

Protect your computer from viruses and spyware

Today, as more and more computers are connected to the Internet, the risk of infection with viruses, spyware, Trojans, and so on is increasing with the rapid spread.

Today, as more and more computers are connected to the Internet, the risk of infection with viruses, spyware, Trojans, and so on is increasing with the rapid spread. Therefore, users should perform some of the following measures to protect themselves from Internet threats.

1. Install an effective anti-virus software

Many computer users trust that free antivirus applications can protect their devices against viruses or spyware. However, these free programs will not provide a full protection for the increasing risks every day.

Therefore, PC users should install more professional and professional antivirus software on their computers. Professional antivirus programs will be updated daily to combat new threats to attack the vulnerabilities of software and operating systems. Amongst these anti-virus, the most common ones are Kaspersky Anti-Virus v9.0, Symantec AntiVirus Corporate Edition, .

2. Install real-time antispware software

It is a mistake that many computer users think that an anti-virus program is always available to protect their device from spyware and adware. Others think, free antispware applications combined with an antivirus software will provide full protection for the device.

Unfortunately, most free anti-spyware programs do not provide real-time device protection against Trojans and spyware. Some free programs may detect the risk of spyware infection when they infect the device. Meanwhile, the professional antispware program will prevent the infection and delete these threats from the beginning.

3. Ensure the anti-malware program is always active



Antivirus and anti-spyware programs require regular data updates and registration. If not updated, malicious programs will not be able to protect the computer against new attack threats. Many attacks take place in a short time but have the power to infect 100-300 thousand websites every day. Therefore, users should regularly update the software to remove viruses and spyware as well as pay attention to the time of registration expiration of this software.

4. Perform daily computer scans

Sometimes, viruses and spyware get out of control of protection software and infect devices. Therefore, daily system scanning will help detect and remove this infection germ from the computer.

5. Disable the autorun function

Many viruses attack the computer when external memory is connected to the computer via the autorun function. Therefore, users should turn off this function when connecting external hard drives, USB, network devices, .

To disable autorun functionality on Windows operating systems, users can perform the following steps:

- **Go to Start , Run type gpedit.msc then OK .**
- **In the Group Policy window, double-click Administrative Templates , select System .**
- **In the right pane, double-click Turn Off Autoplay .**
- **Double-click Turn Off Autoplay , select Enabled . In the Turn Off Autoplay box, select All drives and click OK .**
- **Exit Group Policy.**
- **Restart the device**

6 . Disable image preview in Outlook

When email contains images infected with viruses and the Outlook application allows users to preview images in them, this is a way to boot the virus to infect users' PC systems. Therefore, to prevent automatic infection, users should turn off image preview in Outlook.

For new versions of Microsoft Outlook application there will be no automatic display of images. But if the user changes the default security settings, then turn it off again. If you use Outlook 2007, users do the following to turn it off: go to Tools | Trust Center , turn on Automatic Download and select Don't Download Pictures Automatically Print HTML E-Mail Messages Or RSS .

7. Do not click on the links on the email or in the attachment

Users should never click on email attachments before using anti-malware applications for businesses to scan. Instead of clicking on the link attached to the email, users should visit these Web sites by opening a browser and typing the address of the page.

8. Surf the smart web

Many anti-malware applications for businesses will be integrated right in the web browser to help fight infections from the drive, or to filter attacks. This is to prevent users from getting stolen password, financial or sensitive data.

Users should not type any personal, financial or account information on unreliable websites. Also, do not open the email attachment links directly.

9. Use firewall hardware

When performing printer sharing, accessing network resources, . users can use firewall software. However, this software is not always able to resist countless attacks on Internet-connected devices. Therefore, to protect computers against viruses, worms, . in addition to software firewall users should use hardware devices - firewall.

You finished reading the article "**Protect your computer from viruses and spyware**" 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.