

**Special
Security
Edition**

IU South Bend Information Technologies

IT UPDATE

April 2007

Gone Phishing

Phishing: The technique, occupation, or diversion of catching Internet users off guard with fraudulent e-mails in an attempt to steal passwords, financial or personal information, or introduce a virus attack.

Why Phish?

A criminal uses phishing techniques in the hope of luring you in to providing computer access or enter personal information. Their sole intent is illegal financial gain, usually using your identity and your financial accounts.



For example, an unsuspecting victim of a phishing scheme may have provided enough credit card information to allow someone the ability to use that credit card account to make unauthorized purchases. A victim may have furnished an account password which allows a criminal to directly access the account. Less obvious is the use of computer viruses which gather information without your knowledge.

What Phishing Looks Like

The two main methods for phishing are e-mails containing links to a fake web page, or distribution of a specially formed computer virus.

Phishing is done by people who are masterful at deception. What better way to gather sensitive information about you than to trick you in to giving it to them. You may have already received fake e-mails from PayPal, eBay or a bank of some kind. You may have received e-mails from a financial organization that you do not have an account with. You think those e-mails strange and continue on with your life. Then one day, you receive an e-mail that appears to come from an organization that you do have an account with. The subject line is something like *"Verify your account"*, *"If you don't respond within 48 hours, your account will be closed"*, or *"Dear Valued Customer."*

You are told that you need to verify or update information by clicking on a link which takes you to an "official" webpage. The webpage and the e-mail contain that organization's logos, look exactly like, (and in fact copy), the actual webpage for that organization.

Most of the time, if you follow the instructions from an e-mail, go to a web page and enter personal information, you have just been phished.

The second method, viruses, reach your machine in various ways. They may come as an attachment with e-mail. You may download them from the Internet without knowing it. Many sites that offer free images, screensavers, virus blockers, spam blockers or spyware removal tools are malicious. Yes, even

that official looking website that offers screensavers related to your favorite movie, past time, music or TV star can be malicious in nature.

What You Should Not Do

- Don't follow links in unsolicited e-mails, no matter how official it looks. Call the institution directly (not from a phone number provided in the e-mail) and ask if the request is legitimate.
- Don't download items off of the Internet unless absolutely certain of their validity.
- Don't open e-mail from people you don't know.
- Don't give out personal information to anyone using any medium for which you did not make the initial contact.
- Don't enter information in any web pop-up window.
- Don't give out any of your passwords to anyone, no matter who they are or what reason they give. Period.

What You Should Do

Be cautious of any request for personal information.

A phisher can disguise a fake web address to look like a real one. Most e-mail phishing schemes can be identified by placing your mouse pointer over the web link provided in the message to see if the address that pops up under the mouse pointer is the same as what is in the e-mail. The image below shows that the addresses are different.

<https://www.woodgrovebank.com/loginscript/user2.jsp>

<http://192.168.255.205/wood/index.htm>

But even if the links look the same, use extreme caution. A phisher can use a technique whereby the actual web address is used but part of the official website is faked. To go to an organization's website, it is always best to do so by using a web search, or typing the address directly in to the browser's address bar, and not by clicking on a link contained in a webpage.

Ensure that Spybot and Ad-Aware are kept up-to-date, and run scans at least weekly. These are spyware protection tools IU South Bend IT has provided on all campus workstations.

Verify that your Symantec anti-virus definitions are up-to-date. This software is set up to update and run automatically on your office computer. However, sometimes it can be inadvertently or maliciously turned off.

If You Believe You Were Victimized

If you do provide personal information in a way that later seems suspicious, the three main things to do are:

1. Change all your passwords immediately.
2. Contact your financial institutions immediately and discuss your options.
3. Watch your accounts very closely for illicit activity.

Use Spybot and Ad-Aware

Spybot and Ad-Aware are detection and removal software utilities that will scan and remove spyware and adware from Windows computers. These applications are free to all IU students and employees and should already be installed on all campus computers. If you don't find it under All Programs on your computer or it is not the latest version, you can download it from IUware Online, by visiting the url, <http://iuware.indiana.edu/> and from the menu on the left select Security and choose the available version. Each application should be updated and run at least weekly. The instructions below are a condensed version of instructions available in the Knowledge Base (kb.iu.edu).

Before beginning the scanning process of either application it is recommended that you reboot your computer and go into SAFE mode. To do this, restart your computer and then press F8 repeatedly while the computer is starting. From the list which appears, choose **Safe mode with networking**. When Windows comes up, log in and continue with the instructions below. (These instructions were based on the most current versions of the applications. Screens and procedure may vary slightly depending on the version and configuration of the software being used. If you need assistance, contact the Helpdesk at 520-5555)

Spybot

1. Open the Spybot program. (Some computers may immediately begin the scan—if so, click on Stop Check, then click on Update.)
2. Click the Search for Updates button.
3. Spybot will prompt you if no new updates are available. If so, click OK. Otherwise, a window will display updates available. Place checkmarks next to all available updates and Click Download Updates. Spybot will download and install the most recent updates.
4. Some computers may restart a scan automatically. If not, click Check for Problems to start scanning your computer. (The scanning process may take a significant amount of time).
5. When the scan is done, select all the items on the list and click Fix Selected Problems. If no problems were found you'll receive a "Congratulations" note.
6. When prompted to confirm removal of the selected objects, click Yes. If Spybot could not fix all problems you will see the message, "May Spybot—S & D run on your next system startup?". If you see this prompt, click YES.
7. After objects are removed, Spybot will confirm the number of problems fixed. Click OK to continue.
8. Close Spybot.

Ad-Aware

1. Open the Lavasoft Ad-Aware SE Plus program. You may be immediately prompted that your definitions are old. If so, click OK. Otherwise, click Check for updates now.
2. In the resulting window click Connect. Ad-Aware will check for a new definition file and prompt you to download and install it.
3. If no new reference file is available, you will see a dialog box that says "No updated component available". If this happens, click OK and proceed with step # 5.
4. To download and install the new definition file, click OK.
5. When installation is complete, click Finish
6. In the resulting screen, click the Scan Now button, then select Perform Smart System Scan, then click the Next button. The "Performing System Scan" screen will indicate its progress as it scans the computer. This scan could take a while to complete.
7. When the scan is complete, the "Scan Complete" screen will display. Objects found will be highlighted in red.
8. Click the Next button, and the "Scanning Results" screen will display.
9. Right-click any item in the results list and from the pop-up menu, chose Select all objects. After all objects are selected, click the Next button.
10. Click the OK button to confirm you want to remove all critical adware found.
11. Ad-Aware will remove the adware and return to the status screen.
12. Close Ad-Aware. If you ran Ad-Aware in Safe Mode, restart your computer to return to normal startup mode.

Don't Save Your Password!

Many subscription or "registration required" sites offer the option to remember your password so you won't need to enter it the next time. These passwords are stored on your computer and a hacker could have access to all of them in short order. NEVER have a system save or remember your password.

Switch to Passphrase!

Are you still hanging on to that 8 character password that can be hacked in a matter of minutes? Switch to the more secure passphrase now! It is generally easier to remember and easier to type, but it is exponentially more difficult to hack.

Passphrases MUST contain 15-127 characters, using at least four different characters, and at least four words (words are two or more distinct letters separated by one or more non-letters). You can use spaces between words so typing is more normal.

Get creative and help secure your information and that of the university by changing to a passphrase! Visit <https://passphrase.iu.edu/> to replace your password with the more secure passphrase.

Are You Legal?

Just because you *can* download that song, or movie, or TV show does not mean that you have the *right* to do so.

If you download an illegally distributed file to your own computer, you are breaking the law and are subject to legal action including substantial fines.

Many of the applications used to download such files (e.g. KaZaa, BitTorrent, eDonkey, etc.) are set up to automatically share the files with others, causing you to illegally *distribute* copyrighted material.

For more information on staying legal, visit the Knowledge Base at kb.iu.edu and search for "copyright infringement".

IT Helpdesk

DW1245

Hours:

8:00 am—8:30 pm, Mon-Thurs.

8:00 am—5:00 pm, Friday

www.iusb.edu/~sbit

Phone: 574-520-5555

E-mail: helpdesk@iusb.edu

*Information Technologies
IT Update - April 2007
Beverly Church, Editor*