Title:
How To Secure Your PC, Software And Data

Word Count:
639

Summary:
The role of the personal computer has taken a whole new meaning ever since the introduction of the Internet. There are scores of Internet surfers who use the Internet from shopping to banking to investing and much more and the Internet today, is a buzzing, throbbing center of activity. But there's some bad news - the Internet is also swarming with quite a few elements from the dark side - and they are called hackers and phishers.

Hackers try to break into your computer to ...

Keywords:
GoToMyPC, GoToMeeting

Article Body:
The role of the personal computer has taken a whole new meaning ever since the introduction of the Internet. There are scores of Internet surfers who use the Internet from shopping to banking to investing and much more and the Internet today, is a buzzing, throbbing center of activity. But there's some bad news - the Internet is also swarming with quite a few elements from the dark side - and they are called hackers and phishers.

Hackers try to break into your computer to steal or corrupt your important data, while phishers try to obtain your personal identification using dubious methods. You have no choice but to protect your computer from these elements and here a few, easy, cost-effective steps you must take to make your computer almost as secure as Fort Knox:

1. Take a backup of important data regularly - preferably, daily. Buy another hard drive for the backup, but do not permanently plug it into your computer. The idea is to keep your backups away from your computer just in case it is hacked into.

2. Always update your operating system. All developers of operating systems (Windows, Apple OS and Linux) regularly release patches and updates when they discover holes in their programs. So, remember to keep the "automatic update"

feature on always. Microsoft Tip: Windows users can go to www.windowsupdate.microsoft.com and download the latest updates.

3. Your web browser (Internet Explorer, Opera, Mozilla Firefox, etc.) too must be updated for the same reasons stated above. All you have to do is visit the browser developer's homepage and download the latest version or update. If you are using the Microsoft Office Suite, then you must make it a point to visit www.officeupdate.microsoft.com and update it, as this software suite is a hacker's favorite.

4. Next, install a firewall on your computer. A firewall turns your computer invisible on the Internet and hackers, phishers, virus/Trojan developers, malware and adware cannot break into it. You can visit www.zonealarm.com and download a personal edition, which comes free. However, if your data security needs are critical, then you must consider investing in a 100% hack-proof firewall.

4. Hackers mostly employ Active-X and JavaScript for planting malicious programs into computers. Also, cookies are regularly planted on your computer to track your browsing preferences – but cookies are relatively harmless. To stay away from malicious programs, you need to tweak your web browser's security settings – Set your security setting for the “Internet zone” to High, and for your “trusted sites zone” to Medium-Low.

5. Now, you need virus protection and therefore, need to install anti-virus software. AVG anti-virus is free software that is updated regularly and you can download a personal edition by visiting its developer's website http://www.grisoft.com/.

6. Never ever open mail attachments that come from unknown sources. They are sure to contain a virus or a Trojan. Also, never run a program located at an unknown origin, on a website that does not have a security certificate – such programs will plant a Trojan on your system.

8. The Windows operating system is set to “hide file extensions for known file types”. Turning off this option will help you see files with unusual extensions – which, in all probability, will be viruses/Trojans/Keyloggers.

9. When you are working offline, disconnect your computer from the local area network. That way, a hacker will not be able to attack your computer.

10. Build a boot disk just in case a malicious program crashes your system.

11. Finally, you need to install an anti-spyware program. Ad-Aware SE Personal

is an award-winning tool that can help you detect and eliminate spyware effectively.

These are the basic steps required to secure your computer. Always remember to keep your anti-virus, anti-spyware and firewall programs up-to-date. So, use our guide and turn your computer into a virtual Fort Knox. Good Luck!