STAR Watch

Statewide Technology Assistance Resources Project

A publication of the Western New York Law Center, Inc.

Volume 11 Issue 4 July-Aug 2007

Don't Get Hooked: Avoid Phishing

While there are several different forms of phishing, they share a common characteristic: An attempt is made to trick an unsuspecting person into divulging sensitive personal information such as social security number, credit card numbers, passwords, bank account numbers, etc. Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. Most often, phishing takes the form of fraudulent emails that ask you to "confirm your password", or "verify your account", or "confirm your identity." Many times, these emails will include sentences similar to one of these:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information."

"Please click here to update and verify your information."

When should I suspect that it is a phishing scam?

There are several characteristics of a phishing scam that you can easily spot:

- **A phishing scam will ask you for personal information.** The goal of phishing is to get information from you that can be used for a fraudulent purpose. Somewhere in the email, or one of the links that the sender of the email has provided, will be a request for personal information. As soon as you see the request: STOP. Don't enter ANY information.

- **A phishing scam will appear to come from a legitimate company.** What better way to lull you into a false sense of security than to use the name of a reputable institution? Reputable institutions will never solicit you for information that they already have on file. In fact, on their web sites, most legitimate companies will have this statement: We will never ask you to give us your personal or billing information.

- **A link in a phishing email, if clicked, will not take you to the legitimate web site.** Many phishing scams "conveniently" provide a link to the alleged legitimate organization. If you click the link, you end up on a completely different web site. If that happens, don't enter any information and get off of the site as quickly as possible.

- **Even though a site may appear to be secure, don't be fooled.** In researching this article, several sources stated that if the link contained in the email sent

In this issue…

you to a site whose URL began with "https://:", the site must be legitimate. According to the Anti-Phishing Working Group, that is no longer true. According to the group "Phishers are now able to 'spoof,' or forge BOTH the "https://" that you normally see when you are on a secure Web server AND a legitimate-looking address. You may even see both in the link of a scam email. Again, make it a habit to enter the address of any banking, shopping, auction, or financial transaction website yourself and not depend on displayed links." The group goes on to state Phishers may also forge the yellow lock you would normally see near the bottom of your screen on a secure site. The lock has usually been considered as another indicator that you are on a 'safe' site. The lock, when double-clicked, displays the security certificate for the site. If you get any warnings displayed that the address of the site you have displayed does NOT match the certificate, do not continue."

- **Misspelled words or grammatical errors.** Are there any words misspelled in the text of the email. Are there grammatical errors? If there are, it's a phishing scam.

- **Personal information asked for via the phone.** Sometimes, you will get an email allegedly from an organization that you have done business with asking you to call a "secure" number listed in the email in order to confirm your account number, billing address, or other personal information. This is NOT a legitimate request.

Generic greeting in the phishing email. One subtle way to detect a phishing attempt is to check if you are personally identified in the email content. For instance, if eBay ever tries to contact you, they would use your eBay user ID, not "Dear eBay Customer."

How do I avoid phishing attempts?

Be **Skeptical:** For starters, you should to be very skeptical of any emails sent to you that ask for your personal information. If a bank or other company really needs to get hold of you to verify something, they would most likely send it in writing or via a secure email. Companies do not solicit their clients/ customers for information that they already have.

Be Protected: Internet Explorer 7 has a phishing filter that will help to uncover phishing scams. Be sure that it is enabled.

If you prefer to use Firefox as your web browser, the latest version has a phishing filter in it. If for some reason, you want to stay with an older version of Firefox, the installation of "Google Toolbar for Firefox" includes a phishing filter.

Follow up: If you have been the target of a phishing attempt, contact the company that the scammer attempted to impersonate. On the legitimate company's web site will be instructions for reporting scamming attempts. Forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com"). When forwarding spoofed messages, always include the entire original email with its original header information intact.

Don't get caught in a phishing scam

The bottom line: phishing scams are just going to get more and more sophisticated. In order to avoid being caught, you should be very skeptical of any attempt to retrieve your personal information, and take proper security precautions every time you are on the Web.

Can you recognize a phishing scam?

If you have the time, you might want to go to the location shown in the link below and take a short test. In the process of taking the test, you will be shown 10 emails. From the information in those emails, you must decide whether they are legitimate or not.

http://www.sonicwall.com/phishing/

Online Backup Services: Are They Worth it?

Haiku poetry combines lyric language in a compact form to paint a powerful mental image in the reader's mind. While we would never go out of our way to read Haiku poetry, we came across several web sites that offered up Haiku that address one of the most traumatic events that a computer user might experience:

> Three things are certain:
> Death, taxes, and lost data.
> Guess which has occurred.

> Spring will come again,
> But it will not bring with it
> Any of your files.

One of the most gut-wrenching, infuriating, and terrorizing moments in a computer user's life is that time when he or she realizes that the document that they poured their heart and soul into cannot be found on the computer. Or maybe it's there, but with every attempt to retrieve it from disk, the computer mocks them with error messages. Face it; it's gone. It's defunct. It's kaput. If paper copies of the document exist, maybe the whole thing can be retyped—if there is enough time. But, it has to be ready to go in two hours? Oh. It's so sad to be you.

For every single person who uses a computer to create anything, it isn't a question of "if" an important document will ever be irretrievably lost, it's only a question of "when". Given this fundamental fact of life, a disciplined policy for backing up important data is a necessity. Unfortunately, many organizations don't have the cash available to purchase a backup system that has the capacity to back up all of their critical data. So they don't do anything. They are one hard drive crash away from catastrophe. Any document or data file that hasn't been backed up is in serious danger of being lost forever.

Most traditional backup methods copy files onto some kind of media, be it a tape or external hard drive, CD or DVD, or a USB keychain drive. These methods

are convenient and quick, and many (particularly external hard drives and DVDs) offer plenty of inexpensive storage space.

The problem is that most of the time, most people keep the tapes, external hard drives and DVDs in the same office or building as the computer they're backing up. So, should a disaster--hurricane, earthquake, fire--occur, both the computer and the data backup could be destroyed. To be most secure, backup data should be stored safely off site.

Online Backup Services

Online backup services are accessed by connection to the Internet. The typical backup service provides the software needed to perform the backup to their site. Backups can be scheduled to run at times when no one is in the office or files can be backed up on demand. An online backup service can be a viable solution to the issue of data backup, but in order to make an informed decision, users should be aware of the strengths and weaknesses of online backup services.

Advantages of an Online Backup Service:

- It can be cheaper than traditional tape based backup solutions (after taking into consideration capital costs of equipment, media and staff costs). Some online backup services will store a “small” amount of data for free. Depending on the company, “small” is somewhere between 50 Megabytes and 25 Gigabytes (1 Gigabyte = 1,000 Megabytes). Typically, the free backup services don’t include all of the features of services that have a monthly fee, but any backup is better than no backup.
- Your data is stored securely off site. In the event of a regional disaster that will make your office unusable, the data that was backed up could be accessed from anywhere that an Internet connection is available.
- Set up and installation is usually quick and simple
- Back up and data recovery can be simpler and quicker than more traditional methods
- Some services allow you to backup and restore multiple versions of files - this can be useful if you need to go back to an earlier version of a document for any reason.
- Web access for remote users

Disadvantages of Online Backup Service:

- Ongoing monthly charges which can be prohibitively expensive if you need to back up very large amounts of data.
- Relies on a working Internet connection. No Internet, no backup!
- Speed and amount of data backup is limited by the speed of your Internet connection. A typical aDSL line has an upload speed of somewhere between 384Kbps and 768Kbps. At those speeds, it would take 11 to 22 seconds to upload 1 Megabyte of data, which is reasonable if there are only a few Megabytes of data to upload. However, to upload a single

Gigabyte of data, it could take more than 6 hours. If large amounts of data are going to be backed up, a fast Internet connection is a necessity.

- Reliance on external provider to keep your data secure - If you choose online backup as your sole back up method you'll be entrusting all your valuable data to someone else who potentially could go out of business or otherwise place your data at risk.

Factors to consider when choosing an online backup service:

- Cost – prices for storage of the same amount of data can be substantially different. Some services offer free storage. Don't be afraid to shop around. Choose what is best for your needs.
- Reputation - get recommendations from someone who has used them wherever possible.
- Availability and extent of tech support. Is someone available 24/7 if you have a problem?
- Will the solution work with your particular set up? Will the backup service give a 30-day free trial, or a 30-day money back guarantee if their system doesn't work?
- Can you choose which files to back up?
- Does the service allow automated and unattended backup?
- Is back up of open files and running databases possible? This feature is important if you need it, but not possible with all services.
- Security – Does the backup service provide encryption of data during transfer and while it is stored on remote server. Is access to the backup facility password protected? Can different passwords be assigned to individuals in your organization that give different levels of privileges?
- If needed, is central management of backup/restore from one or more locations possible?
- Will you get notification of any problems with the backup/restore?

While all backup methods have their pros and cons, we would encourage organizations to consider the use of online backup services as part of a comprehensive data integrity strategy. While we would never recommend that an online backup service be the only backup method used by an organization, if currently no backups are being done, any method of backup is better than no back up at all. We might also recommend to those people who are members of organizations that don't do backups, that they sign up for a free backup service and protect all of the documents that they are responsible for.

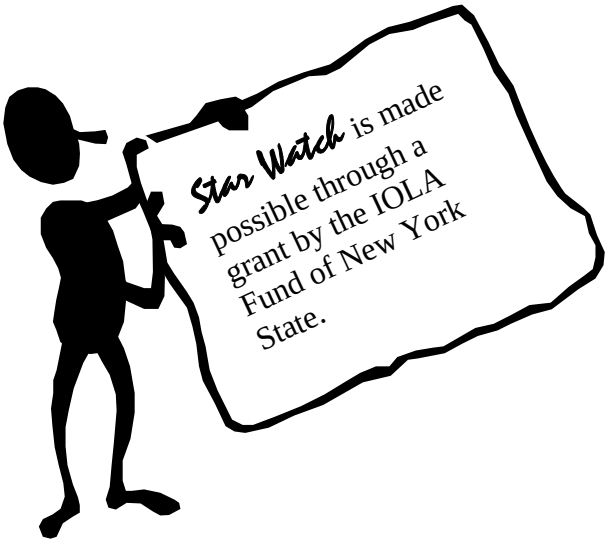
A parting thought…

Having been erased,
The document you're seeking
Must now be retyped.

WNYLC Web Statistics For July 2007

Total Hits…..……371,578
Number of Pages Viewed.....……143,412
Total Visitors.....……71,174
Average Hits/Day….....……..11,611
Average Pages /Day…….……..…….4,481
Top Web Browsers Used:
Internet Explorer 6.x……...47%
Internet Explorer 7.x…….…….....29%
Firefox.....…..……...……....10%
Safari.....……..…1%

Top Operating Systems Used:
Windows XP.....……76.90%
Windows 2000.....……...8.51%
Mac OS.....……....….2.15%
Windows 98.....……...2.58%
Windows Vista.....…….1.68%



WHO WE ARE

Joe Kelemen - Attorney
Kathleen Lynch - Attorney
Tom Karkau - Programmer
Sherry Soules - Administrator
Holly Lindstrom - Data Analyst

Wnylc@wnylc.com

716-855-0203

www.wnylc.net

Western New York Law Center, Inc.
237 Main Street, Suite 1030
Buffalo, New York 14203