

10 steps to protect your PC before connecting to the Internet

The Internet provides a lot of useful knowledge for users, but it is also a source of spreading worms, viruses, trojans, spyware ...

The Internet provides a lot of useful knowledge for users, but it is also a source of spreading worms, viruses, trojans, spyware . Because of the very cause, your computer system will be a good bait. for them. Therefore, follow these steps before connecting to the Internet.

Step 1. Create a CD-ROM boot disk

Before accessing the Internet, stay a few minutes to create a boot disk using the CD-ROM drive containing the latest version of your favorite antivirus program.If you still want to keep it simple and free, then use AVG and Avast or other antivirus programs in the country also bring high efficiency as D32 and BKAV, the top antivirus software like Norton or MacAfee is too great great but they're a bit "heavy" in terms of price as well as storage capacity.

To save time, you should also include spyware removal tools like Spybot, and Adware.It is a good idea to include the latest driver updates for graphics cards, audio, etc. There are all hardware drivers in the CD-ROM drive.Because you do not need to connect to the Internet to install drivers for the PC.

Step 2. Remove unused software

The first thing to do is clean up your PC.It is recommended to remove all trial software or additional software that is not intended to be used.Because these trial software requires you to activate or register via Internet connection.In some cases, they automatically access the Internet without asking the user.Therefore, computers are also very susceptible to virus infection.To remove unwanted programs from the system.You just need to go to Control Panel-> Add / Remove Programs.Next, remove the trial software or unused software and restart the computer.

Step 3. Install antivirus software

Next, install anti-virus and anti-spyware software that you "burn" to CD-ROM in step 1.Then perform a full system scan to ensure that the system is clean and immune to viruses and spyware.Most anti-virus and anti-spyware software have the ability to automatically prevent the dangers and risks of infection.Turn on the automatic protection of spyware and viruses of these software.



Step 4. Install firewall software

In Windows XP SP2, a built-in freeware firewall software, Windows Firewall, was built in. If you want more features, just run 3rd party software like ZoneAlarm or SyGate. Firewall software should also be available on the CD-ROM set created in step 1. Please install the firewall software to protect your system.

Step 5. Install printers and other peripherals

Before you connect to the Internet, install the peripherals into the new PC. Because after you connect to the Internet, you only need to install peripheral devices, they will automatically connect to the Windows update page. They will automatically search for devices and make suggestions for upgrading new and appropriate drivers for each hardware. This is really good and useful for Windows, but it will probably be a weakness that hackers can take advantage of to get into your computer.

Step 6. Create strong passwords for administrator accounts (*Administrator*)

This is one of the weaknesses of security on Windows systems, the administrator account allows managing access to the entire system and is very dangerous. Hackers can steal system information, viruses, worms, trojans, spyware . can automatically install and infect the system when using an administrator account. You don't want anyone to have access to administrative rights for your PC. And in most passwords can easily be "cracked" by qualified hackers.

Step 7. Create restricted user accounts, and use secure passwords

This is as important as protecting the administrator account password. For daily use, you don't want to use an administrator account. Instead, you want to use a restricted account and have a password to protect (this password must be different from the administrator's password and must also be strong, not easy to guess). It is because of this limited download that your computer will resist infection or installation from malicious software due to restrictions on access.

Step 8. Turn off unnecessary Windows services

Microsoft tried to turn off some unnecessary services in SP2, but there are still some unnecessary services that still work by default on PCs. If you want to see how many services are in use, just use *Task Manager* (CTRL + ALT + DEL) and click the *Processes tab*. Most applications, services and processes operating in the background will be displayed. The problem here is that most external attacks use and exploit vulnerabilities from these services. Turn off these unnecessary services to save system resources and prevent remote attacks.

Step 9. Set up a restore point

If you have completed the above 8 steps, perform a restore point using the System Restore utility. To create a Restore Point, you need to run System Restore by clicking *Start / All Programs / Accessories / System Tools / System Restore* and follow the wizard. This step is really important because at this time your system is still "clean", so if the system is later infected with viruses, worms, trojans or damaged, this recovery point is really a lifeline for your PC.

Step 10. Install and configure the Router

This is the last and seemingly unnecessary step that requires additional investment. But in a time when viruses, worms, trojans are releasing power on the Internet, the router setting separating the boundaries between you and the outside world is really necessary. Connecting a PC directly to the Internet means that the PC will have a private IP address, and this may affect the computer system. But installing additional routers when connecting to broadband, the router will take that real IP address and give the new PC an IP address in the LAN. Furthermore, a router with a hardware firewall prevents intrusion. Therefore, using a router or ADSL modem with built-in router is a safe and inexpensive solution.

You finished reading the article "**10 steps to protect your PC before connecting to the Internet**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.