

Phishing: No Ski Mask Required

By Ashish Sawhney

Remember when crooks would impersonate utility company employees to gain access to your residence before robbing you blind? Well, welcome to the 21st century—now you have a new breed of impersonators known as *phishers*.

These individuals set their own work hours and are not even limited by geographic location. They could be working from down the street or from halfway around the world. Thanks to the Internet, location makes no difference to them.

Webopedia (www.webopedia.com/TERM/p/phishing.html) defines phishing as “The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.” Simply put, it is a method used to siphon information from unwilling and unsuspecting consumers by impersonating a real company via e-mail.

Information collected by phishers can be used for purposes ranging from identity theft to simple credit card fraud. For the month of December 2004 alone, there were more than 9,000 new and unique Web sites reported to the Anti-Phishing Working Group (APWG). This organization (www.antiphishing.org) is a global

pan-industrial and law enforcement association focused on eliminating fraud and identity theft resulting from phishing and e-mail spoofing of all types. According to APWG, that is a growth rate of 24 percent since July 2004.

So the pen (or mouse button) truly is mightier than the sword. When compared to bank robbery, phishing can provide similar returns but with significantly lower risks. Stealing from people just by writing an e-mail is alarmingly simple.

A few clicks of a button can send e-mail to millions of people around the world asking for information such as name, credit card numbers, Social Security number, and debit card numbers, along with PINs, account numbers, usernames and passwords. Even if only one percent of the recipients fall for the scam, you can see how lucrative phishing might be. All this and phishers don't have to put on a ski mask or worry about being perforated by a bullet.

You must be wondering how people would be so gullible as to just hand out confidential information. It is true that some phishing scams are pretty easy to spot. They are poorly written with multiple mistakes in spelling and grammar, incorrect use of words, and are badly formatted. These e-mails do not appear to be a formal communication from any organization.

But just as predators in the jungle evolve and adapt to their environment, phishers are getting more sophisticated and creative. They are using techniques such as hijacked logos, spoofed e-mail addresses, and verbiage that could insinuate rewards or even be threatening. Phishers use information freely available on the Internet to compose their clever e-mails. A well-baited phishing e-mail contains all the proper logos of the organization being used in the scam, and includes proper verbiage, e-mail addresses—even the name at the bottom of the e-mail is of a real person at the unwitting company.

To most normal consumers, these e-mails look legitimate. Even the hyperlinks in the e-mail appear to have the company name and will take you to sites that appear to be valid company pages. This is excellent phishbait that can fool many otherwise cautious victims.

Here are some common phishing methods:

Reconnaissance: Go to a company's Web site and gather information such as names of company officers (needed for signing the e-mail to make it look official). Next, roll your mouse over the company logo and save it to your hard drive. The logo makes the e-mail look legitimate.

Spider: To "spider" a Web site means to crawl through the site and all of its hyperlinks. There are tools available to help spider a Web site and copy the content to your specified location. Using this technique, phishers can set up a fake Web site with most of the original content. They modify part of the site to allow them to capture your confidential information.

Pop-ups: You may receive an e-mail with the actual link to the organization's true Web site. When you click on the link from within the e-mail, it takes you to the actual site, but you will also get a pop-up asking for verification or to provide personal information. It appears that the pop-up is legitimate because it appeared from visiting the organization's Web site, but in reality, any information entered

in the pop-up window is recorded at a surreptitious location.

"They work with each other to find new flaws in products, which allows them to be successful in their scams."

There are other phishing methods as well. Some of them are successful because phishers are able to exploit newly discovered vulnerabilities. Such was the case in January 2004 when the FDIC was the targeted organization.

This particular phishing e-mail contained a hyperlink that used a Microsoft IE browser exploit to mask the URL in browser. This technique caused the victim to believe they were visiting the actual FDIC Web site, but behind the scenes they were directed to an address that was registered in Karachi, Pakistan. Details of this phishing scam can be found at www.antiphishing.org/phishing_archive/FDIC_1-24-04.htm.

Thwarting phishing scams is not easy. Detecting the true source of e-mails is difficult at best, thanks to anonymous re-mailers and free e-mail hosting servers. The abundance of mis-configured or insecure e-mail servers on the Internet provides phishers another avenue for soliciting their e-mails.

Additionally, e-mail headers are easy to forge, so phishers can pose as anyone when sending the e-mail. Even the fake Web sites are hard to track because, according to the APWG, a phishing site only stays online for an average of 5.9 days.

We all have to do our part to make the Internet safer. Here are some tips from

CyberScience Laboratory (www.cyberber-science.com) on how to keep your information safe and not become another victim of identity theft:

- Treat every e-mail with caution; it could be forged.
- Never use a link in an e-mail to get to any important Web pages. Instead, open your browser and type in the URL address yourself.
- Never send personal or financial information by e-mail.
- Regularly check your bank statements for fraudulent charges.
- Verify that your software (*i.e.*, the operating system, Web browser, and e-mail application) is properly protected with the latest software updates.

In this age of technology, criminals are finding high-tech methods to take advantage of people. They don't have the corporate or legal politics and bureaucracy to inhibit them, and there is even a spirit of camaraderie among these individuals that allows them to work as a single team. They work with each other to find new flaws in products, which allows them to be successful in their scams. If we are to prevail against these individuals, we need to start working with each other and adopt the same spirit of camaraderie that they use.

Ashish Sawhney is a security analyst for State Farm Insurance. He has worked for State Farm for more than 10 years, focusing the past seven years on Intranet, Internet and Network security and computer forensics. He has a Master's Degree in Information Systems Management and several security, related certifications such as CISSP, EnCe, Security+ and GSEC.

