SECURITY NEWSLETTER

Security Newsletter No. 2

October 2004

Welcome to our new Monthly Security Newsletter. Last month in our first issue we discussed basic security techniques and specific ways in which you could increase Internet Explorer and Email security, plus some tips to help reduce Spam. This month, I'd like to focus on a fairly recent security risk that has been on the rise called Phishing.

Phishing Defined

Phishing is a type of deception designed to steal your identity or financial information – the term is derived from fishing. In a phishing scam, the malicious person doing the phishing tries to get information like credit card data, passwords, account information, or other personal information from you by convincing you to provide them this information under false pretenses. Often these come through email or a popup window while you are browsing and they may appear to be from valid entities. The more convincing the phisher is, the more likely they are to scam you into providing sensitive information.

How does phishing work?

The most common phishing scam works by the malicious user sending out many bogus emails that appear to come from web sites that you use or trust, like your ISP, bank, credit card company, etc. The emails often include embedded web pages and links, complete with official-looking graphics that look identical to the vendor's web site or normal email. Believing that the email is valid, the unsuspecting user will provide information that is requested or click on a link to "update" their account.

To make these emails look real, a scam artist might put a link in the email that appears to go to the legitimate web site, but actually takes you to a scam web site. Often they use web addresses that look to be valid at first glance – for example, http://earthlink.security.com might appear to be an official Earthlink site, but it is not – the upper-level domain is "security.com" and might be mistaken by the average user as a site having something to do with Earthlink. Something else that is common is to embed an official-looking web page complete with actual vendor graphics within the email with data fields you must fill out and send back to the scammer. The scammer can then use your personal data to purchase goods, apply for a new credit card, or steal your identity. The moral of the story is, just because it may look legitimate doesn't mean that it is!

The graphics to the left were taken right from Citibank's website. Looks official, don't they?

Ways to protect yourself from phishing

In the year 2004, phishing schemes have increased 40% over 2003 stats. One thing is guaranteed, the online scam artists will continue to develop new and innovative ways to trick their victims. By following these simple steps you will help protect you and your information.

- **Never** respond to requests for personal information via email. If there are ANY questions, pick up the phone and call the institution that claims to have sent the email.
- Only visit web sites by TYPING in the address in your Internet Browser's address bar – never click on a link included in the email itself.
- Check that the web site is using encryption
- Review your credit card and bank statements regularly
- Report suspected fraud to the proper authorities
- Keep your computer's security measures up-to-date

STEP 1: Never respond to requests for personal information via email

Most legitimate businesses will NOT ask for passwords, credit card numbers, or other information of this type in an email. If you do receive email of this type, never respond; contact the company by phone to confirm this information. If you are asked to "click here" to visit the company web site, see step 2 below.

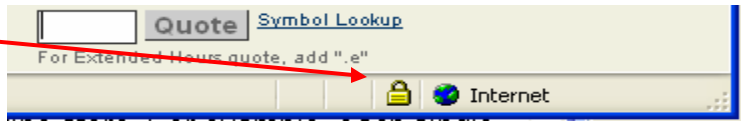
STEP 2: Visit web sites by typing the URL into your address bar

Links in emails can look legitimate but are often not – taking you to a bogus web site where sensitive information is gathered for the phisher rather than the company they purport to be representing. Even if the address looks legitimate, there are methods that can be used to fool the browser into displaying the URL correctly but take you to the fake site instead. It is important to keep your browser up-to-date and secure (the focus of our 1st newsletter) because often these security weaknesses have been addressed by patches and updates.

STEP 3: Check that the web site is using encryption

Many web sites that are designed to accept private information use encryption techniques to help guarantee the privacy of your data. In Internet Explorer, look in the lower right corner of your browser window for the yellow lock icon in the status bar.

This symbol identifies that the web site uses encryption to protect your privacy.



You can double-click this icon to display the security certificate of the site. *If you see no status bar, check View, Status Bar in Internet Explorer.* The name following the "issued to" title should match the site you think you are on. If the name differs, you may be on a spoofed site. If there is ANY doubt, leave the site and do not enter any information.

STEP 4: Routinely review your credit card and bank statements

Even if you follow all of these steps, you may still become a victim of identify theft or fraud. Reviewing your statements routinely will help to identify questionable items that otherwise may go unnoticed even by the credit card company fraud units. A number of small, insignificant charges can ultimately add up to a large loss! Later in this newsletter we provide some tips to safe online credit card usage that you should put into effect as well.

STEP 5: Report suspected abuse to the proper authorities

If you feel you've received a fraudulent email and are the victim of phishing, you should do the following:

- Immediately report the scam to the company being spoofed. Either call or visit their web site – often companies have a special email address to which you can forward this type of fraud.
- Provide details of the scan to the FBI through the Internet Fraud Complaint Center. Their web site is located at www.ifccfbi.gov and has a link to file a complaint.

STEP 6: Keep your computer's security up-to-date

As described in our first newsletter, keeping your system secure is a full-time job but increasingly important so I will repeat this whenever possible. Keep Windows updates current, a firewall enabled, and antivirus products updated and enabled. Plus, new tools to stop spyware/malware are increasingly important. Next month, we'll talk in detail about spyware prevention so don't miss it!

Tips to help secure online transactions

Once you've purchased something on the Internet, you probably have become a big fan of the efficiency of the purchase and the ease at which most transactions occur. Online purchasing is very popular and growing daily. But as we've described earlier in this newsletter, so are the online scams and fraud. But there are simple things you can do to help secure your transaction:

1. Don't ever enter credit card data unless the page you are on is secured with encryption (step 3 above) by noting the lock icon at the bottom of your screen. Typically, website addresses that are secure will begin with https:// instead of the usual http://.
2. Use specific credit cards for online transactions. This makes it easier to review and control, and if you need to cancel a card due to fraud it won't affect your other credit cards.
3. While it may be less convenient, when given the option, do not have the online vendor save your credit card information.
4. Use a single-use credit card if possible. American Express started this trend a few years back but has now discontinued the service. However, other credit card companies and banks have picked up on the idea including Citigroup and MBNA. Contact your credit card company and ask about this service. Basically, this allows you to obtain a credit card number that (while charged to your account) is only valid for a specific purchase, period of time, or amount. This is an excellent tool to reduce the risk of internet-based transactions.

Hope you've enjoyed this month's "phishing" expedition. Next month, I'm going to focus on a major problem facing computer users – spyware. We'll talk about the tools and techniques to not only clean your system, but to prevent it in the first place so don't miss it!

***Special Note**: I've had inquiries about providing our newsletter to clients of our clients. If your firm services clients that would benefit from these security tips and would like to provide this newsletter to them, a customized version can be emailed for a small fee. For more information, please give me a call.*

Dave McCann