PC Security

If you ever connect your computer to the Internet, it's only a matter of time before something comes along to attack it. It would be risky enough to leave your computer open to attack if the only potential damage was to your own computer. But today's attackers can hijack your computer **without you ever knowing it** and use it to harm you and everyone with whom you communicate.

Why let malicious people injure you when you can protect yourself and others, and do it for free?

To protect your computer from attack, you need five kinds of protection: (1) from viruses, (2) from unauthorized access to your computer, (3) from spyware, (4) from flaws in the software that runs your computer, and (5) from your unwitting participation in others' attempts to harm you.

==========

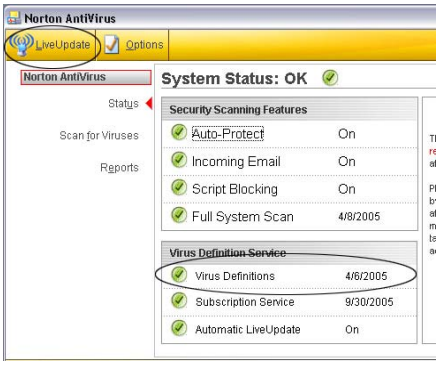
1. Protection from viruses: Anti-virus programs.

A computer **virus** is a computer program that "infects" your computer by making copies of itself, usually without your knowledge. Viruses can damage your hardware and your software. They can erase or corrupt your data. They can capture your data (credit-card numbers, love letters, tax returns, embarrassing photographs, etc.) and send it to other people.

To protect yourself against viruses, you must install, update, and run an anti-virus program. The most common anti-virus programs for sale are made by Norton (Symantec) and McAfee. There are many others made by TrendMicro, Computer Associates, Kaspersky, etc.

Go to http://www.symantec.com to find information about viruses and other threats, run a free online scan, and download removal tools for specific viruses.

Good free anti-virus programs are: Grisoft AVG at http://www.grisoft.com/us/us_dwnl_free.php. and Alwil Avast at http://www.asw.cz/i_idt_153.html. For a *PC World* review of free anti-virus software, see http://www.pcworld.com/howto/article/0,aid,113462,00.asp. Your internet provider (ISP) may offer a free antivirus program (but don't rely solely on an ISP filtering your email—you need protection for your computer).



Important! With any anti-virus program, you must update the virus definitions file often (even as often as every day) to keep the program current. Open your anti-virus program window and look for a button or link to click that says something about updating. Many anti-virus programs have automatic updating features, but you should still check and make sure that the updates are current.

Anti-virus programs vary in terms of ease of use and amount of information presented. Updates often involve paid subscriptions and sometimes it is necessary to obtain a new version of the program. If you are not satisfied with your anti-virus program, you should find one that better suits your needs.

2. Protection from unauthorized access: Firewalls.

A software **firewall** is a computer program that separates what's inside your computer from what's outside your computer. It gives you the power to decide what can get in and out.

To protect yourself from unauthorized access to your computer, you must install a software firewall. Currently, the best one is ZoneAlarm, which is available in a paid version and a free version. You can download either version at http://www.zonelabs.com.

The Windows firewall was greatly improved in the SP2 (Service Pack 2) update to Windows XP. If you're running an older version of Windows or do not have SP2, you shouldn't rely on the Windows Firewall. If you have SP2, you may choose between using the Windows Firewall and a third-party program like ZoneAlarm or Norton Personal Firewall. SP2 also adds a "Security Center" control panel that helps you govern security settings in Windows XP.

See http://www.pcworld.com/howto/article/0,aid,112920,00.asp for a *PC World* article on firewalls.

==========

3. Protection from spyware: Anti-spyware programs.

Spyware is the general name for computer code someone else installs on your computer—usually without your knowledge—to keep track of what you do online. Specific types of spyware are **adware**, which markets to you, either subtly or by bombarding you with ads; **foistware**, which is foisted onto you by web sites you visit; **malware**, which is designed to harm your computer; and **nuisanceware**, which may not do any harm, but is a pain to deal with.

To protect yourself from spyware, you must install an anti-spyware program. Two good free anti-spyware programs are: Ad-aware, which you can download at http://www.lavasoft.de/, and Spybot Search and Destroy, which you can download at http://safer-networking.org/.

See http://www.pcworld.com/reviews/article/0,aid,110654,pg,4,00.asp for a *PC World* article about anti-spyware programs.

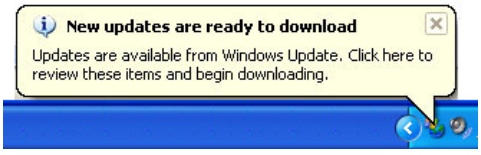
Remember: You'll need to update your anti-spyware definitions to detect the latest threats.

==========

4. Protection from flaws in your Windows software: Windows Update.

Windows software is not perfect (!). Microsoft is constantly discovering security holes and releasing patches/updates to fix them.

To protect yourself from flaws in your system software, you need to run Window Update regularly to download the latest patches for your software. Go to http://windowsupdate.microsoft.com. If your computer has automatic updates enabled for Windows, you may see a notification appear by the clock when updates are available or have been downloaded. Do not ignore these notifications; click on the balloon or the update icon, and follow the directions from there.



5. Protection from shooting yourself in the foot.

Ignorance is not bliss. Your anti-virus software, firewall, and anti-spyware programs will protect you from outside threats, but not from the consequences of your own behavior. Some tips to make your computer safer:

- **Keep your anti-virus and anti-spyware definitions updated.**

  No excuses! Your security programs can't protect you from the newest, most damaging, threats if you don't let them learn what the threats are.

- **Disable e-mail preview windows.**

  Turn off the preview windows in Microsoft's Outlook and Outlook Express, which automatically open messages—and may inadvertently unleash a virus. Delete suspicious messages without previewing or opening them!

- "**Just say no" to web-based installers.**

  When you see a Security Warning box appear with a message like "Do you want to install and run [X]?" click **NO** unless you *know* the answer is yes. (A good rule of thumb in general.)

- **Take control of the cookies on your computer.**

  Cookies are tiny text files placed on your computer by the web sites you visit. When you visit a site and let it put cookies on your machine, the site will know about you on subsequent visits. That can be good, because cookies let sites "remember" you and your activities on the site; it can be bad because cookies allow sites to track your Internet usage. It's up to you to decide how much surveillance you'll tolerate. Everything you want to know and more: http://www.cookiecentral.com/

- **Create strong passwords/logons.**

  You'll need usernames and passwords to gain access to networks and some web sites. Keep your passwords "strong" and unique, especially the passwords that you use to access financial data. Don't use simple words found in a dictionary. Strong passwords use a combination of uppercase letters with lowercase letters and numbers. Sometimes you have the option of using special characters also. These passwords should also be changed periodically. Not all passwords need to be geared for the highest security. Ask yourself the question, "What's the worst that could happen if someone got access here?" when deciding the level of risk. If there is a high risk, then the password needs to be stronger and needs to be changed more often. Keeping track of passwords is a necessary evil. Some people use programs designed to document on the computer. For more information see *PC World*'s article on password security at http://www.pcworld.com/howto/article/0,aid,112042,00.asp.

- **Use secure sign-ins.**

  Some web sites, Yahoo for example, offer a link to a "secure sign-in" page. If you click the link, you'll be taken to an encrypted page, which makes it harder for someone else to capture what you type when you sign in. A secure web page will display a padlock icon in the browser's status bar, and the address will begin with "https" instead of "http."

- **Be wary of giving out personal information, especially financial information.**

  Protect your privacy! Give minimal information to web sites; check a site's privacy policy before you entrust it with any information, and NEVER provide financial information to a site you don't have good reason to trust. If you get an email that looks like it is from one of your financial institutions or from a company that you do business with, asking for personal information to be updated, beware! Some spammers use a technique called "phishing," sending bogus emails that look like legitimate correspondence, in an effort to con you into giving them your personal data.

- **Avoid downloading free peer-to-peer fileswapping programs.**

  When you download free programs from the Internet—Kazaa, for example—you often get much more than you bargained for: It may have you sharing your hard drive (and your processor) with the world. Read the fine print before you agree to any terms. Sometimes a "free" thing has its own price.

- **Make your teenagers and preteens aware of security issues.**

  Kids are dangerously fearless in their interactions with the Internet. It is not enough to make sure that your kids understand security and safety issues—or prohibit them from downloading or installing anything. It is not unrealistic or overly intrusive for parents to monitor their kid's activities online in order to protect their kid's curiosity. Asking for the password to be able to do so is not out of line and does not mean that a parent will read every bit of mail that may be safe and personal. Parents are supposed to protect their kids.

==========

I hope you find this information useful. I am happy to answer your questions, and provide you with more information on any of these topics. Do what you can to keep your computer safe, and know that you can count on me for help along the way.

—Eileen