# Guarding against Web Spoofing and Phishing Attacks

Doina Bein, Wolfgang W. Bein, Vasu Jolly, and Shahram Latifi

*Abstract* — **Browsing the Internet securely has been a pressing issue for years. "Phishing" – also referred to as "web spoofing" – is a set of techniques to mislead unsuspecting users. Phishers set up fraudulent websites to gain access to important data such as pass codes for bank or credit card accounts, or other private information that will help identify users. Such users are lead to believe that they are communicating with trusted websites while instead they are communicating with completely different websites - websites set up for malicious purposes, often referred to by an initial direct email. Usurping trusted brands of renowned banks, online vendors and credit card companies, phishers are successfully enticing recipients to react to them. We address the level of phishing and efforts to curtail it.**

*Keywords* — **phishing, web spoofing.**

## I. Introduction

TO most "Information is power" but to some imposters, the Internet is just another opportunity for fraud. It used to be the case that crooks would just be satisfied to obtain email addresses through free offers and the like to then only bury their prey under tons of junk mail. But the crooks are becoming more daring. Investing a bit more effort they now set up polished yet also bogus websites where users risk leaving critical data such as social security number, date of birth, passwords, credit card numbers and the like.

The term phishing comes from Biology and describes the technique used by birds to attract mates by making a group of sibilant noises (see [1,2]). This term has been carried over to Information Technology to describe a new technique used by never tired malicious scammers. It is also sometimes called "web spoofing". Of course, the term phishing is used because the technique is a bit similar to what goes on in Biology: Attract unsuspecting users to bogus websites in order to gain personal data such as pass codes for bank or credit card accounts, or other private information that will help identify users. The prime method used with phishing involves luring users into believing that they are communicating with trusted websites, while instead they are communicating with completely different websites - websites set up for malicious purposes. The initial contact could come from an email to users referring to the malicious site, through pop-up messages.

By 1996, the prey, i.e. hacked accounts were called "phish", and shortly thereafter phish were actually being traded among hackers as a form of currency. People would routinely trade ten working Americal Online phish for one piece of hacking software. Over the years, phishing attacks grew from simply stealing AOL dialup accounts to a more proficient and sinister criminal enterprise. Phishing attacks now targeted users of online banking, payment services (such as PayPal) and generally all sorts of online e-commerce sites. To this day, phishing attacks are growing quickly in number and also sophistication. In fact, since 2003, most major banks in the USA, the UK and Australia have been hit with such phishing attacks [3].

## II. Examples of Web Spoofing

A small letter substitution, especially when the URL of a website is a long string, can be quite deceptive. For example, assume that a user, either by mistake or by following a link received in an email, accesses the following website:

www.wel1sfargo.com/checking/paybills-online/onlineid.php.

Given that this page has the familiar look and feel of the Wells Fargo Bank that the URL seems alright, the user may assume that indeed a trusted page for online banking has been loaded. In reality Wells Fargo's link has only a slightly different syntax, its true URL is:

www.wellsfargo.com/checking/paybills-online/onlineid.php

The user may furnish a password, which now ends up in criminal hands. Often pass codes involve social security numbers; this clearly opens up opportunities for identity theft. For extra measure, to keep the user lulled into complacency, a "sorry-page" (website down temporarily down for maintenance, too many users connected, etc) is displayed.

Having received an email appearing to originate from a popular commercial site, warning perhaps about a security breach or some account problem, this may be enough to entice a visit to that website and to log in. (Figure 1 shows such an email.)

Doina Bein is a Ph. D. student in the School of Computer Science, University of Nevada Las Vegas, USA (phone: 702-895 1634; Fax: 702-895 5222; Email: siona@cs.unlv.edu).

Wolfgang W. Bein is an Associate Professor in the School of Computer Science, University of Nevada Las Vegas, USA (Phone: 702-895 1477; fax: 702-895 5222; Email: bein@cs.unlv.edu).

Vasu Jolly is a Ph. D. student in the Department of Electrical and Computer Engineering, University of Nevada Las Vegas (email:jolly@egr.unlv.edu).

Shahram Latifi is a Professor in the Department of Electrical and Computer Engineering, University of Nevada Las Vegas, USA (Phone: 702-895 4016; Fax: 702 895 0488; Email: latifi@egr.unlv.edu).

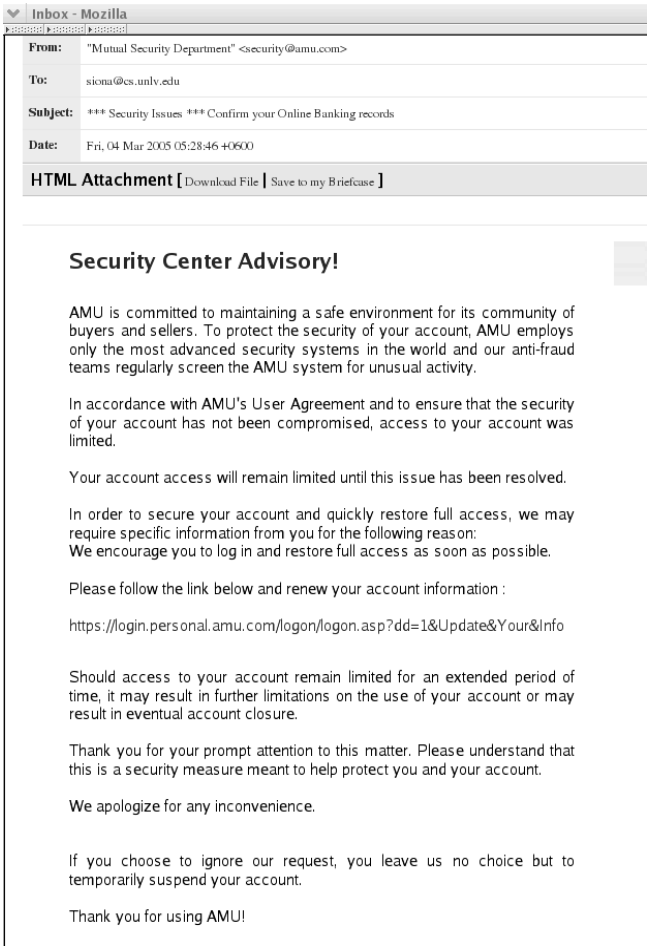


Figure 1. Sample of an email inviting to visit a spoofed website

Instead, the link in the email sends the user to a bogus malicious site, which collects whatever user information can be obtained.

Another "spoof" exploits flaws in how the browsers interpret Unicode, the broad character set used in Internationalized Domain Names (IDN) allowing URLs to include non-English characters. Unicode can be used to craft "homographic" strings, in which two different combinations of characters represented as an HTML link can display in the browser the same URL, but send users to different sites. The spoofing flaw was demonstrated by the Shmoo Group, which used a Unicode link to display www.paypal.com in the address bar of affected browsers, but sent users to www.xn--pypal-4ve.com - which then displayed "www.paypal.com" in its address bar. A similar spoof has worked on SSL-enabled URLs (https) commonly used on banking and e-commerce sites.

Another common technique related to phishing is "pharming". Pharming uses malware/spyware to redirect users from real websites to the fraudulent sites typically by DNS hijacking.

Addressing and solving such an issue is not easy, because there are several technologies and groups involved: browser(s), Internet Service Providers, mail client vendors, website owners, domain registrars, and certificate authorities.

The Anti-Phishing Working Group (APWG) [3] is the global association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. The latest report available at the site of the APWG [3] shows a steady increase in spoofed websites (see Figure 2, which is taken from [3]).

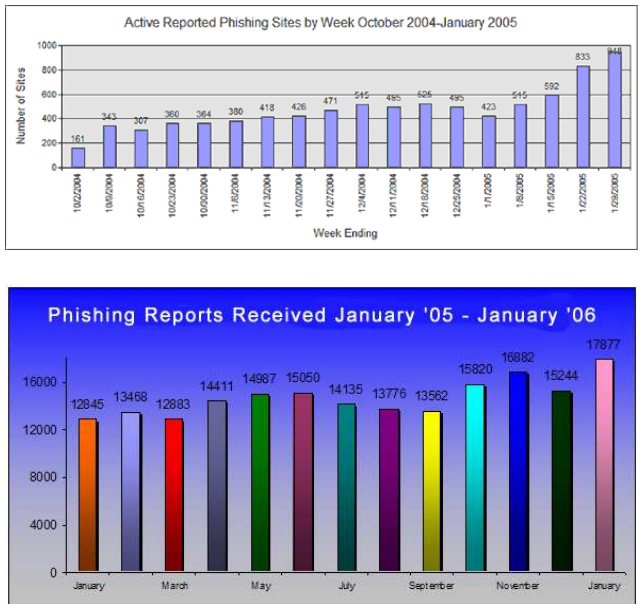


Figure 2. Active phishing sites between October 2004-January 2006. (Figures taken from [3])

A list of the sample phishing attacks follows bellow:

- 01-03-05 - e-Bullion- 'e-Bullion accounts investigations' www.antiphishing.org/phishing_archive/03-01-05_E-bullion/03-01-05_E-bullion.html
- 24-02-05 - Washington Mutual Bank- 'Unauthorized Access To Your Washington Mutual Account' www.antiphishing.org/phishing_archive/02-24-05_Wamu/02-24-05_Wamu.html
- 22-02-05 - SouthTrust Bank- 'Notification From Southtrust Online Banking' www.antiphishing.org/phishing_archive/02-22-05_SouthTrust/02-22- 5_SouthTrust.html
- 18-02-05 - Huntington Bank- 'Huntington Bank Security Update Notification' www.antiphishing.org/phishing_archive/02-18-05_Huntington/02-18-5_Huntington.html
- 17-02-05 - Paypal - 'Unauthorized Access...' www.antiphishing.org/phishing_archive/02-17-05_Paypal/02-17-05_Paypal.html
- 15-02-05 - MSN - 'Microsoft Network customer data verification' www.antiphishing.org/phishing_archive/02-15-05_MSN/02-15-05_MSN.html
- 08-02-05 - KeyBank - 'Secure Your Account Now' www.antiphishing.org/phishing_archive/02-08-05_Key/02-01-05_Key.html

## III. PROTECTION: IS THERE A PANACEA?

In [4,5], Gervase Markham, member of the Mozilla project, gives a number of interesting solution approaches for the problems discussed here. Specifically, in [5]

Markham explains why the secure socket layer (SSL) is essential for any protection from phishers, and why anything else that does not use SSL has to necessarily be a a patch, i.e. something that does not solve the core problem.

The browser is generally under the control of the user, so one can set up proper parameters in order to obtain better background about the visited or to be visited websites. During visits to an SSL site, it is important that its identification and security status be known. The Open Source Mozilla-Firefox browser displays the site domain name in the bottom right corner and makes the status bar permanent, see Figure 3. Indeed, Open Source Standards play an important role in fostering secure Information Technology environments.


Figure 3. SSL website displayed using Firefox

In addition, keeping a list of the domains accessed using SSL is certainly advised; Firefox addresses this issue by displaying a descriptive message whenever a new site is dialed up (see Figure 4).

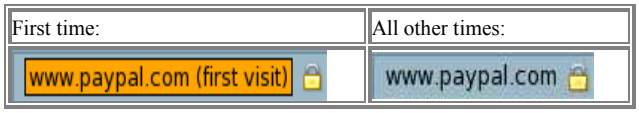


Figure 4.Visiting a SSL domain using Firefox for the first time (Figure taken from [4])

The browser's history cache also plays a role in this context. History is kept for a limited time only and many users to not like to keep a history log, especially when they are accessing the Internet from their workplace, or a public desktop. A partial but not complete solution to the privacy is to keep not the name of the website, but some encoding of the name (name-hashing). In that way, depending on the hash function, if the website was never visited before, there is a computable probability that the hash value obtained from the website's name to not be within the cache, and the browser give a warning to the user. There could be false negatives, if the hash value of a bogus website matches some existing hash value from a different visited website. So the quality of the hash function decides the accuracy of guesses.

Upcoming releases of the Mozilla Firefox browser have, by default, the support for "IDN turned off" to help protect users from spoofing and indeed current versions of Mozilla-Firefox, Opera and the Safari browser for Macintosh, have this parameter set by default. Thus settings should be set to option 'network.enableIDN' to false in the browser's configuration (One would enter about:config in the address bar to access the configuration functions). Users who demand IDN support are thus still empowered to turn it on, but will be warned about the risks involved.

A project initiated at Stanford University attempts to prevent phishing. SpoofGuard [6,7] is a browser plug-in compatible with Microsoft Internet Explorer. The user sets parameters that evaluate the probability of a site to be a spoofed site. A traffic light placed in the browser toolbar varies its color from green to yellow to red as one navigates across different sites (see Figure 5).

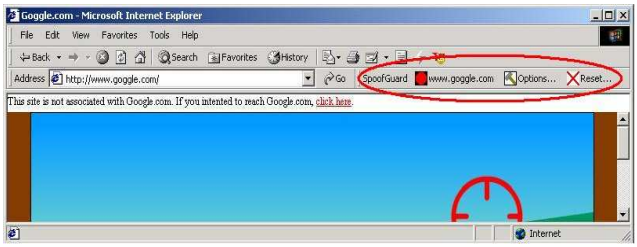


Figure 5. SpoofGuard attached to IE browser (taken from http://crypto.stanford.edu/SpoofGuard/#description)

If you try to enter sensitive information into a form of some site that based on the indicators you have set is perceived as spoofed, SpoofGuard will save your data and warn you (see Figure 6).

EarthLink's ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phishing Web sites. It can be downloaded for free at http://www.earthlink.net/earthlinktoolbar.

In case none of the available anti-phishing tools are installed on a system, minimally the browser should have all current security patches applied. (Go to http://www.microsoft.com/security; there is also a special patch relating to certain phishing schemes.)

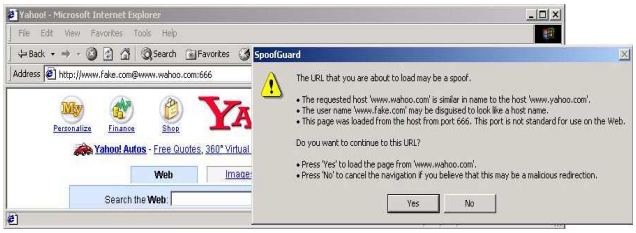


Figure 6. Warning regarding spoofed site (Figure taken from http://crypto.stanford.edu/SpoofGuard/#description)

Also one should use great care around email and be aware that any email with "urgent" requests for personal

financial information can indeed be a phising attack. Unless the email is digitally signed, one certainly cannot be sure it was not forged or “spoofed”. An S/MIME digital signature allows an email recipient to verify that the "from:- address” in a message has not been 'spoofed'.

It is also advised to not fill in forms regarding personal records in email. Legitimate companies would not request such information trough email. High-value information such as credit card numbers or account information must only be communicated via a secure website (the website address must start with "https://").

In case there is suspicion that one may have become a victim of phishing, one should assume the worst (i.e. credit card fraud, bank fraud, or identity theft). Based on the kind of information that has been compromised to the suspected website, [3] provides a list of suggested courses of action. They consider the following categories:

- credit or debit or ATM card information, bank account information, eBay account information.
- virus or Trojan that has captured information off of your computer.
- personal identification information (e.g. SSN, Driver License Number, etc.)

## IV. CONCLUSION

Phishing damages brands, the reputation of financial institutions, and, worse, exposes consumers to potential fraud. To deal with the wide variety of Internet identity theft schemes, increased data sharing between financial institutions, Internet Service Providers and law enforcement agencies should is mandatory. Current legislation is under way to combat phishing. The Anti-Phishing Act of 2005 introduced Senator Patrick Leahy [8] `Anti-phishing Act of 2005' targets the scams. Meanwhile, users have to vigilant to use technical means available to protect themselves as best possible.

## V. REFERENCES


[1] K. Zimmer, The western bird watcher: An introduction to birding in the American West, Prentice Hall, 1991.

[2] Linda Therese Caissie, Gone pishing: The social world of birding by older adults, The University of New Brunswick, Dissertation, 2001.

[3] Anti-Phishing Working Group, http://www.antiphishing.org/.

[4] Gervase Markham, A plan for scams, http://www.gerv.net/security/a-plan-for-scams/.

[5] Gervase Markham, Phishing - Browser-based defences, http://www.gerv.net/security/phishing-browser-defences.html,2005.

[6] Dan Boneh, Jonh Mitchell, Robert Ledesma, Neil Chou, Yuka, Teraguchi, Client-side defense against web-based identity theft, 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, February, 2004.

[7] Dan Boneh, Jonh Mitchell, Robert Ledesma, Neil Chou, Yuka Teraguchi, SpoofGuard Project, Stanford University, http://crypto.stanford.edu/SpoofGuard/.

[8] `Anti-phishing Act of 2005'. Available at http://thomas.loc.gov.