HOW TO STOP PHISHING, SPYWARE AND SPAM

Spyware is the means through which hackers gain access to your computer and your private information. Spyware is defined as any software that covertly gathers user information through your Internet connection without your knowledge, usually for advertising purposes. It watches everything you do on the Internet and sends that information, including private e-mail, passwords, and credit card numbers to the hacker invisibly, without your knowledge.

Phish•ing

Usage: phish, v; phisher, n

the practice of luring unsuspecting Internet users to a fake Web site by using authentic looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack; the creation of a Web site replica for fooling unsuspecting Internet users into submitting personal or financial information or passwords.

No matter how careful you are, regardless of what virus protection you buy, you will always be at risk without the proper anti-spyware tools to protect you. How do you know if you have been infected? If the Start page in your Web browser keeps changing by itself, if your computer starts crashing more often than usual, or if you have tried to uninstall unfamiliar programs only to find they are still there after you restart your computer, then you are infected. Spyware can be pretty malicious.

Keyloggers watch your every keystroke and mouse click, then records your passwords, log-ons, and account numbers. You might think you don't need to read this column because you've taken steps to protect yourself. Well, if you have all the most current antivirus software, have installed Service Pack 2 for Windows XP, and have a very powerful firewall to protect you, then you would be WRONG! The fact is that all of these items do absolutely nothing to protect your computer from spyware at all, leaving you completely vulnerable to attack. Also, you know all those updates that Microsoft Windows XP installs? None of them protect you from spyware writers, who exploit ways to transparently install spyware through your Internet Explorer browser. These programs can even prevent Service Pack 2 from installing correctly. Once these programs infect you, your computer becomes very slow, because all your computer processing power is eaten up by the spyware itself. Don't allow yourself to be lulled into a false sense of security from any one anti-spyware program that claims to provide total protection - it doesn't exist.

Spam is the most virulent form of abuse that any Internet user must endure. The problem is so common that most people find they are forced to change their e-mail address just to avoid getting junk e-mail. Unfortunately, changing your e-mail is worse than changing your phone number because nobody knows how to contact you.

Microsoft Outlook

EUDORA

Microsoft Outlook 2003 and Eudora 6 are two of the major programs that have the ability to filter incoming e-mail as messages are received. If a message is believed to be spam, the message is filtered to the spam folder for later review.

Many mail servers running on UNIX machines run a program called Spam Assassin(www.spamassassin.org) which separates messages that contain potentially unsafe attachments, match keywords representing spam or rejects messages from known spamming addresses.

Internet phishing (pronounced “fishing”) is when a hacker sends you an e-mail falsely claiming to be an established legitimate enterprise. The idea is to try to scam you into surrendering private information that will be used to steal your identity. This e-mail asks you to visit a Web site where you are asked to update your personal information, such as passwords, credit card numbers, Social Security number, and bank account numbers information that the legitimate organization already has. The scam is that this Web site is bogus and is set up only to steal your confidential information.

You must be careful whenever you receive an email from what appears to be a trusted company. Hackers are very good at writing convincing letters that appear to be genuine. You must never ever click on a link in one of these e-mails, because even though it might look authentic, it almost always is not. It is very simple matter for a hyperlink to show one Web site and send you somewhere completely different when you click on it. These links are designed to take you to the hacker’s site. Don’t even cut and paste these links into your browser, because the hidden information in the URL takes you directly to the hacker instead of where you intended to go. When you need to go to a Web site, open a new browser window and type in the address by hand. That’s the only way you can be sure. So, if you somehow find yourself on a Web site and you just aren’t certain if it is from the hacker or not, what can you do? Well, here is a good tip. If the site asks you for personal information, just type in any random set of information. If the site says you have entered invalid information, then at least you have a good clue that it is most likely authentic. However, if the Web site lets you type in any random information and comes back to tell your information has been updated, then the site is almost certainly from a hacker designed to capture anyone’s information (no matter what they type).

https:// That “S” means “secure”

Another telltale sign of phishing is when e-mails are not addressed to you specifically by name but instead say, “Dear Customer.” If an e-mail doesn’t take the time to address you by name, something is wrong! When you receive an e-mail, ask yourself, “Why am I receiving this note?” If you are unsure, call the company directly and ask. Never assume an e-mail is authentic just because it looks like it came from a trusted company. Hackers easily spoof the “from” field of an e-mail to make it appear it is a legitimate correspondence. Never click on an attachment contained in an e-mail, because you never know what virus or spyware is lurking beneath the surface waiting to steal your private information and send it to the hacker world. It is important when you go onto a Web site to make certain the page begins with https:// That “S” means “secure,” and, if it is not there, anything you input can be intercepted by a hacker. One of the nasty tricks hackers use when trying to redirect you to a fraudulent site is to mimic the URL of the trusted site. For example, you might want to go to mycard.citibank.com, but the hacker site might say something like mycard.citibank.com@216.45.54.303 where that @ symbol means you are connected to a hacker’s

Web site pretending to be your credit card.

Hackers are very good at what they do. Sometimes you can take every precaution and still find yourself in trouble, not knowing if you are giving your information to a hacker. The best protection is your own vigilance. Don't click, don't open unless you feel confident about the sender.

Source : http://www.geeks.com/techtips/2005/techtips-NOV17-05.htm