

Why I'm glad to be a Mac User

reason number 89

Recently, computer pundit Kim Kommando published an article that reminded all Windows PC owners of the steps that they *must* take to protect their computers against attack by malicious viruses, worms, hackers, crackers and spyware. As you can see by her byline, Kommando wrote the article under the *aegis* of the Microsoft Small Business unit. So, what follows is official Microsoft policy for setting up a Windows PC.

You can read more Kim Kommando articles at her web site: <http://www.komando.com>

Many of the step-by-step instructions in the article are only applicable to Windows and cannot and need not be done on any Mac. I have removed some of these passages for the sake of brevity and to avoid confusion. The removed instructions are indicated with ellipses: . . . I have added a few of my own comments in **CCC red**.

Six steps to help secure your brand-new PC

By Kim Kommando, Microsoft Small Business

There's nothing like cracking open the box of a brand new computer. But don't be so quick to just connect it all up and hop right on the Internet.

According to the software security company Symantec, it takes only 20 minutes for an unpatched and unprotected [Windows] computer to be attacked once connected to the Internet.

In that time, your pristine computer could be turned into a zombie. Zombies are machines that have been secretly taken over by hackers. The zombie networks are leased to criminals who use them to send spam or attack Web sites. [see CCC News March, 2004]

Some criminals want to put keyloggers on your computer, to steal passwords, credit card numbers and other sensitive data. There are plenty of vandals out there, too, who want to destroy your data for fun. And advertising outfits, many shady, hope to put spyware on your [Windows] computer. With that, they will track your surfing and bury you with ads.

Compromised computers are found in homes, businesses and government offices. To make sure you aren't victimized, here are six steps

you must take to secure your [Windows] computer and the network on which it runs.

1. Install a firewall.

If you are running a network and sharing a broadband connection, you probably have a firewall built into the router.

But that's not enough. Most routers used in small businesses utilize a Network Address Translation (NAT) firewall. Basically, it hides all of the computers in the network. It protects you from outsiders trying to get in.

Windows XP's firewall works in a similar fashion. It's able to block incoming traffic but not outgoing data.

. . .

The most secure method is to have a third-party software firewall in addition to the firewall on your router. It provides an extra layer of protection by alerting you to outbound traffic. Anytime a program tries to access the Internet, the user will be alerted. If it's a valid application, such as Internet Explorer, Outlook, and so on, the user grants it access to the Internet. If it's an unknown application, such as a worm, you can block it. My favorite third-party firewall is ZoneAlarm, which is free.

You're not ready to go onto the Internet just yet, so download the firewall onto another computer, save it on disk and install.

Even if you're not using a broadband connection, you still should install a software firewall. Hackers are greedy. They will infect or take over any [Windows] computer [not Macs!]
— even ones with a slow Internet connection.

[Mac OS X comes with an excellent, built-in firewall (open the Sharing System Preference). Even so, it is an option, not a necessity. Mac OS 9 has no need of a firewall.]

2. Disable file sharing.

Before you go onto the Internet, disable file sharing. It's one thing to share your sales presentation with others in your office. It's another to share it with the entire Web community.

In Windows XP Professional, file sharing is turned on by default. [In Mac OS (all versions) file sharing is turned OFF by default.]

. . .

3. Install antivirus software.

This may seem as obvious as the others, but it's oh, so important. Many new [Windows] comput-

ers have a trial version of an antivirus program already installed on the computer. That doesn't mean it's ready to go. You still need to update the definition files.

To update the definition files, you'll need to access the Internet. Since you've turned off file sharing and installed a firewall, you should be safe. Remember that trial versions of antivirus software are only good for a short time, usually 30 to 90 days. The trial version will then continue to run on your computer, but its antivirus definitions will be out-of-date. Outdated definitions offer nothing but a false sense of security.

[There are NO, not even one, viruses that can attack Mac OS X. The few viruses that could strike Mac OS 9 (and earlier) are effectively extinct. No Mac user needs an anti-virus application. This may change in the future, but that would be an unlikely change.]

4. Modify your HOSTS file.

Setting up your HOSTS file will prevent spyware and any kind of "malware" (short for malicious software) from communicating outside your computer. This allows you to surf the Net anonymously.

Countless numbers of hackers, vandals or unscrupulous marketers would love to hijack your Web browser or give your [Windows] computer some nasty worm. Sometimes malware is bundled with shareware and freeware. Other times it can get on your [Windows] computer by opening an infected file.

"Tracking cookies" get on your [Windows] computer from Web sites and even online ads. They track your Web surfing habits

and report back. This helps the ad servers know which ads to place on your computer. . . .

[Attacks of this sort are completely unknown in the Mac World and, for all intents and purposes, impossible to create.]

5. Keep your Windows system updated.

Even if your computer comes with Windows XP Service Pack 2 (SP2) already installed, you still need to update Windows. Although SP2 contains a multitude of critical updates, more have become available since its release. . . .

[As you know, I strongly recommend against blindly installing updates. Updates are just as dangerous in the Windows world, but, for Windows users, not updating is even more dangerous. To not update opens Windows users to malicious attacks.]

6. Stop spyware before it takes root on your PC.

Spyware collects information about your interests and then uses that information to display advertising.

Take preventive measures by downloading and installing Spyware Blaster. It's a free program and prevents most spyware from being installed on your [Windows] computer.

Another program, Spybot Search and Destroy, prevents spyware and adware from being installed on your [Windows] computer by immunizing it. It also has the ability to remove adware already installed on your computer.

Spybot Search & Destroy also has a tool called TeaTimer. TeaTimer monitors

changes to specific keys in your registry. Whenever a change is detected, a pop-up will alert you and ask if you want to allow or deny the change. . . .

The makers of Spybot Search & Destroy recommend that you run SpywareBlaster in tandem with Spybot Search & Destroy.

[Spyware does not exist that can affect Mac OS (all versions). Mac OS is too well protected to make such software possible.]

Now that your [Windows] computer is locked down as much as possible, you should be safe to set up your e-mail account for the computer and surf the Net.

Take this time to check the other computers in the office. Make sure your Windows and Microsoft Office software are updated. Make sure antivirus programs are up-to-date. And check for spyware.

This may sound alarmist. But these security steps are very important. By setting up your computer properly, you can feel confident that your computers and network are as safe as possible.

You must admit that it feels really good not to have to worry about these dangers. We get to save the time, concern and expense that our Windows using friends waste. In the end we have more time for business, education and fun.

Of course, things can change. But, unless Apple does something really stupid with Mac OS, we will remain happily spared from the dangers of modern computer life.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

Like an
auto club
for your
computer.