Avoid threats from the Internet

The Internet is always a threat to everyone who surfs the Internet, even for those who know and guard it. Therefore, whether a professional or a non-professional in the field of computing ...

The Internet is always a threat to everyone who surfs the Internet, even for those who know and guard it. Therefore, whether you are a professional or not in the field of computing, you need to equip yourself with some basic knowledge to protect yourself really safe when exploring the Internet. The following article will help you not take much time or spend any cost but still know all about the dangers from the Internet.

1. Information about the threat of the Internet

The concern about Internet threats is still spyware or **Virus** so you need to master all of their functions as follows:

*** Malware** (an acronym for malicious software which means malicious software: they exist and operate on your computer freely. Malware can be understood as malware and includes: viruses, spyware , keyloggers, and Trojans .

*** Spyware** (spyware): this is a type of spyware to gather information about users, including personal information and habits (websites you often visit). It also has the ability to activate ads and install other malware.

*** Virus:** is a type of malicious software that can replicate and infect other computers through a network or media (such as a flash drive). Viruses can do many harmful things to your computer, such as walking and using it for malicious purposes.

2. Three steps to make it safe to use the Internet

This tutorial will take you through three relatively simple steps to protect your computer while surfing the Internet:

Step 1: Install Mozilla Firefox

Installing Mozilla Firefox will help you browse faster on the Internet because this is a very specialized support software in the following areas:

*** Pop-up blocker:** perhaps this is the most annoying problem with ads and with Firefox it will help you avoid this trouble, will tell you whether to block a pop-up in case Come on.

*** Warning of unsafe websites:** if you go to an unreliable, or secured site, Firefox will prevent the downloading of information from these websites.

*** Integration with antivirus software:** Firefox works with resident antivirus programs to scan downloaded files that threaten computer safety.

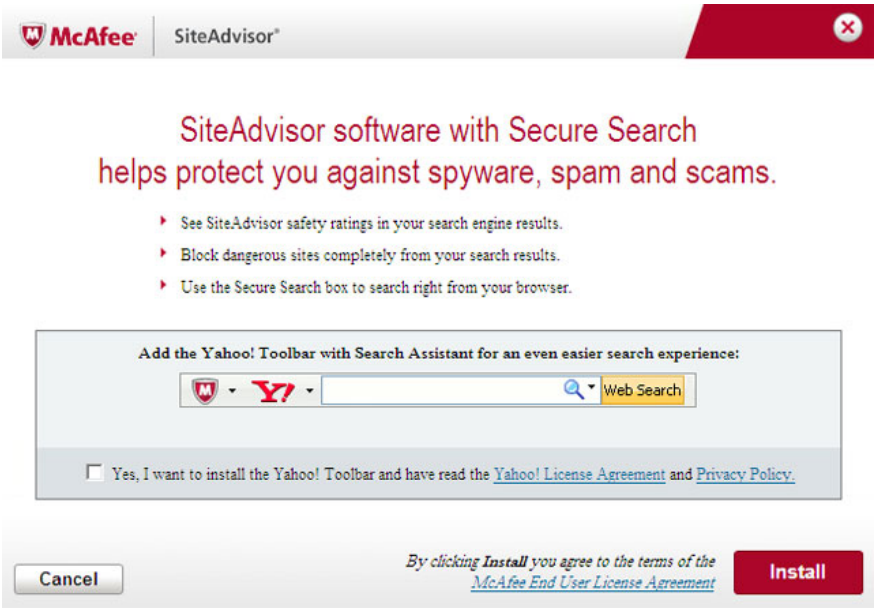
*** Automatic update:** Firefox automatically updates itself, so you don't need to care much about whether its version is too backward or not.

*** Private browsing:** Firefox often remembers the entire content of the web page you visit, but in private browsing mode it won't remember anything you did. This feature is very handy when logging into important websites that you don't want to leave traces on your computer (or someone else's). Firefox has a very small capacity of only 8MB, usually you use the Internet Explorer utility with very limited functionality, so install and use Firefox to get and adapt to the above convenience.

Step 2: Install McAfee Site Advisor tool

Many phishing websites are designed to steal your personal information, **McAfee** is a computer security company, there is a website consulting tool displayed next to the links in search engines. (such as Google and Yahoo), showing whether or not the safe listing sites are **McAfee Site Advisor** , which is a tool to advise and work with both Mozilla Firefox and Internet Explorer to prevent malware infection. harm from your computer to another computer. Simply download and install McAfee Site Advisor using the default settings.

After installing, restart Firefox and experiment with this tool, in the upper right next to the search box, click on the down arrow and select **McAfee Secure** . Now when searching and when the results are available, it is easy to see if those utilities are safe.



Each link has a small icon next to it, green means good; yellow is a warning; red means unsafe, unreliable; The question mark indicates that the website has not been scanned. So you should just click on the green icons for safe use.

Step 3: Change online habits

The biggest and only danger you face on the Internet is your own routine. Specifically, more information is posted online almost anyone can see, among them secure websites can be hacked. Even limited sites like Facebook, you can still access and copy information when you are still unsure completely safe. The key point here is that you need to be careful with yourself on the Internet and overcome some habits like:

*** Connect to a wireless network:** any Wi-Fi is provided free of charge in certain Net stores or cafes, which may not be cost-effective but are not really safe. Because an unsecured connection is an open network that allows anyone to connect information transmitted from your laptop to a wireless router and vice versa can be blocked by people with the right tools. because it is not encrypted. In addition, network attacks can be performed from other computers connected to the network.

*** Access secure websites in public places:** Even on a secured network, remember that people can see what you type on your laptop screen with just a phone camera. The same is true in the office, if one of the colleagues is curious to create a spy administration network on the workstation so that all your login passwords become volatile, it is very intense. So the safest website access is when you're at home.

*** Save personal information on shopping sites:** Most shopping sites provide address information for easier inspection. So it becomes a bridge for many Internet dangers, you should not save information on every shopping site. Although the information is believed to be secure, hacks can attack and steal data at any time. In particular, the more you should not save credit card numbers on shopping sites.

*** Do not post personal information** on social networking sites like Facebook .

*** Create personal computers:** Internet Explorer and Mozilla Firefox browsers make it easy to store passwords and information (such as names and addresses used in orders). Anyone who opens a web browser on your computer can check your browsing history. So you need to avoid storing passwords on websites or passwords that protect your computer and lock it when not in use (press **Windows** and **L** keys to lock your computer). Create a second account on your computer for others to use so that your information is stored separately, and make sure that the account is password protected, never save the password on the computer you share.

*** Do not install the software** you are not clear and minimize the installation of software.

*** Note:** Your online safety guarantee is 10% dependent on others and up to 90% depends on you. In short, the majority of risk factors can be controlled through simple steps outlined in this article. Controlling the online environment with a secure web browser has to say Mozilla Firefox has many advantages, it prevents you from going to malicious websites, scanning the files you download, blocking pop-ups, and Help protect personal data. Links in search engines can be dangerous. The **McAfee Site Advisor** tool helps identify links that are safe and vice versa, information that tells you about a site before you click to select it.

These simple tips hope to help protect you from most online threats and adjust your Internet online habits.