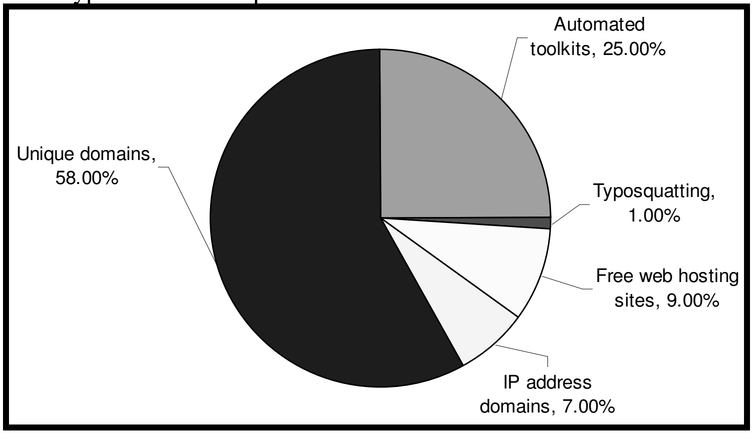


Figure 7. Phishing site categories in 2009 [20]

VII. Precaution against phishing attacks

Phishing attacks do not only hold the potential for harsh monetary losses to the target, but also possible identity theft. All Internet users need to be aware of current trends and techniques employed by phishers. Below are a couple of guidelines on how to protect you from a phishing attack:

- Be wary of any email messages asking for personal information. It is highly unlikely that a bank will request such information by email. If in doubt, call them to check.
- Do not complete a form in an email message asking for personal information. Only enter such information

using a secure website. Check that the URL starts with https://, rather than http://. Look for the lock symbol on the lower right-hand corner of the web browser and double-click it to check the validity of the digital certificate (resourceful cyber criminals have been able to replace the legitimate digital certificate lock symbol with a useless lock icon).

- Report anything suspicious to your bank immediately. Do not use links in an email message to load a web page. Instead, type the URL into your web browser.
- Visit your anti-virus' website to check if the anti-virus program blocks phishing sites, or consider installing a web browser toolbar that alerts you to known phishing attacks.
- Check your bank accounts regularly (including debit and credit cards, bank statements, etc.), to make sure that listed transactions are legitimate.
- Make sure that you use the latest version of your web browser and that any security patches have been applied [8].

Although cyber criminals will always find new ways to trick people into giving of their personal credentials, computer users can be aware of current trends and protect themselves accordingly.

VIII. CONCLUSION

Certain cyber crimes, especially phishing and spoofing related to financial and identity fraud, do not generally depend on a lack of technical protection, but rather lack of awareness by targets. Phishing attacks are very effective because they are a form of social engineering. Social engineering takes advantage of the interface between people and technology. People often trust information they receive via e-mail or from a website, and will unfortunately react on this.

REFERENCES

[1] ZIZZO, T. 2006. *Vendors, VARs try to stay one step ahead of cyber-criminals* [online]. URL: http://www.crn.com/security/181501701; jsessionid=TJWSNUCKPIKSFQE1GHPSKH4ATMY32JVN (Accessed 18 December 2009).

[2] BLACKBIRD, J. 2008. *ISTR XIII: Phishing and spam trends* [online]. URL: http://www.symantec.com/connect/blogs/istr-xiii-phishing-and-spam-trends/ (Accessed 10 December 2009).

[3] MANNING, R. 2009. *Phishing activity trends report - 1st half 2009* [online]. URL: http://www.antiphishing.org/reports/apwg_ report_ h1_ 2009.pdf (Accessed 14 December 2009).

[4] KIRK, J. 2007. *'Pharming' attack hits 50 banks* [online]. URL: http://news.techworld.com/security/ 8102/pharming-attack-hits-50-banks/ (Accessed 10 December 2009).

[5] GLOBAL ONENESS. ND. *Phishing - History of phishing* [online]. URL: http://www.experiencefestival.com/a/Phishing_-_History_of_phishing/id/1845385 (Accessed 18 December 2009).

[6] WEBSENSE. 2005. *Phishing and pharming*. California: WebSense.

[7] NORTON. 2009. *Online fraud: phishing* [online]. URL: http://www.symantec.com/norton/cybercrime/phishing.jsp (Accessed 14 December 2009).

[8] KASPERSKY LAB. 2009. *Phishing* [online]. URL: http://www.kaspersky.com/phishing (Accessed 14 December 2009).

[9] MURPHY, P. 2008. *Using mail for phishing* [online]. URL: http://blogs. zdnet.com/Murphy/?p=1131 (Accessed 14 December 2009).

[10] OLLMAN, G. 2004. *The phishing guide - Understanding & preventing phishing attacks.* URL: http://www.ngssoftware. com/papers/NISR-WP-Phishing.pdf (Accessed 17 December 2009).

[11] MSDN. 2006. *Chapter 2- Threats and countermeasures* [online]. URL: http://msdn.microsoft.com/en-us/library/aa302418.aspx (Accessed 23 December 2009).

[12] NARAINE, R. 2009. *Emerging threats: The changing face of email.* Kaspersky Lab Americas.

[13] FLETCHER, O. 2009. *China warns of Skype phishing attack* [online]. URL: http://news.techworld.com/security/3208353/china-warns-of-skype-phishing-attack/?cmpid=TD1N18 (Accessed 14 December 2009).

[14] CONSUMER FRAUD REPORTING. 2008. *Phishing popup - Fake requests for personal financial information* [online]. URL: http://www.consumerfraudreporting.org/phishingpopups.php (Accessed 17 December 2009).

[15] CARRICK. 2009. *Attackers continue to phish for trouble and dish out spam* [online]. URL: http://www.carrick.co.za/ca/viewnews. aspx?id=59 (Accessed 14 December 2009).

[16] KEIZER, G. 2009. *Google admits Gmail login details were leaked online* [online]. URL: http://news.techworld.com/security/3203481/ google-admits- gmail-login-details-were-leaked-online/ (Accessed 10 December 2009).

[17] SUPPIAH, S. 2009. *The Internet is the new Wild West reports IBM consultant* [online]. URL: http://news.techworld.com/security/ 3201556/the-internet-is-the-new-wild-west-reports-ibm-consultant/ (Accessed 10 December 2009).

[18] MESSMER, E. 2009. *Phishing attacks down in 2009* [online]. URL: http://news.techworld.com/security/3200461/phishing-attacks-down-in-2009/ (Accessed 10 December 2009).

[19] APWG. 2009. *The Internet has never been more dangerous* [online]. URL: http://www.antiphishing.org/ (Accessed 14 December 2009).

[20] NAMBIAR, S., SAINKAR, S., COWINGS, D. & WEE, Y. 2009. *The state of phishing: A monthly report – May 2009.* URL: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_ report_05-2009.en-us.pdf (Accessed 17 December 2009).