Ten free ways to keep your computer safe

You do not have to use the risk to protect your computer from viruses, trojans, phishers, scammer or snoop. And in fact, you don't have to lose a penny.

You do not have to use the risk to protect your computer from viruses, trojans, phishers, scammer or snoop. And in fact, you don't have to lose a penny.

From the moment you turn on until you turn off, your computer is always at risk of being attacked. Hackers try to break it; viruses, trojans and worms try to infiltrate the machine; And spyware tries to understand what you're doing. Then there are the dangers of wireless networks and the worst is the peering of colleagues.

What should you do? You can spend hundreds, hundreds of dollars for software and services, in addition to countless time just to keep your beloved device safe. We will show you ten simple steps to protect your computer without losing a dime.

10 free ways to keep your computer safe 1. Use free anti-spyware and anti-spyware software
2. Check online safety
3. Use free wireless network protection software
4. Use a firewall
5. Data encryption
6. Protect yourself from phishers
7. Disable file sharing
8. Surf the web anonymously
9. Say no to Cookie
10. Protect yourself against the "Nigerian Scams" risk on eBay

1. Use free anti-virus and anti-spyware software

If you want to protect your computer against viruses, you may have to pay many times. **Antivirus vendors** are currently selling at the same annual fee. They are not only a price, so the final price you buy can be in the hundreds of dollars.

That's when you even know which program to use. Companies like McAfee and Symantec sell this way. However, there are actually two free antivirus programs with all the necessary features like those of the other giants. For example, the function always automatically prevents viruses at all times, scans for viruses and automatically updates to the latest version

A program is Grisoft's AVG Anti-Virus Free that includes an antispyware program. Both are free, non-commercial and for home personal computers.

The second most commonly used program is Avast 4, which is also free and non-commercial. Avast can even work with the beta version of Windows Vista, something that no antivirus program can do.

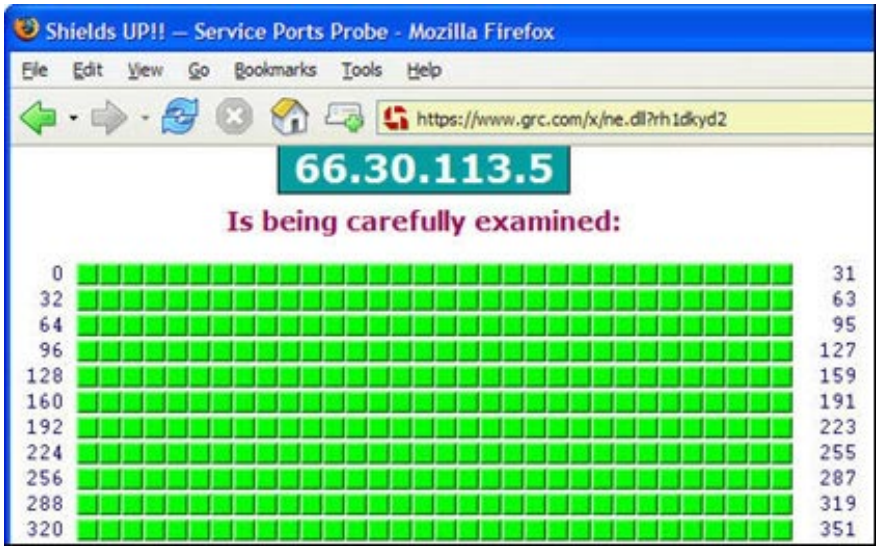
For antispyware, there are many free programs. In which Ad-Aware Personal and Spybot Search & Destroy are excellent choices. Both are protection programs like Microsoft's Windows Defender. Antispyware programs don't always catch the same type of malware. So you should scan your computer regularly with at least two programs at once.

Windows Defender protection program. The Software Explorer section shows all the programs running in your computer and allows you to exclude anything that could be mailware.

Check security and wireless network protection

2. Check online safety

How safe will you be when surfing the web? To know that, you can find free online safety inspection programs. Shields Up is the first choice you should take because it helps you know how to fight hackers, curious people and computer criminals on your computer. The program gives your computer meticulous analysis and a series of tests. For example, check Internet ports, see if your device is in 'stealth' mode (the safest mode), and whether it responds to the ping command (in the safest mode, it will not respond). It also provides instructions to shut down your computer if your computer is turned on by dangerous people.



Success! The green squares indicate that you have successfully prevented hackers, crackers, snooper

Symantec also offers an online safety checker program, but don't be surprised if you are often advised to buy its security software. Similarly, McAfee also has a free Wi-Fi scanner to check the safety of wireless connections. When trying to use McAfee's program, do not 'shock' if you are advised to buy McAfree Wireless Home Network Security to solve more problems. However, in addition to buying major brands' programs, you have many other options for protecting your computer.

3. Use free wireless network protection software

Most home networks are vulnerable to war crashes, which are vulnerabilities that allow hackers to infiltrate and destroy your wireless network. There are many ways you can do that with the router's settings to protect yourself.

But don't you want to go around with the MAC address filter, change the SSID (network name) or disable the SSID broadcast name? So you should use a free security program that can do those things for you. Network Magic is a good choice with two versions, free and paid. If all you want to do is reconfigure your wireless network with the highest level of security, the free version is enough.

After installation, it will check the router, the entire network and build a network map with all devices connected internally. It then checks the router's security settings and records what it finds. For example, if it detects that you are promoting your SSID, it will warn you. With just a click of the checkbox, Network Magic will stop promoting for you.

Network Magic will help you reconfigure your wireless router to the highest level of security.

The paid version has some additional features such as directory configuration and printer sharing, but if you're only interested in security, you don't need to use that version.

Free firewall and data encryption

4. Use a firewall

Using a firewall is simple, but it is the best way to help you fight Trojans, viruses, and worms. It can prevent hacker remote attacks, the penetration of computer worms.

If you use Windows XP Service Pack 2 then you have half the purpose you need. (If you haven't already, go to Windows Update to update).

By default after you install SP2, the firewall will be turned on. If you suspect it will suddenly turn off, you can click on the *Security Center* icon in the system tray to check, the *Security Center* screen will appear. (If the *Security Center* icon does not appear, go to *Control Panel -> Security Center*). Notice the top part of the *Security Center* screen (Firewall section) to make sure the firewall is turned on. If it is not enabled, click on the Windows Firewall icon at the bottom, select On -> OK. The firewall will be turned on.

At least make sure the firewall is turned on in Windows XP

But the built-in firewall in Windows XP only performs one-way protection programs, in other words it only blocks incoming connections without checking out the connections. Spyware and Trojans often perform 'phone home' sessions to create outbound connections from your computer without your knowledge. If you want to block outbound connections, you need a two-way firewall. The best free software you need is ZoneAlarm, which can be found on Zone Labs website. If you just need to find a two-way firewall, you don't need to buy a paid version because this version only adds some extra component features.

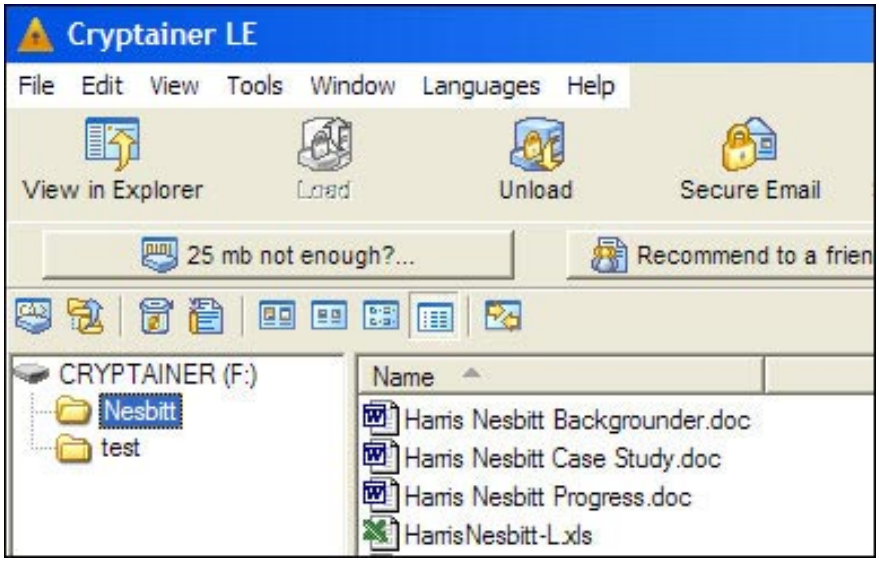
For older Windows users, there are not many compatible free anti-virus and spyware programs for them. ZoneAlarm does not support in Windows 98 or ME. So if you are using these operating systems, you will need to buy some firewalls like Symantec's Norton Personal Firewall or Trend Micro's PC-cillin Internet Security.

5. Data encryption

You have set up a mode to prevent others from accessing your computer, but it is not surprising if someone can access it and use it freely. It could be a hacker, or someone who is using the network with you or even a colleague sitting next to you when you go out.

So what solution for those problems? Data encryption is a fairly effective method. Most data encryption programs need to be paid. Moreover, it is not easy to use. But Cryptainer LE of Cypherix is ??simple and free. Install it and you will have a new encoder. It will create or transfer files to the disk and encode them in the blink of an eye. You can still work with them normally as with other files without using a password.

When you want any file or folder to be hidden from prying eyes, click on them, then click the Unload button in Cryptainer LE. They will naturally disappear. To have them appear again, click the Load button and type the password. Only those with passwords can see them.



Protect your data from prying eyes with the free Cryptainer LE software

This software is also very useful for those who use USB portable hard drive to store data. You can encrypt the entire drive. If you accidentally lose the drive, no one will see the file in it.

Protect your computer against phishing and security files

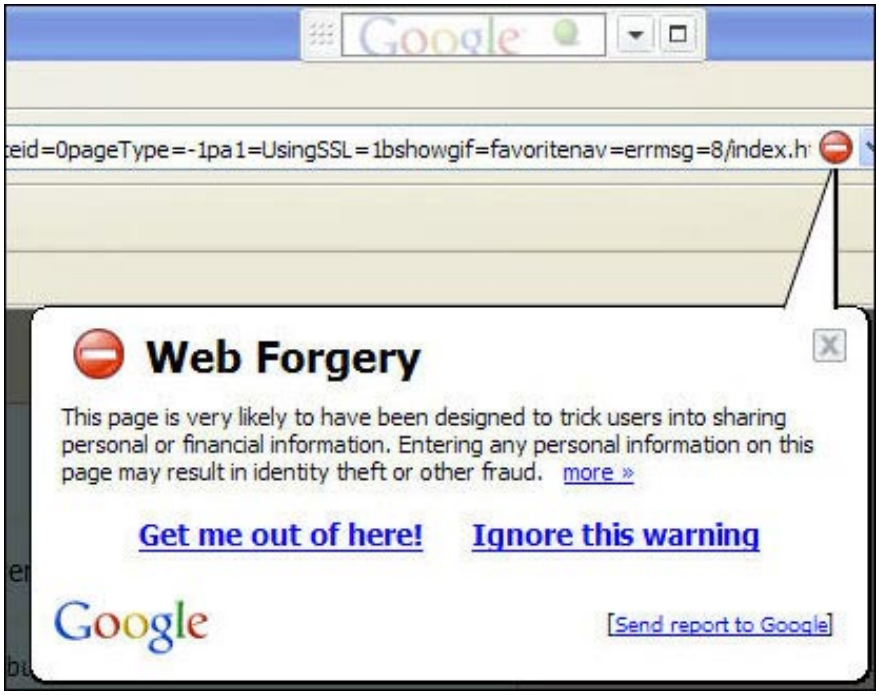
6. Protect yourself from phishers

Phishing is one of the most insidious and evil attacks. You are viewing a confirmation email from a bank, eBay, PayPal or other financial firms warning that you must click a link to log in to your account for some reason such as updating, checking good information even for protection purposes.

After the click is complete, you go to the website that you think is real but not (actually just like the interface). After logging in you may be asked to provide additional personal information such as a social security number and as a result you will have to 'bid farewell to your money'. Some scammer has sent an email and installed a fake website, using the personal information you entered to get all the accounts and steal your identity.

There are a few simple ways to prevent phishing attacks: Never click on a link from an e-mail sent by financial firms, eBay or PayPal. Don't worry about its legitimacy, instead go to the website and log in yourself.

Second, use an anti-phishing tool bar. It will block sites that have phishing that you visit or will warn if you are visiting a phishing website. You can use the Google Toolbar for example. After you install the toolbar, click the ' *Option* ' button. Then, under the ' *Browsing* ' tab, check the box next to ' *Safe Browsing* '. Click the ' *Save Browsing Settings* ' button and reconfigure the protection you want. Finally click on the ' *OK* ' button.



Don't come in here! Goolgle with anti-phishing components to protect you from phishing scammers

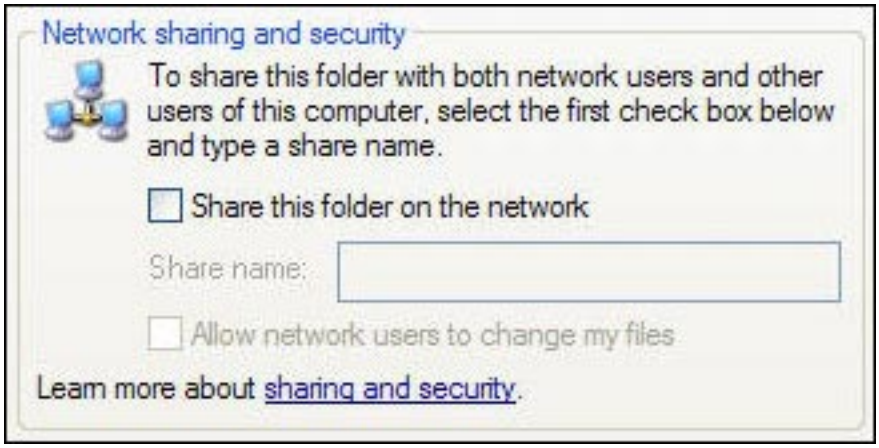
Another good anti-phishing tool is the Netcraft Toolbar with similar protection functions.

But soon you won't need any such toolbar. Because both Internet Explorer 7 and Firefox 2.0 will have anti-phishing functionality right in the browser. In preliminary tests, anti-phishing options in IE7 "caught" more phishing attacks than Firefox 2.0. But both products are only beta versions.

7. Disable file sharing

There is the greatest security risk you can get, but you don't know it, even if you don't even know what the threat is. That is the file and folder sharing. If you leave sharing mode, other people will be extremely easy to see all your files, gather information and even delete those files and folders, but sometimes you are in that mode without knowing it. I'm turning it on.

It's easy to identify and then turn off that sharing mode. Open Windows Explorer, view all your folders. Any folder with a small hand below it means it is shared. Anyone who connects to your network can access it. To turn off this mode, right-click on the folder, select ' *Sharing and Secur* ity', click on the ' *Sharing* ' tab, select ' *Do not share this folder* ' and click ' *OK* '.



How to turn off all shared files or folders

When a folder is shared, all subdirectories below it are automatically shared. But those subdirectories don't have an outlined hand or any indication that it's being shared in the 'Sharing' tab. So carefully consider the top-down folders to see if they are shared. And check regularly to make sure your root drive is not shared. Otherwise others can access all folders and files on your computer.

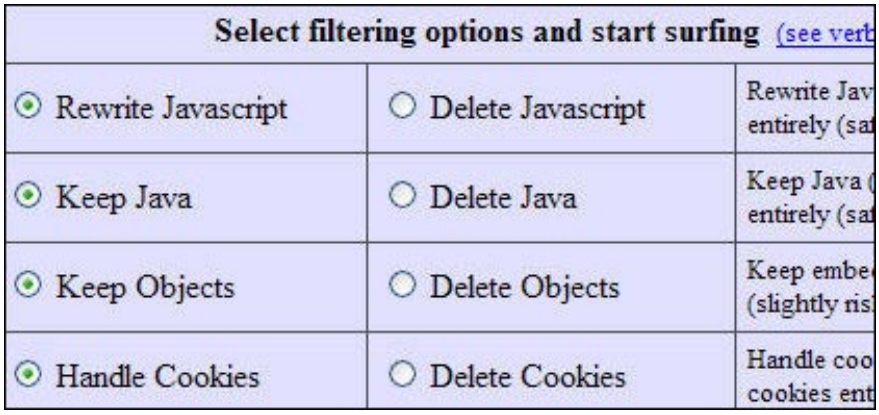
Anonymous web and boring cookies

8. Surf the web anonymously

When you surf the web, your life is like an open book. Websites can detect your ' *online tours* ', know the operating system and browser you are using, find out the host name, discover the last website you visit, check IE's History and Get everything from the cache. They can also check their IP address for basic information about you like a geographic area and other miscellaneous information.

But if you like, you can surf the web anonymously so that websites can't catch IP or anything from you. There are many software you can buy to support this issue. But you don't do it for free by placing an anonymous proxy between your computer and the Web site you're visiting. When you use an anonymous proxy service, your browser will not contact the website directly. Proxy server acts as a buffer. This means that the website will see the proxy's IP address, not your computer. The website cannot read cookies, history or check the clipboard and cache because the computer is not directly connected to it. You surf the web without leaving a trace.

You can try The Cloak website. Click on the 'Surf' link on the left. From there, type in the URL you want to visit. Website will act as a proxy and hide all your information.



Surf the web anonymously without paying a dollar using The Cloak

If you want, you can set your browser to use an anonymous proxy server. Find an anonymous proxy at AiS Alive Proxy List. Write down the server's IP address and the ports it uses (For example, in the 24.236.148.15:80 list, the IP address is 24.236.148.15 and the port number is 80).

Then, in *Internet Explorer* , select *Tool -> Internet Option* click on *Connections -> LAN Settings tab* , check the box " *Use a proxy server for your LAN* ".

In *Address* , type the IP address of the proxy server, in *Port* enter its gateway address, check the " *Bypass proxy server for local addresses* " box (You don't need to leave anonymous information in the local network) - > Click *OK* twice to close the dialog box.

In Firefox, select *Tool -> Options -> General -> Connection Settings* ; Click " *Manual proxy configuration* " button, enter proxy information and click *OK* twice.

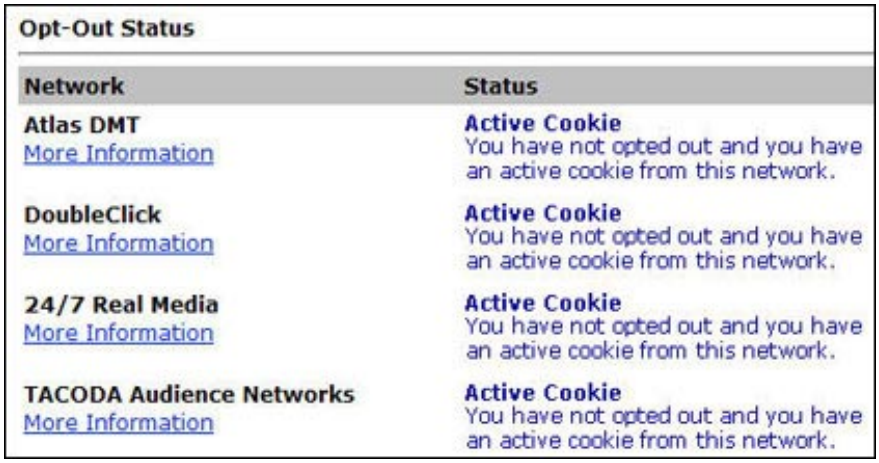
9. Say no to Cookie

Online advertising networks have the ability to create detailed profiles about the websites you visit and your personal preferences. Do they use trickery? No, they only put cookies on the hard drive and track the websites you visit.

You can prevent it by setting the *opt-out* cookie option. This option is provided by the ad networks themselves.

For example, to exit the huge online advertising network DoubleClick, go to the company's opt-out page, click the " *Ad Cookie Opt-Out* " button at the bottom of the screen.

Some other ad networks also allow you to remove cookies. For more information you can go to the Network Advertising Initiative, check the *Out-box box* next to any ad networks you want, then click the Submit button.



Remove coookies with the opt -out function of ad networks

The dangers on ebay

10. Protect yourself against the ' *Nigerian Scams* ' risk on eBay

The most known and longest-known " *Nigerian scams* " email scam on the Internet. When sending an e-mail asking for help moving millions of dollars out of Nigerian, I don't know why your bank account is empty.

There were actually fraudsters involved and now the ' *Nigerian scams* ' is gaining popularity on eBay. They are aimed at sellers, not buyers.

So how do they work? You set a price on the auction box. At the end of the auction the highest bidder will contact you and ask you to ship the goods to Nigeria or any other country. Usually a strange story comes, popular is the story of a buyer who lives in the US but just adopted a child in Nigeria and is in need of goods to send directly to the child.

The winner of the auction will send you PayPal identification, stating that the price has been paid. Or he sent you an email saying he would pay the fastest after he received the goods. And he will pay you via PayPal.

Shipping and the result is that you were tricked. The identity information on PayPal is actually fake. And of course if you transfer before you receive the money, you will never be able to receive it again.

How to prevent this behavior? First, never ship unless you verify that you have been paid. Do not trust the e-mail of the buyer or from PayPal itself if the letters say there is a payment. Instead, log in to PayPal yourself and check if you have any more.

Secondly, only sell goods to those who are willing to buy at other auctions. Phishers often create new accounts and these accounts have a working number of 0. If you see a high level of initiation, the account's operating number is 0, go to the website: http:///offer.ebay.com/ws/eBayISAPI.dll?CancelBidShow and remove that fake buyer

But scammers also realized that the number of accounts in their accounts could be against them. So they bought some goods in the " *Buy It Now* " section at 99 cents to build a program that works properly for the account.

Please check the details in the activity of the buyer. If most purchases are in 99-cent Buy for now, then it is definitely a fraud.

If you know or suspect someone, you can delete his name in future purchases. Go to http://cgi1.ebay.com/ws/eBayISAPI.dll?bidderblocklogin and block the name of that scammer.

T.Thu (***According to Informationweek*** **)**

You finished reading the article "**Ten free ways to keep your computer safe**" 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.