Holzsager Technology Services, LLC
P.O. Box 535, Fair Lawn, NJ 07410-0535
(201) 797-5050 info@tech4now.com
Visit us on the Web at http://www.tech4now.com

Phishing: Will they catch the big one this time?

By Fred W. Holzsager

Last April, I spoke to the third, fourth, and fifth graders at the Radburn Elementary School during Career Day. The topic was "Online Safety" and the children listened attentively as I imparted friendly warnings about using the computer and connecting to the Internet. Many children volunteered to share their experiences (and those of family) with those present. It was a wonderful exchange of information as well as a positive learning experience. The thought that then arose was to give the same presentation to parents.

Today's lesson is about the big one that got away. As a child, my father used to take me to the Dunkerhook Park to go fishing. It was always fun and a great opportunity to let my father share his techniques. Well, today the word has changed from Fishing to Phishing. Mind you, my father is not phishing, it's just to relay a point. *Phishing*, as the term goes, is when someone constructs an e-mail message for the sake of committing fraud, typically through identity theft.

Picture yourself sitting at your desk while working on the computer. A message arrives from a familiar origin—it may be from your bank, your credit card company, your favorite charity, or even the extended family of a long deposed dictator from the Ivory Coast or Nigeria. The message from the latter recants the history of the political situation in the country just prior to the *coup*. The writer then begins to describe a convoluted plan by which you will be able to help him/her expatriate the millions that were hidden by the deposed family member by processing all of the millions inconspicuously through your personal bank account. Keep in mind, this example (from the recouped fortune) is an easy scam to spot. Less than 1% of all recipients respond to these spam e-mails.

The first examples given, however, will be well masked and designed to strongly resemble the genuine article. You have just received a message from your bank in an e-mail. The message is addressed to you in an impersonal manner, either as "Dear Account Holder" or "Attention." There are even some phishing messages that are sent with actual names embedded in them due to stolen databases, in fact, nearly 5% respond to these mails ("IT Tackles Phishing", Delio, Michele, InfoWorld: 24 January 2005, pp 30-35). You notice the familiar logos pasted all over the message to lend credibility to the missive. Highlighted within the message are sites that you are directed to in order to confirm your identity and verify the data. The site reads **verify.*your_institution*.com** and you feel comfortable in responding. The biggest question nagging you is that deep in your gut, you don't understand why your institution would choose this method to reconfirm information that they already have.

The first thing to recognize in this situation is that your gut feelings and intuition are doing their best to protect you. Trust your intuition, call your institution and ask them why you would be prompted for such information. Even if it were an

e-mail from AOL, you would NEVER be asked by a tech or customer service for your password. They may be able to reset it, but they DO NOT ASK FOR YOUR PASSWORDS. Anytime that someone asks for your password, think twice!

The second clue in the message… You noticed that some or all of the graphics on the screen are unclear or fuzzy. They might not be, but in many cases, the graphics have been copied from a high resolution copy and pasted in a lower resolution. You may even notice that the color in the logos may be off or wrong altogether.

The third clue is revealed when you hold your mouse cursor over the hyperlink provided by the sender. Although it may read **security.*your_institution*.com/verify**, when you hold the mouse over the link, you will notice a different address is displayed by your browser with an address that does not come close to the one you saw shown. Again, trust your intuition on these!

Finally, let's pretend that you have gone to the referenced site. Look at the URL of the sites in your browser's address line. Does it compare with what you expected? Is the name of your institution listed as the first part or a lesser part to the address, such as ***your_institution*.oursite.com** or does it display as **security.*your_institution_spelled_incorrectly*.com/verify**? Either way, be wary of this site.

What can you do if this happens? First of all, do not go to the site. It is always possible that visiting such a site may launch a script which could place spyware or another snippet of code onto your system which may report keystrokes or other "Trojan-like" activities to the author. If you hear of a fire in a building and curiosity attracts you to the flames, the likelihood of getting burned increases as you get closer to the building. The greater the distance maintained from the risk, the safer the position maintained. If you wish to report the e-mail to your institution's fraud department, visit their legitimate site and you should find a link relevant to your issue. If not, you may also report the details to the Federal Trade Commission at www.ftc.gov. They even have a detailed information page dedicated to phishing:

http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

Simply put, phishing is a fraud primarily based upon identity theft. If you are too casual about your personal information, you can get burned. Remember to be certain your credit cards are returned to you, that your IDs and passwords are not posted on your computer monitor and for added security, do not use the default browser autocomplete on your computers: If you visit eBay, your bank, or broker online and someone steals your computer, they will have the benefit of access to your accounts without doing any further work (In Internet Explorer click: Tools, Internet Options, Content Tab, AutoComplete…, Clear Passwords). Play it safe and think of your personal information as if it were cash because that it was it really is.

If you are interested in learning more about the items discussed above, feel free to contact Holzsager Technology Services, LLC at (201) 797-5050 or by e-mail at support@tech4now.com. For general information about other services for your home or office, kindly visit www.tech4now.com, there you may retrieve additional information bulletins and articles to help you use technology to your fullest advantage.

