

## Securing a Home PC

### Essential Items that everyone should do

1. Use a firewall – Turn on the Windows Firewall. It is free and included with Windows. Start/Settings/Control Panel/Windows Firewall. If you have a complete security suite like Symantec, use the firewall included in that suite.
2. Turn on Automatic Updates for Windows. Open Windows Security Center (Start/Settings/Security Center) Make sure Automatic Updates is on and pick a time to install updates. If you pick a time at night, you do not need to leave the computer on all night, it will update the next time it is turned on.
3. Install an Anti-Virus software package. AND MAKE SURE IT IS UPDATED REGULARLY! Microsoft is now providing their Microsoft Security Essentials anti-virus/anti-spyware for free to home users. [http://www.microsoft.com/Security\\_Essentials/](http://www.microsoft.com/Security_Essentials/) If you have purchased an AV software package, or if one was installed when you bought your computer, make sure you are paying for and receiving the updates. An outdated AV is worse than no AV!
4. Make sure that your AV is set to scan AND disinfect removable media. This is NOT the default on most AV products, including MS Security Essentials.
5. Use a Local Hosts file from a site like [www.mvps.org/winhelp2002/hosts.htm](http://www.mvps.org/winhelp2002/hosts.htm). This will keep your computer from being able to contact over 16,000 sites that distribute software called malware that can steal your personal information, user accounts and passwords. About ½ way down the page there is a folder icon with a link to download the hosts.zip file. Download that file, open it on your computer and extract the hosts file and mvps.bat files to your desktop and doubleclick the mvps.bat file. That is all there is to it.
6. Run Secunia Personal Software Inspector ([www.secunia.com](http://www.secunia.com)). It is free and it will tell you when you need to update your other software (Adobe Acrobat, Firefox, Java, Quicktime, RealPlayer, etc). There have been some significant vulnerabilities in all of these applications in the past 6 months.
7. Educate yourself on what Phishing is and don't become a victim. <http://www.microsoft.com/canada/athome/security/quiz/phishingbasics1.msp>
8. Don't click on links in e-mail, use a bookmark or retype the URL instead.
9. Don't give out your password to anyone, ever, for any reason, especially in an e-mail!!!!!! Real technical support people can change your password and tell YOU what it is. If your tech support people are asking for your password, kindly remind them that is a security breach and don't give them the information.
10. Never enter your password into a site that is not using HTTPS (look at the URL and make sure there is a lock in the lower right corner).

## Items that most should do as it adds significant layers of protection with no additional cost.

1. Install Firefox ([www.mozilla.com](http://www.mozilla.com)). It is free and will protect you from Active-X exploits that are specific to Internet Explorer. Internet Explorer is the most exploited browser, if you can avoid using it for daily browsing you will have a more secure system. (You must keep Firefox updated, too!)
2. Firefox has many extensions that can also help you protect your system. The following are highly recommended: NoScript and Adblock Plus. These extensions do disable some functionality on some websites, but they do this to stop your system from being infected without you knowing about it. You might have to change a few settings here and there to make some sites work correctly. (Tools/Add-ons/Get Extensions from within FireFox and then search for these extensions.)
3. Install McAfee Site Advisor ([www.siteadvisor.com](http://www.siteadvisor.com)). If you installed Firefox as recommended above, you will want to install both the Firefox version and the IE version so that you are alerted when you use either browser. Site Advisor will warn you of malicious sites when you are searching for sites using Google or other search engines. Just watch for the green check or the red X when searching.
4. Download Malwarebytes free version ([www.malwarebytes.com](http://www.malwarebytes.com)) and run it. This will detect and remove current malware on your system. The full version has some additional monitoring and real-time detection and removal capabilities.
5. Create an everyday account that you use that is NOT an administrator account and use it most of the time. You should not use the administrator account or an administrator-equivalent account unless you really need to.
6. Setup a Software Restriction Policy. We have a document describing how to do that at <http://www.more.net/pdfs/srp.pdf>. If you combine this with step 5, your system will be very secure.
7. If you choose to use IE, consider using SandboxIE <http://www.sandboxie.com/>. While not free, it can help secure IE by running it in a protected mode. If you are using 64-bit versions of XP, Vista or Windows7, SandboxIE might not be compatible. Read on their download site before installing.

## Our favorite tools (available at no additional cost).

**SecCheck from MyNetWatchman.com:** tells you what is running on your computer and helps determine what malware might be installed and causing problems.

**Virustotal.com:** site that allows you to upload suspicious files to tell you whether it is malware or a legitimate program.

**KeePass ([keepass.info](http://keepass.info)):** software that lets you keep track of all of the passwords you have.

**TrueCrypt ([truecrypt.org](http://truecrypt.org)):** software that lets you encrypt your valuable data

**HashTab ([beeblebrox.org](http://beeblebrox.org)):** Handy to verify the file you downloaded is really the same one that you think it is by adding a tab to the Properties section of Explorer or MyComputer.

Check out the October, 2008 web seminar at <http://www.more.net/content/2008-security-topics-archive> for more information. Tell all your friends and neighbors, this is one e-mail that could get forwarded to everyone in your address book. ☺