

Of Virii, Trojan Horses, and Adware... Who's Lookin' at YOU, Kid?

Greetings, NSDCAR members!

The following is an excerpt from "AETalk", an Internet Crusade listserv, provided and monitored by the ubiquitous Saul Klein and Mike Barnett. The information was of such a timely and important nature, that I thought I'd include it here, along with some additional information that will, hopefully, enlighten many of you and trigger a little reassessment of your current practices with regard to virus prevention and email usage. Here's the quote from Saul:

Today's viruses have the ability to "spoof" the "From" and "Subject" fields of an e-mail message, which prevents you from knowing who really sent you the virus or the content of the e-mail.

Familiar names are now a dangerous decoy, luring you into a false sense of security and tempting you to open infected e-mail. Be careful and keep your virus protection software updated with the latest virus definitions. I try to update daily (it takes only seconds) and have my Norton Anti-virus software set to run automatic updates (instead of asking me if I want to update).

Run a complete virus scan if you ever suspect that you have a virus. I have my computer set to scan on a regular basis.

It might be a good idea to inform your clients of the above so they don't someday think you sent them a virus.

If your e-mail address is in the e-mail address books of others, there is a good chance that someday your e-mail address will appear in the "From" field of an infected e-mail and some of the recipients who do not understand the nature of today's e-mail viruses will think you sent them a virus.

Saul's succinct and accurate description of the "spoofing" phenomenon is, as usual, right on the money. There are, however, many new and much more pernicious methods being used to compromise your computer and gather information about you, without your knowledge, and there are easy and quick solutions to most of them, if one knows where to look.

When is a virus NOT a virus?

Today's crop of "viruses", as we're used to referring to them, are, in many cases, not viruses at all, but rather "Trojan Horse" or "Backdoor" programs, sent to us in the form of web page programming snippets, email attachments, or even legitimate files shared with us by our business contacts.

For instance, if you receive email advertising something you're interested in, like a new marketing technique, or real estate websites at unbeatable prices, you're curious. You might open the email even though you don't know the sender. Or, as in Saul's example above, it *seems* to be coming from a company or contact you're familiar with, or perhaps someone you've corresponded with, in the past. So, you click to open, and a bit of HTML code, (the language used to write web pages all over the internet), executes an instruction on your computer to drop a file in the Windows folder. This file, in and of itself, is harmless; however, it's carrying a payload that immediately begins to run on your machine. First, the program searches for shared hard disks on

your computer, or perhaps looks for user accounts and passwords. Later, it may access your email program's address book, and begin mailing itself to everyone listed there. At worst, it may disable or corrupt your computer's operating system files, and render your PC useless at the next attempted power-up.

The Consequences of Virtual Free Enterprise

As if these examples of "malware" or malicious programming were not enough, there's yet another flavor that's probably running, in unbelievably large numbers, on your PC right now... the stuff called, "Adware", or "SpyWare". These are programs downloaded to your computer while visiting web pages, or from within malicious emails, that take over certain functions of your PC, and send information back to the person or company who deployed them. These little programs can perform functions as benign as logging all the websites you visit, to actually recording keystrokes and passwords, (and credit card numbers and social security account numbers), and sending them to the originator, giving them complete access to your personal and financial information. Almost all of these programs gather more information about you than you'd be comfortable sending to strangers, and the senders of these things are using that information on YOU!

Enough, already, I'm going back to pencils, typewriters and fax machines!

Now that we've identified some of the scary stuff out there... what the heck to we do about it? Well, Saul's advice was right on... ***get a good antivirus program, and pay the nominal subscription fee to keep it regularly updated.*** Set the software to download updates automatically whenever you're online. If you can't set this up, then hire someone who can. The hundred bucks you spend on a technician now might save you thousands later on, and will also help prevent you from being the cause of someone else's nightmare, as well. We all know someone we'd just love to send a virus to... chances are, we'll end up sending it to someone we love, respect, or rely upon for our livelihood... like our clients!

Quality Software at the (Most) Competitive Price!

In addition to your antivirus software, ***get a good "spyware" checker.*** The April 22nd issue of PC Magazine has an excellent article reviewing the best of these programs, and revealing that the "Editor's Choice" is a program called ***SpyBot Search & Destroy***, by PepiMK Software of Germany, which is actually free! You can download it from the Internet for free, and all the author asks is that you contribute any donation you care to send his way, and say a little prayer to whatever deity holds your devotion. This little program not only finds all the adware and spyware on your computer, but also inoculates your PC against future reinfestation. Spybot, too, updates itself automatically whenever you use the program, if you so choose, and is incredibly easy to install and use. I ran it on my home computer, and was shocked by the number of nasty little eavesdroppers residing in my little patch of cyberspace.

Know Your Computer, and What's Running on It!

A last little note... ***know what's normal and what's not, on your own computer.*** We all grow accustomed to turning on our computers and then turning our attention elsewhere, while it "boots up". When was the last time you reviewed all the little messages that pop up on your screen as the computer comes online? Do your kids have access to your PC? Have you browsed the web, lately? Then there's probably something running on your computer that you didn't ask for, don't want, and need to get rid of. Again, if your level of expertise won't allow you to address this stuff, then find a good support company and pay for a "check-up" every six months. Put it right in your budget, like auto insurance and oil changes for your car. Doing business on the World Wide Web doesn't have to be painful, but apathy and a fatalistic approach will guarantee it, sooner or later. And the consequences, unfortunately, affect hundreds of other people who come in contact with you, in cyberspace, every day. Be a mensch... take ownership of your cyber-security!