

10 Quick Tips for Keeping Your Computer Safe

By Tim Shoemaker
Synectics, Inc.

It's becoming an almost daily occurrence. We see a business manager in a panic because they have just been infected by malware (spyware and/or viruses) or have somehow lost critical business data from their systems. They can't run their business effectively and they are losing time, money and customer good will. We are almost always able to help them get back on their feet, but wouldn't it have been better (and cheaper) if it hadn't happened in the first place? Here's the first installment of "10 Quick Tips For Keeping Your Computer Safe". Next month we will give you the remaining five tips, but this should keep you busy and a little safer until then.

1. Do your Windows updates.

Turn on the windows update feature on your system and download the security updates from Microsoft. This is one of your best defenses against spyware and viruses. You can get them at <http://update.microsoft.com/>. Let the website check your computer and install the recommended security and critical updates. This could take a long time with a dial-up connection, so over a lunch or after work are the best times. If you purchase a maintenance contract from a reputable computer consultant, this will be done for you as part of the monthly maintenance.

2. Establish a password for the administrator account.

Many Windows-based PCs ship with wide-open administrator access to the root directory. You never want anyone but you to have unrestricted access to the admin settings on your PC. Think of it as leaving the front door to your business wide open. When on the Internet, the average time to get infected is just **12 minutes** if you don't take precautions. The administrator account has complete access to your system and can wreak havoc with your data. Most malware will instantly take advantage of an unprotected administrator account. Having a password will slow them down. But mostly, it will make getting rid of the infection easier and less expensive. Sometimes, if the admin account is very severely infected, we have to reinstall the whole operating system. If the admin account is clean, we can usually just clean up the infected accounts. That is much less expensive and intrusive.

3. Give everyone their own user account.

This is equally as important as password protecting your administrator account. You do not want to be using your admin account for daily use. Instead, you should be using a user account that is rights limited and also password protected (a different password than the one you are using for the admin account). This adds another layer of protection for your system because a limited user account does not have the global access permissions like an admin account. This level of permissions restriction alone might thwart some malicious software.

4. Be proactive with maintenance.

Most people don't realize that the most expensive and critical component of their computer system is NOT the hardware or the software. It's your *data*. You can easily replace equipment. But if you lose your data, your business could grind to a halt. **Data is often worth more than 10 to 50 times the cost of the equipment.** Client data, financial data, payroll, receivables, and payables all are critical to running your business. A well thought out and implemented periodic maintenance program will save you money over the life of the equipment. Whether you do it yourself or purchase a support package, this will head off many problems before they even start. And the cheapest problem to have is having NO problem at all.

5. Install a software firewall.

Windows XP SP2 comes with a modest but useful software firewall. You should turn it on. If you have Windows 2000 or earlier you can install an alternative third-party software firewall like Zone Alarm. You can download a free version of Zone Alarm from their website at www.zonelabs.com. The free version is limited but still fairly effective against attacks. But even more important, it will tell you when something on your computer is trying to reach out to the Internet—possibly a malware program.

10 Quick Tips for Keeping Your Computer Safe (Part Deux)

By Tim Shoemaker
Synectics, Inc.

Well, here's the second half the list of things that you can do to keep your computer (and data) safe. I hope you have been implementing the first five tips and are starting to feel a little safer.

6. **Install an antivirus program.**

Install a good antivirus program and **KEEP IT UPDATED**. It does you no good if you don't have the current updates for the latest viruses. There are a number of good ones, just make sure you do the updates regularly to keep the virus databases current.

7. **Remove any unused or unneeded programs.**

If your computer is a big name brand, it usually contains lots of programs that were loaded by the manufacturer. These programs are usually time limited or cut down versions, intended to get you hooked on them so that you purchase the full versions when they time out. Most of these have no place on a business computer. Some even access the Internet without your knowledge when you first use them. But don't just delete their directory on the hard disk. That only causes problems. Remove all programs that don't serve a purpose in your business by clicking on Start | Control Panel | Add or Remove Programs and select the programs that you wish to remove. Just be sure that you really do want to remove them before deleting them for good.

8. **Don't let your kids play on your business computer.**

This one always amazes me. Otherwise intelligent business owners let their kids surf the Internet using their business systems. Usually, using their admin sign on or one with admin rights. Invariably, they get malware that either steals their data or trashes it. This is a great way to lose your data or have it stolen. Kid interest type sites are notorious for being malware broadcasters. Just say NO. Get your kids their own system and keep them off your business system. If you absolutely must let your little darlings use your business system, give them their own user account with very limited rights so that they cannot infect the whole machine.

9. **Establish a system restore point.**

Now that you have performed the first eight steps you should establish a system restore point. To manually create a Restore Point in Windows XP, for example, you launch the System Restore utility by clicking Start | All Programs | Accessories | System Tools | System Restore and then follow the steps in the wizard. This step will establish a fall back point if something happens to your system later. This can be a real lifesaver if you have a crash or malware infection.

10. **Install and configure a router.**

This last step may seem like an unnecessary added expense to many, but in this age of viruses, worms, and other nasty Internet infections, a router standing between you and the outside world offers another significant layer of protection. Connecting a PC directly to the Internet means that PC gets its own IP address, which means it can be seen by every sleazebag with malicious intent. By adding a router to your broadband setup, the router gets the visible IP address and gives your new PC a secret internal address. In addition, routers have hardware firewalls and other features that help block the bad guys before they can get to your PC.