SSBG IT Solutions
Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

How to Spot Phishing Attacks

By Scott Pinzon, Editor-in-Chief, LiveSecurity Service

[**Editor's note:** This LiveSecurity Foundations article is intended to help a network administrator raise the level of computer security awareness within his or her corporate culture. Please feel free to forward this article within your organization to non-technical users who could benefit from a more educated approach to Web surfing. -- *Scott*]

When comedian Steve Martin hit prominence in the 1970s, one of his stand-up bits dwelt on his important finding that in France, they don't call a hat, a hat. They call it a "chapeau." As if divulging news certain to shock and outrage us, Martin marveled, "It turns out the French have a different word for *everything!"*

You might feel the same if you're a normal person (meaning, not a computer geek) trying to keep up with computer security. Hackers have a different word for *everything!* Lately they've filled the news with references to "phishing attacks." What are those? How do you make sure you're not a victim? And why in the world can't hackers spell correctly? Answers ahead.

"Phish" Phollows "Phreak"

Phishing definitions on line agree: "Phishing" is the term for a type of con perpetrated via e-mail or Instant Messaging. In a typical phishing attack, the perpetrator sends out an e-mail that appears to come from a company you might do business with. It solicits confidential information. The tricksters hope you'll reveal personal data they can use for fraud, such as username/password combinations; bank account numbers; Social Security numbers -- anything they can use to impersonate you on line and grab some free money.

Why "phishing"? A typical phisher is not after you personally, any more than the typical fisherman goes to the ocean to catch one specific fish. Phishers generally use the techniques of spammers to send their deceptive e-mails to thousands of users, to see who is naive enough to "bite."

Why the phunny spelling? In the late 1960s and early 70s, before the Personal Computer, proto-hackers tested their skills against America 's phone system. Hackers who devised ingenious ways to place long-distance calls for free borrowed the "ph" from "phone," mixed in late 60s slang, and referred to themselves as "phreakers." Using "phisher" instead of "fisher" follows this hacker tradition.

But don't let the misspelling phool -- er, *fool* you: phishers are not stupid. Some of their crafty tricks will hook you unless you know what to watch for.

What a Phishing Attack Looks Like

To see some phishing attacks from a safe distance, visit the Anti-Phishing Working Group's educational site. Two highlights:

- In a classic phishing example, the intended victims received a simple e-mail (seen here) supposedly from eBay. "eBay" wanted you to click a link and enter your user name and password, to "complete their records." Clicking the link took you to a Web page that looked like eBay's, but actually belonged to some guy in Sweden. People who fell for the trap duly entered their eBay credentials -- which were just as duly captured for abuse by the phishers.

- A more elaborate attack used a well-designed e-mail that seemed to come from Citizens Bank. It looked like an online survey and claimed that Citizens Bank would pay you USD $5.00 for participating. When you clicked the link and filled out the form, the clever scammers asked for your credit card number "so we can deposit the $5.00 in your account." But Citizens Bank had nothing to do with any of this. Tracing the Web site that displayed the survey form took investigators to the computer network of some unwitting school in Korea.

These examples give the merest glimpse of phisher cleverness. The most sophisticated attacks can link you to a real company's legitimate Web site, then pop up a cunningly devised window that seems like part of the site, but in reality is a trap added by the phisher. On the Web, what you see is not necessarily what you get.

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

So how do you dodge phishers' tempting hooks? A few quick tips follow.

Phishing's Phatal Phlaws

Common sense is your best defense.

Recently while helping make an independent film, I visited a gigantic warehouse packed with rentable props and sets for movies. Stepping into the high-ceilinged storehouse dazzled me. Sci-fi and spaceship props jostled against castle walls. A 1950s American diner, complete with jukebox, sprouted palm trees around a fake dead body. The packed-to-the-rafters place was so crazy, distracting, and marvelous, I soon forgot why I had come there.

Isn't that like the Web? Sometimes you can lose your senses amid all the flashing ads, headlines, funny videos, and densely-packed information. So when a polite e-mail arrives saying "Thanks for opening your account! Please verify by entering your credit card number," you just might do it. But hang onto your wits! Maybe the reason you don't recall opening that account is because you never did.

Phishers have a phatal phlaw: they have to guess which companies you patronize on line. They have to guess what transactions you have with those companies. So: if you receive business e-mail asking you to do something that makes little sense in the context of your usual business relationship with the supposed sender, don't trust the e-mail.

Don't be a churl; check the URL.

A Uniform Resource Locator (URL) is what you type into your Web browser's address bar, so it can find something on the World Wide Web for you. (If this is new to you, you might like to read, "Foundations: Avoiding Dangerous URLs.") In the consumer world, if a link in an e-mail claims it takes you to PayPal, the URL of the Web page you arrive at generally ought to start with http://www.paypal.com. Since a boobytrapped phishing site does not actually live on the PayPal domain, a phishing site will not have a URL that says www.paypal.com. So, any time you travel from an e-mail to a Web page, read the Web page's URL and verify that it ties to the company who supposedly sent the e-mail.

Phishers try to weasel around this dead give-away by using subtle variations on the legitimate company's domain (e.g., "pay-pal," or "paypall"). Such misspellings indicate phishing. (I mean, c'mon, what valid Web site can't spell its own name properly?) Phishers also try to baffle you by using a URL that shows an IP address instead of a domain name; for example, http://211.250.204.133/docs. Most consumer-facing businesses don't use this type of unfriendly addressing scheme, so be suspicious when you see it.

To dodge evil phools, bring in power tools.

Some phishing attacks are too brilliant to spot unless you're a savvy security expert with time to spare. To help you analyze what's going on behind the scenes at Web pages, consider installing a helpful free tool such as Spoofstick. (**Note**: Do not install any software without consulting your network administrator.) Each time you visit a Web page, Spoofstick performs some quick snooping to verify what page you're really on. It displays its results in a nice, large font in your browser's Toolbar. Before you enter sensitive info at a Web site, just glance up at Spoofstick's results to verify you really are where you think you are. Another helpful free anti-phishing tool is the Netcraft Toolbar, also worthy of your consideration.

Be safe out there!

So there you go. Now you know what phishing is about, how you can tell when a phisher is dangling a hook in front of you, and how not to phall for their tricks. The one thing I didn't explain is whether the French do, in fact, have a different word for phishing. I'll have to get back to you on that. Until then, I wish you safe Web surphing! #

Original Article from Watchguard.com