

Is It Still Identity Theft?

By Elaine Bryskar, MCSE, MCT, A+ Certified

If you give away your own secrets, is it still identity theft? The question is posed in *Safe Computing, Unsafe PCs*, an article in the March 2, 2004 issue of PC Magazine, and is something worth our consideration.

While you may think you are well protected, the 12/14/04 issue of PC Magazine reported on a recent study from the National Cyber Security Alliance and America Online (available at staysafeonline.info), "70% of those surveyed thought they were either 'very safe' or 'somewhat safe' from online threats." Where do you fit on the "safety" scale?

In this issue, we will discuss two techniques for stealing information. In point of fact, there are a number of ways someone can steal information about you. Many examples can be found in the documents noted in last month's article.

First example: a Trojan can contain code to open ports on your system. Spyware can then steal your keystrokes, including passwords and user ids, unbeknownst to you.

All computers have ports; they are created by your operating system. Think of them as phone connections used by your programs (including spyware programs), to communicate with software on your and other systems. When you use your browser to access the Internet, your browser is using port 80 to communicate with another computer through its port 80, and visa versa. There are a total of 65,356 ports available on all computers. However, they can be closed via a firewall for added protection. Spyware, in many instances, uses infrequently used open ports.

Microsoft offers a tool (netstat) to review YOUR ports. However, another tool called **fport**, giving more information and also free, can be found at www.foundstone.com. This tool, when run at the command prompt, will tell you what ports you have open, the pathname of the programs which open the ports, and which processes (a number assigned by the OS) are controlling them. Think of the process as the pipeline connecting the program to the port.

Closing ports, as with any technical subject regarding your computer, requires good information. In addition to closing ports, purging your system of unwanted spyware may require several steps. Safe procedures can be learned from research, a good firewall, and/or assistance from a technical consultant.

Another technique for stealing your identity is called spoofing. Spoofing may occur because of a phishing (pronounced fishing) attack, in which you are sent an email that either contains a link or an embedded web page that looks like a legitimate or a trusted source on the Web. The intent is to get you to click on the link or fill in a form, responding to a query using your personal information. The link or web page then redirects you, not to the legitimate site but to a fraudulent (spoofed) look-alike site.

Once you have clicked on a link, there are several ways to identify the actual address of the website in your browser. The first one is simply to look at the address bar to see if the address looks legitimate. For example, in the following address, <http://www.paypal.com@spiesrealdomain.com/index.html>, Paypal is spoofed. The real address appears after the @ symbol. Therefore, clicking on the link would cause you to be redirected to a third party site (*spiesrealdomain.com*).

A second way to verify if the site is legitimate is to select the *File* menu and the *Properties* command. The Address information will reveal the true address of the Web page shown in the browser, whatever the address bar says.

There are several ways to avoid problems: accept email only in text format and never click on a link of which you are suspicious. Turn off the HTML feature. Web pages embedded in email can only be displayed if the HTML feature is active. This change also has the added benefit of not allowing malicious code to be transmitted to your computer via HTML email.

Of course, if you are curious, you can always type the address of the actual trusted site into the browser and see whether the trusted site mentions the email you received.

It is worth repeating. Don't become complacent.

Elaine Bryskar is a computer consultant and teacher interested in computer security and privacy. You may email questions and article suggestions to computersecure2000@yahoo.com or call 951.672.2799.