

How to Keep Your Computer Safe

Do the Mandatory Computer Setup:

1. Use a Firewall

- For instructions on how to setup the Windows/Mac OSX built-in firewall, check out the Mandatory Computer Setup, step 1.

2. Update your Operating System

- For instructions on how to setup automatic updates for Windows/Mac OSX, check out the Mandatory Computer Setup, steps 2 and 4.

3. Use secure passwords

- Use a secure password to logon to your computer and for all of your online accounts (but not the same password!) For detailed instructions on how to setup a password to logon to your computer, check out the Mandatory Computer Setup, step 3.
- What is a secure password? There are a number of techniques for creating secure passwords, but the most important things to keep in mind:
 - Don't use dictionary words (in any language)
 - Combine letters, numbers and punctuation
 - Longer passwords are harder to crack
 - Don't use the same password for everything
- If you'd like some more information, read this article on Strong passwords from Microsoft (<http://www.microsoft.com/athome/security/privacy/password.msp>) or use the PCTools.com Secure Password Generator (<http://www.pctools.com/guides/password/>)

4. Install an AntiVirus application & set it to auto-update and auto-scan.

- Norton AntiVirus is available from the Columbia CUIT website, and instructions for installation & configuration are available here: <http://www.columbia.edu/acis/software/nav/>
- Even if you already have another version of Norton or McAfee, it is a good idea to switch to the Symantec Corporate Edition supplied by Columbia because it will never "expire" for as long as you have your computer.

5. Install AntiSpyware

- PestPatrol, SpyBot, and AdAware are all available on the Columbia CUIT website, with instructions for installation & configuration. PestPatrol is the most effective/easiest to use, but it's a good idea to have more than one (but only run one at a time.)
- For PestPatrol installation and configuration instructions, go here: <http://www.columbia.edu/acis/software/pestpatrol/>
For links to free downloads of SpyBot and AdAware, visit the Resnet site: <http://www.barnard.edu/resnet/downloads.html>

For extra security:

1. Download & install an alternative browser like Firefox or Opera

- Many malware "infections" install themselves by exploiting security holes in your web browser. Unfortunately, Internet Explorer has had a very bad track record with these kinds of security holes -- which is why we recommend that you choose a different default browser.
- To set Firefox as your default browser, after installing & opening Firefox, go to:
 - Windows XP: Tools > Options > Main, and then under "System Defaults," hit "Check Now" and set Firefox as your default browser.
 - Mac OS X: Firefox > Preferences > General, and then under "Default Browser," hit "Check Now" and set Firefox as your default browser.

2. Secure Internet Explorer

- Even if you use an alternate browser, you will have to use Internet Explorer when you

update windows (and maybe for some other sites). (And when you open IE, it may ask if you want it to be the default browser -- you don't.)

- Open IE and go to Tools > Internet Options > Security. Choose "Internet" as your zone and set the security level to "Medium-high" and click "OK" or "Apply." Now you will be asked whether you want ActiveX objects to be executed and whether you want software to be installed. Sites that you know for sure are safe can be moved to the "Trusted Zone" by going to Tools > Internet Options > Security. Choose "Trusted Sites" as your zone and click on "Sites" to see a list of your trusted sites. For example, you could add your credit card or bank website to this section if you are always prompted before entering those sites.
- If you are curious how "safe" your web browser is, you can run some tests on this site: <http://www.jasons-toolbox.com/BrowserSecurity/>

3. *Be careful what you download*

- Many "freeware" programs (AIM Triton, Weatherbug, IE Toolbars, Kazaa, BearShare etc) come with an enormous amount of bundled spyware that will slow down your system, spawn pop-up advertisements, or just plain crash your browser or even Windows itself.
- Peer-to-peer (P2P) programs like Kazaa, BearShare, Grokster, Imesh, and others are amongst the most notorious "dirty" programs. If you insist on using P2P software, there is a list of "clean" P2P clients listed on this site: <http://p2p.malwareremoval.com/>
- ** Note also that even if the P2P software you are using is "clean", the files shared on your P2P network could be infected. Do not open any files without being certain of what they are!

4. *Checkout your startup items*

- Whenever you boot your computer, a number of programs will startup with the operating system. Some of these programs are necessary (your antivirus and antispysware programs should always startup "at startup"), while others just slow things down (iTunes, AIM, Quicktime, RealOne, to name a few). There are two ways to stop these unnecessary programs from opening at startup, one is to change the program's preferences, and the other is to turn them off on the operating system level. If you can't find the preference to change a program's startup options, or you have a lot of programs to turn off, try this:
 - From the start menu, choose Run... and type in msconfig
 - Choose the Startup tab, where you will find a list of all of your startup items.
 - To stop a program from opening at startup, just uncheck it. But, be careful because if you uncheck a necessary startup, you could mess things up a bit. Here is a useful website with an explanation of startup items that will help you decide what to keep and what to disable: <http://www.sysinfo.org/startuplist.php>
 - When you are done click "OK" and restart your computer.

5. *Uninstall Suspicious and Unused programs from Add/Remove Programs*

- From the Start Menu, go to the Control Panel and choose "Add/Remove Programs". Now you can uninstall all of the programs you don't use anymore (or never did). If you have one of the "dirty" programs described in step 3, you might have unknowingly downloaded some adware. Now is your chance to get rid of it.

6. *Disable Windows Messaging Service*

- The Windows Messenger Service can be exploited by spammers and hackers to add annoying popups to your computer (even while you aren't surfing the internet) or to use your computer for their own purposes without your knowledge (or permission).
 - From the Start menu, choose the Control Panel.
 - Open Administrative Tools and choose Services.
 - Double-click Messenger and in the Startup type list, click Disabled.
 - Click Stop and then click OK.