



# Enterprise Security Office Monthly Security Tips NEWSLETTER

OCTOBER 2008

Volume 3, Issue 10

## Phishing – How to avoid getting hooked!

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall information security posture.*

### **What is phishing?**

Phishing is a scam that attempts to entice e-mail recipients into clicking on a link that takes them to a bogus Web site. The Web site may prompt the recipient to provide personal information such as Social Security number, bank account number or credit card number, and/or it may download malicious software onto the recipient's computer. Both the link and Web site may appear authentic, however they are not legitimate.

### **How does it work?**

Have you received an e-mail, an instant message, or another communication that just did not seem right, even though the communication appeared to be from a reputable organization? This communication could very well be a phishing scam. It's important to note that in the past, phishing scams were often more easily detectable because of misspellings, typographical errors and blatantly bad grammar; however, they are increasingly more difficult to detect because they often appear legitimate.

Phishing scams try to "bait" the recipient in a number of ways: the malicious e-mail could include notice of an account cancellation, a request to verify/update personal information, a notice of a purchase that you did not make, or just about anything else that would get you to respond to the communication. The types of messages used in phishing are expanding almost every day, so it is important to be cautious of any communications you receive.

If the e-mail communication, with its enticing subject line, is the "bait," what is the hook? The hook is getting you, the user, to take some action that enables the phisher to obtain information or otherwise gain access. You may be "tricked" into visiting a Web site, which appears to be a legitimate organization's Web site. Once at that site, you may be asked to enter personal information. Another method of attack may be to get you to open an attachment in an e-mail, and malicious code, such as a Trojan horse will be installed onto your computer. Other variations include a telephone call, in which the phisher will ask you to provide personal information. Once the phisher has "hooked" you, they may use the information to open accounts in your name, access your bank account or make purchases using your credit card. There is also a type of phishing attack known as "spear phishing" where the attacker targets specific individuals by name or organization. For example, an e-mail invitation to attend an event that may be of interest could be sent to an organization's employees. When an employee clicks on the link contained in that e-mail, malware is downloaded to the employee's computer. The attacker may be targeting specific employee information, such as user names and passwords, or proprietary organization information.

### **How do I know it is a phishing scam?**

- If you receive an e-mail appearing to be from a legitimate business, requesting you submit personal information, it is most likely a scam. Legitimate businesses do not send e-mails requesting personal information.

- Use an Internet search engine to research the subject line of a suspicious e-mail to determine if that subject line is a known phishing scam.

### What can I do?

- Be cautious about all communications you receive. Think before you click.
- If the communication looks too good to be true, it probably is.
- If it appears to be a phishing communication, do not respond. Delete it. You can also forward it to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov).
- Do not click on any links listed in the e-mail message and do not open any attachments contained in suspicious e-mail.
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens.
- Install a phishing filter on your e-mail application and on your Web browser. These filters will not keep out all phishing messages, but will reduce the numbers of phishing attempts.
- Ensure that your computer is up-to-date on all patches.
- Ensure that your antivirus program is installed and up-to-date.
- Use bookmarks in your Web browser for the organization's you regularly communicate with to limit the chances of being redirected to malicious sites.
- If you think you have been scammed, visit <http://www.ftc.gov/idtheft>.
- Look for unauthorized charges or withdrawals on your credit card and bank statements/bills.
- Review your credit report - visit <http://www.ftc.gov> for a link to request an annual free credit report.

### For more information on phishing, please visit the following sites:

- **AntiPhishing Work Group:** [www.antiphishing.org/](http://www.antiphishing.org/)
- **OnGuard Online:** [www.onguardonline.gov/phishing.html](http://www.onguardonline.gov/phishing.html)
- **Federal Trade Commission:** <http://ftc.gov/bcp/menus/consumer/tech/privacy.shtm>
- **National Consumer League's Internet Fraud Watch:** [www.fraud.org/tips/internet/phishing.htm](http://www.fraud.org/tips/internet/phishing.htm)
- **US CERT:** [www.us-cert.gov/cas/tips/ST04-014.html](http://www.us-cert.gov/cas/tips/ST04-014.html)
- **WatchGuard Video:** [www.watchguard.com/education/video/play.asp?vid=budhasmail](http://www.watchguard.com/education/video/play.asp?vid=budhasmail)
- **National Phishing Webcast- October 9, 2008 2:00pm Eastern:** register at [www.msisac.org](http://www.msisac.org)

## October is National Cyber Security Awareness Month

The Fifth Annual National Cyber Security Awareness Month is being celebrated during October 2008 as a collective effort among the Multi-State Information Sharing and Analysis Center, the National Cyber Security Division and the National Cyber Security Alliance to raise cyber security awareness nationwide and empower citizens, businesses, government and schools to improve their cyber security preparedness and help promote a safe Internet experience. For more information and awareness materials, please visit the MS-ISAC at [www.msisac.org](http://www.msisac.org).

Brought to you by:



[www.msisac.org](http://www.msisac.org)

