No. 136, April 2007 

THE COMPUTER CORNER

# No. 136. Protecting Your Computer

- by Stan Kaplan, WB9RQR
715 N. Dries Street
Saukville, WI 53080-1664
(262) 268-1949
skaplan@mcw.edu

What steps should you take to protect your computer? First, understand that this protection means freedom from malware of any kind (malware = malicious software designed to damage your machine or to infiltrate it without your informed consent). Perhaps even more important, what are the steps in order of importance? Here are my suggestions, and I suspect most knowledgeable computer gurus would agree with this order.

**1. USE WINDOWS UPDATE** (unless you run Linux, or some other non-Windows operating system). There is simply no more effective step you can take to protect yourself than by installing every security update available. You are leaving yourself open to trouble if you do not use Windows Update regularly, even if you take all the rest of the steps mentioned in this article! New updates are released regularly on every second Tuesday of the month, unless an unusual situation prompts Microsoft to release one sooner. The Windows Update site works very well, and actually saves you time. For example, when I build a new machine, I use the site to send me well over 50 updates for Windows 2000 and then it installs them all, with only a single reboot at the end. This is much, much faster than installing the updates individually. As I have said before, the Windows Update site is definitely one thing Microsoft got right.

a. BEST: Leave Automatic Updates on so they are downloaded and installed automatically. This is the best ploy because you don't have to remember to do it.
b. GOOD: Have Windows Update automatically download them, and you install them without delay.
c. Also Good: Have Windows Update notify you, and you download and install them without delay.

While you are at it, don't forget to update your copy of Microsoft Office. There are a bunch of security updates for that suite, too.

**2. GET BEHIND <u>BOTH</u> A HARDWARE AND SOFTWARE FIREWALL**. Even if you have only one computer, using a DSL or cable router (Linksys, D-Link, Netgear and the like) is a great way to add a layer of defense. If you get one from your high-speed service provider, add another one with multiple ports and plug your single computer into it. If you add another computer later, the box will protect all computers on your network, besides allowing you to share resources and the Internet. Routers are hardware firewalls that offer strong protection for everything connected. Just don't forget to change the router's default password to one you make up! Follow up the hardware firewall with a software firewall such as Zone Alarm (free at zonelabs.com) installed in each machine. Another one I hear is very good is Comodo Personal Firewall, but I am personally partial to Zone Alarm because they have been providing free firewalls to the computing public for many years, just because they thought it should be done. And, they did this long before they started selling Zone Alarm Pro. The free one is excellent and adequate.

**3. USE A VIRUS SCANNER.** But, use <u>just one</u> (installing more than one virus scanner can lead to big problems). Want a free one? A recent review showed AntiVir Classic V7 and Bitdefender 8 free to be among the best of the free scanners. I have recently installed a newly available free one to my own machine - AOL Active Virus Shield - which is based on Kaspersky Antivirus, said to be the best in the world at detection and repair. It seems very good, and does its work in the background, scanning only those files that changed since the initial scan. It also updates automatically, but only when the CPU is not burdened with other tasks. It is a terrific security tool that works quietly and efficiently in the background (I hate programs that interrupt your work just to tell you about a mundane task it is performing). Just

Google **AOL Active Virus Shield** to get it. They will ask for your email address so they can send you the key for installation.

You can even get an online scan free at several sites. They are listed alphabetically, but Kaspersky is likely to be the best at detection. On the other hand, the free on-line Kaspersky scan won't remove a virus, but the others will. Be sure to use IE when you request a scan; other browsers (Firefox) won't work.

a. BitDefender Online Scanner
b. F-Secure Online Scanner
c. Kaspersky Online Scanner
d. Panda Online Virus Scanner

If you want to pay for your virus scanner, Kaspersky Antivirus 6, NOD32 and F-Secure are said to be the world leaders in detection and removal. Stay away from home user bloatware. Unfortunately, Norton Antivirus/Systemworks/Internet Security uses huge amounts of system resources (memory and hard disk space) with unessential processes. Too bad Norton is so poor now; it was once a world leader. Another to avoid at all costs is McAfee. It is constantly urging you to buy more useless products, making it little more than an advertising gimmick. These products are difficult to uninstall, especially McAfee. Before I found out about specific removal tools, I had to completely reformat a brand new hard drive to get rid of "in your face" McAfee products that Dell had installed on a new computer. If you have either of these products, get rid of them. Use Google to search for Symantec removal tool or McAfee removal tool to find a way to do it cleanly.

4. **USE AT LEAST TWO SPYWARE SCANNERS.** Scan with two independent spyware scanners, not one, because there is no single scanner available that will catch every spyware intruder that is out there. BUT, let only one run in the background between scans, or they might conflict and cause problems. Spy Sweeper and Spyware Doctor are said to be the best "pay-for" scanners in this area. I personally use both Ad Aware and Spybot Search and Destroy religiously, both of which are free. Whenever there is a definition update, I download it on all my machines and run a full system scan on all. Sometimes one will detect a piece of spyware (such as a tracking cookie) that got through, sometimes the other. Using two works!

5. **USE YOUR HEAD.** If you surf to find freeware and shareware, stay away from sites you don't know are secure. Visit majorgeeks.com for a start, and feel free to go to any links they provide – they are safe and the best on the web. If you accidentally visit a pornography site, or even get a pornography email, expect your computer to get infected with something or other. Run both virus and spyware scans immediately afterwards. Block all ads, banners and 3rd party cookies in your browser, because malware can enter your machine this way. Keep your senses heightened, be skeptical, and don't trust what you read on the web. Browse smart! Happy computing!