

Simple and easy ways to keep your computer safe and secure on the Internet

[Click here to view this topic in its original format](#)

Original formatted version can be found here:

<http://www.bleepingcomputer.com/tutorials/tutorial82.html>

Written by: **Bleeping Computer** On: Aug 17 2004, 12:33 AM

Simple and easy ways to keep your computer safe and secure on the Internet

It is a fact; the Internet is just not a safe place to connect your computer to. There are worms constantly scanning for vulnerable computers to infect, trojans disguised as helpful programs but actually install malicious ones, spyware that reports your activities back to their makers, and hijackers that take control of your web browser and browsing experience. For those people who have been the victim of one of these mentioned infections, removing them and getting your computer back in your control can be a daunting and frustrating experience. The purpose of this article is to teach you how to setup your computer in such a way that you minimize as much as possible the risks of contracting one of these infections. Each step is very easy to do and regardless of your computer experience you will have no trouble following along. It is also important to note that there is not one step listed below that is more important than the other. They are all equally important to keeping your computer safe and secure.

1. **Educate yourself and be smart about where you visit and what you click on** - Understanding how you can get infected and what to avoid when using the Internet will be the most important step in keeping your computer clean and secure. The majority of people who have infections on their machines were infected due to lack of knowledge and clicking on things that they should not. I will provide a list of actions under this step that you should not do:
 1. Do not open attachments from users that you do not know. This is one of the most effective ways for viruses to infect you. If you do not know the user, then simply do not open the email and delete it.
 2. Never open an attachment that is a .exe, .pif, .com, or .bat

unless you specifically know the file is clean. The majority of these are always bad!

3. If you visit a site and a popup appears saying that your computer is unsafe, ignore it! These are gimmicks that are used to make you click on the ad which then can potentially install unwanted malware. For an example of how these types of foistware can be installed on your computer, you should read this article: **Foistware, And how to avoid it.**

An excellent list that contains a list of antispware apps that should be avoided and a list of ones that are recommended can be found here: **Rogue/Suspect Anti-Spyware Products & Web Sites**

4. When a you go to a site and a popup occurs, many times they will make them look like a normal Windows message box in order to trick you into clicking on them. Instead just close them by clicking on the X.
 5. Do not visit porn sites! I know some of you may not be happy about this, but the reality is that the majority of spyware and browser hijackers are put on your computer through porn sites.
 6. Do not visit warez sites! Not only is pirated software illegal, but it is a breeding ground for malware.
 7. Do not visit crack sites! Many of the cracks include malware in them!
 8. If you use P2P software, make sure you are careful about what you open. Malware is all over the P2P networks.
 9. Read the license agreement for any software that you install. Many free downloads are offered with spyware and other programs that you DO NOT want on your computer. Reading the agreement may help you to spot them.
2. **Use an AntiVirus Software** - It is very important that your computer has an antivirus software running on your machine. By having an antivirus program running, files and emails will be scanned as you use them, download them, or open them. If a virus is found in one of the items you are about to use, the antivirus program will stop you from being able to run that program and therefore infect yourself.

See this link for a listing of some online/stand-alone antivirus programs:

Virus, Spyware, and Malware Protection and Removal Resources

3. **Update your AntiVirus Software** - There is no point running an antivirus program if you do not make sure it has all the latest updates available to it. If you do not update the software, it will not know about any new viruses, trojans, worms, etc that have been released into the wild since you installed the program. Then if a new infection appears in your computer, the antivirus program will not know that it is bad, and not alert you when you run it and become infected. Therefore it is imperative that you update your Antivirus software at least once a week (Even more if you wish) so that you are protected from all the latest threats.
4. **Install an Anti-Spyware Program** - Just as you installed and use an antivirus program, it is essential these days to use a Spyware protection and removal program. These programs can be used to scan your computer for spyware, dialers, browser hijackers, and other programs that are malicious in nature. The 4 program that we recommend are AVG Anti-Spyware, Spybot - Search and Destroy, and Ad-Aware, and Windows Defender.

A tutorial on using some of these programs can be found below:

Using Ad-aware to remove Spyware, Malware, & Hijackers from Your Computer

Using Spybot - Search & Destroy to remove Spyware , Malware, and Hijackers

5. **Commercial Spyware Removal/Protection Programs** - If you feel more comfortable installing a commercial Spyware removal program then we recommend WebRoot's Spysweeper or Lavasoft's Ad-Aware Professional. Both are excellent products and a worthy addition to the arsenal of software protecting your computer.

Spysweeper Product Information

6. **Occasionally Run Online Virus Scans** - Unfortunately not all antivirus programs are created equal. Each program may find infections that other antivirus programs do not and vice-versa. It is therefore recommended that you occasionally run some free online antivirus scanners to make sure that you are not infected with items that your particular antivirus program does not know how to find. Two online scanners that we recommend are:

Kaspersky Web scanner

Trend Micro Housecall

Every once in a while, maybe once every 2 weeks, run one or both of these scanners to see if they find anything that may have been missed by your locally installed antivirus software.

7. **Visit Microsoft's Windows Update Site Frequently** - If you are a Windows users you must visit <http://www.windowsupdate.com> regularly. This site is a Microsoft site that will scan your computer for any patches or updates that are missing from your computer. It will then provide a list of items that it can download and install for you. When visiting the site, if it asks if you would like to install the Windows Update software, allow it to do so and it should only ask you to do this once. When the site is loaded you should then allow it to check for new updates and download any that it finds. If it has you reboot your computer, reboot and when your back at the desktop visit the site again and check for new updates. Repeat this process until there are zero critical updates available. This will ensure your computer has all of the latest security updates available installed on your computer and is secure from any known security holes.
8. **Visit the Apple Security Updates Site Frequently** - If you are an Apple user then you frequently check the **Apple Security Site** for any new updates and download them if they are available. Information on finding and downloading the latest updates can be found at the Apple security site that we linked to earlier in this step.
9. **Use a Firewall** - I can not stress how important it is that you use a Firewall on your computer. Without a firewall your computer is susceptible to being hacked and taken over. You may say "Why do I need a firewall?" I have all the latest updates for my programs and operating system, so nobody should be able to hack into my computer". Unfortunately that reasoning is not valid. Many times hackers discover new security holes in a software or operating system long before the software company does and therefore many people get hacked before a security patch is released. By using a firewall the majority of these security holes will not be accessible as the firewall will block the attempt.

For a tutorial on Firewall's and a listing of some available ones see the link below: **[Understanding and Using Firewall's](#)**

10. **Install SpywareBlaster** - Many known malicious programs are ActiveX programs that integrate into Internet Explorer. If you use Internet Explorer, then we recommend that you download and install SpywareBlaster. This program will load a huge list of known malicious programs into your computer's configuration and make it so that you can not run these programs on your computer and

therefore become infected.

A tutorial on installing & using this product can be found here:

Using SpywareBlaster to protect your computer from Spyware and Malware

11. **Update your security programs regularly** - As always if you do not update your programs, your programs will not be able to find the newest infections that may be racing around the Internet. It is therefore important that you upgrade the software and spyware/virus definitions for a particular program so that they are running the most effectively.

12. **Switch to another browser, like Firefox, or make your Internet Explorer more secure** - The latest version of Internet Explorer 7 is now shipped with much more secure settings. On the other hand, if you use Internet Explorer 6 there are settings that need to be changed. With that said you have two choices; either make Internet Explorer 6 more secure or switch to another browser like **Mozilla Firefox**. It's an excellent browser and is secure right after installing it. You can find more info on switching from Internet Explorer to Firefox here

Switching from Internet Explorer to Firefox

If you decide you would rather continue to use Internet Explorer, then follow these steps to make it more secure:

1. From within Internet Explorer click on the tools menu and then click on **Options**.
2. Click once on the **Security** tab
3. Click once on the **Internet** icon so it becomes highlighted.
4. Click once on the **Custom Level** button.
 1. Change the **Download signed ActiveX controls** to **Prompt**
 2. Change the **Download unsigned ActiveX controls** to **Disable**
 3. Change the **Initialize and script ActiveX controls not marked as safe** to **Disable**
 4. Change the **Installation of desktop items** to **Prompt**
 5. Change the **Launching programs and files in an IFRAME** to **Prompt**
 6. Change the **Navigate sub-frames across different domains** to **Prompt**
 7. When all these settings have been made, click on the **OK** button.
 8. If it prompts you as to whether or not you want to save the settings, press the **Yes** button.
5. Next press the **Apply** button and then the **OK** to exit the Internet Properties page.

By following all these steps you are sure to keep your computer at minimal risk to future infections or hack attempts. This is unfortunately not a fool proof method of securing your computer as new risks are released almost every day, but your susceptibility to these attacks will be diminished greatly.

--

Lawrence Abrams

Bleeping Computer Basic Internet Security Tutorial

[BleepingComputer.com: Computer Help & Tutorials for the beginning computer user.](#)