Title:
Securing Your Computer System

Word Count:
486

Summary:
Today, more and more people are using their computers for everything from communication to online banking and investing to shopping. As we do these things on a more regular basis, we open ourselves up to potential hackers, attackers and crackers. While some may be looking to phish your personal information and identity for resale, others simply just want to use your computer as a platform from which to attack other unknowing targets. Below are a few easy, cost-effective steps...

Keywords:
computer security, virus, trojan, worm, spyware

Article Body:
Today, more and more people are using their computers for everything from communication to online banking and investing to shopping. As we do these things on a more regular basis, we open ourselves up to potential hackers, attackers and crackers. While some may be looking to phish your personal information and identity for resale, others simply just want to use your computer as a platform from which to attack other unknowing targets. Below are a few easy, cost-effective steps you can take to make your computer more secure.

1. Always make backups of important information and store in a safe place separate from your computer.

2. Update and patch your operating system, web browser and software frequently. If you have a Windows operating system, start by going to www.windowsupdate.microsoft.com and running the update wizard. This program will help you find the latest patches for your Windows computer. Also go to www.officeupdate.microsoft.com to locate possible patches for your Office programs.

3. Install a firewall. Without a good firewall, viruses, worms, Trojans, malware and adware can all easily access your computer from the Internet. Consideration should be given to the benefits and differences between hardware and software based firewall programs.

4. Review your browser and email settings for optimum security. Why should you do this? Active-X and JavaScript are often used by hackers to plant malicious programs into your computers. While cookies are relatively harmless in terms of security concerns, they do still track your movements on the Internet to build a profile of you. At a minimum set your security setting for the “internet zone” to High, and your “trusted sites zone” to Medium Low.

5. Install antivirus software and set for automatic updates so that you receive the most current versions.

6. Do not open unknown email attachments. It is simply not enough that you may recognize the address from which it originates because many viruses can spread from a familiar address.

7. Do not run programs from unknown origins. Also, do not send these types of programs to friends and coworkers because they contain funny or amusing stories or jokes. They may contain a Trojans horse waiting to infect a computer.

8. Disable hidden filename extensions. By default, the Windows operating system is set to “hide file extensions for known file types”. Disable this option so that file extensions display in Windows. Some file extensions will, by default, continue to remain hidden, but you are more likely to see any unusual file extensions that do not belong.

9. Turn off your computer and disconnect from the network when not using the computer. A hacker can not attack your computer when you are disconnected from the network or the computer is off.

10. Consider making a boot disk on a floppy disk in case your computer is damaged or compromised by a malicious program. Obviously, you need to take this step before you experience a hostile breach of your system.