

FOUR EASY STEPS TO PROTECT YOUR WINDOWS PC AND YOURSELF:



1. Update Your Operating System

No software is perfect. Unfortunately, when it comes to operating systems, there are security vulnerabilities that can be exploited. The good news: updating your operating system is relatively easy to accomplish.

For example, to update Microsoft® Windows™ operating system, either (1) go to <http://windowsupdate.microsoft.com> or (2) go to Internet Explorer™, click on "tools," then click on "Windows update" and follow the instructions. You should update Web browsers, such as Internet Explorer, as well.

2. Install & Update Virus Protection Software

With the prevalence of computer viruses, having virus protection on your machine is a MUST. Some virus protection software's offer automatic update, but only if you have a full-time Internet connection (DSL or cable). If you don't have full-time Internet or your virus protection software does not automatically update, then you need to update by following the software manufacturer's instructions.

3. Install & Update Spyware Protection Software

Spyware/adware exploit holes in browser security and install unwanted software on your computer that over time can slow down your computer. While most of these intrusions are just nuisances, many are actually gathering information on your Internet habits and transmitting it to a third party. A Web user is left with few options. Either you increase browser security settings and severely limit your use of the Internet or obtain a spyware protection program, such as "Spybot: Search and Destroy." For many reasons, obtaining a spyware program is a better idea. You might want to try using one of the alternate browsers (like FireFox-- <http://www.mozilla.org>) as they are not as frequently targeted by spyware.

4. Install a Personal Firewall

Most hacking dangers come from scripts run by individuals searching for a specific set of criteria--usually open ports on random computers that they can use later to launch attacks. The danger is magnified by computer users with DSL/cable or other "always on" connections, especially if they leave their computer on all the time. A personal firewall will help protect you. In most cases, a firewall will also allow the user to dictate which programs can and cannot access the Web.

The sad fact is that the more we use computers and the Internet, the more ways are going to be found for them to be used against us. The best way to fight back is to educate yourself and set up good computer protection habits. Update your operating system and your Internet browsers regularly. Add virus and spyware protection and be vigilant about keeping them updated. Add a firewall, especially if you use an "always on" connection.

Finally, if you use the Internet and have difficulty dealing with these four steps, I suggest you seek advice from family or friends because these *four* steps are crucial to safeguarding your computer from intrusions.