Title:
How To Keep Your Computer From Spreading Viruses

Word Count:
888

Summary:
There are some simple steps you must take to avoid becoming a victim of computer viruses and also stop from spreading viruses to others. Here are some things that you can and should do.
Email Issues to watch

Never open an E-mail with an attachment you were not expecting.

The latest batch of virus programs are often spread by E-mail. Even if your anti-virus program does not warn you about the attached file and even if the eMail appears to come from someone you know, do ...

Keywords:
antivirus software, norton antivirus, pccillin, anti virus, norton, virus, trojan horse

Article Body:
There are some simple steps you must take to avoid becoming a victim of computer viruses and also stop from spreading viruses to others. Here are some things that you can and should do.
Email Issues to watch

Never open an E-mail with an attachment you were not expecting.

The latest batch of virus programs are often spread by E-mail. Even if your anti-virus program does not warn you about the attached file and even if the eMail appears to come from someone you know, do not open it if you were not expecting it, and if you were expecting it, only open it AFTER scanning it with your up-to-date virus software.

Scan ALL incoming email attachments (regardless of who sent it).

Be sure to run each attachment you plan to open through the anti-virus check. Do this even if you recognize and trust the sender; malicious code, like Trojan horses, can slip into your system by appearing to be from a friendly source.

Turn off the 'automatic preview' in your email program.

Automatically previewing an email message has the exact same effect as opening and reading an email. My of the newest internet worms, trojans, and viruses simply need to have an email message read in order for them to be activated. Turning off the preview feature allows you to scan any email BEFORE you actually read it.

Disk Issues to watch

Don't boot from a floppy disk.

Floppies are one of the most common ways viruses are transmitted. If you are using a floppy while working on your computer, remove it when you shut the machine off or the computer will automatically try to boot from the floppy, perhaps launching any viruses on the disk.

Web Based Issues

Keep your web browser set to its highest security level.

Its a pain to get the warning messages on every other web page you visit, but its the best way to protect yourself - especially if you use Microsoft Internet Explorer and Outlook.

Don't download programs from the Web.

Unreliable sources such as Internet newsgroups or Web sites that you haven't heard of may be willing providers of viruses for your computer. Avoid downloading files you can't be sure are safe. This includes freeware, screensavers, games, and any other executable program - any files with an ".exe" or ".com" extension, such as "coolgame.exe." Check to see if the site has anti-virus software running on their side. If you do have to download from the Internet, be sure to scan each program before running it. Save all downloads to one folder, then run virus checks on everything in the folder before using it. Regardless of where you download from, ALWAYS scan downloaded software.

Routine Maintenance

Make regular back ups of important data

Make it a habit to back up all of your most important files at least once a month. Store the back up discs in a safe place.

Clean any virus/worm/trojan off your computer
(Details: http://www.antivirus-report.com/trojan-horse-removal.html )

Using your antivirus software, perform a full system scan of your PC, hopefully it will detect and remove the virus. If a virus was detected, restart your computer and run the full scan again. Sometime the virus will keep reappearing, due to the evolving nature of viruses. Symantec is particularly fast at providing removal tools should you ever get a virus or worm infesting your computer.

What is a removal tool? Well simply put it is a simple software that will scan your computer for infections, and then remove them from your machine. You most often need this if your machine got infected BEFORE you installed antivirus software.

Top Considerations for PC Protection

And the final and most important two things to do to keep your computer clean and make sure it does not spread viruses to other computers...

Install a Firewall

If you use a broadband/high-speed method to access the internet, you need to get a firewall. A firewall is a program that defends your computer from hackers who attempt to gain direct access to your computer over the Internet. There is a very good firewall program called ZoneAlarm that will do the trick if you use Windows.

Install and use a high-quality anti-virus program.

This is the key to protecting your computer. Buy one of the major anti-virus programs - Norton Anti-Virus, PC-Cillin, or McAfee Anti-Virus. The primary benefit of the commercial packages is the frequency and ease of updating the virus definition files that these programs use to detect viruses. With new viruses popping up all the time, unless your protection software is kept updated, you start to become ever more vulnerable to infection.

Get immediate protection.

Configure your anti-virus software to launch automatically on start-up and run at all times. This will provide you back-up protection in case you forget to scan an attachment, or decide not to. And in case you forget to load up your

anti-virus software, configuring it to start by itself will ensure you get immediate protection anyway. The top antivirus software programs all do this (but only if you have one installed on your computer). You do have current antivirus software installed right? If not, you can go to this page for more information on why you need antivirus software and how easy it is to use.