CMP
United Business Media

InformationWeek
Business Innovation Powered By Technology
April 10, 2006

10 Free Ways To Keep Your PC Safe

You don't have to spend a fortune to protect your PC from viruses, Trojans, phishers, scammers, and snoops. In fact, you don't have to spend a penny.

By Preston Gralla, TechWeb

From the moment you turn on your PC until the moment you turn it off, it's under assault. Hackers try to break into it; viruses, Trojans and worms try to crawl into it; spyware tries to watch everything you do. Then there are wireless dangers, snooping co-workers, and worse.

What to do? You could spend hundreds or thousands of dollars on software and services, and spend countless hours trying to keep yourself safe...or you could instead read on. We'll show you ten simple ways to protect your PC without spending a penny.

While some of these products are free versions of commercial packages, others are provided free of charge by hardworking individuals. If you find their services valuable, you can choose to give them a donation. But that's entirely up to you.

10 Free Ways To Keep Your PC Safe

1. Get Free Anti-Virus and Anti-Spyware Protection

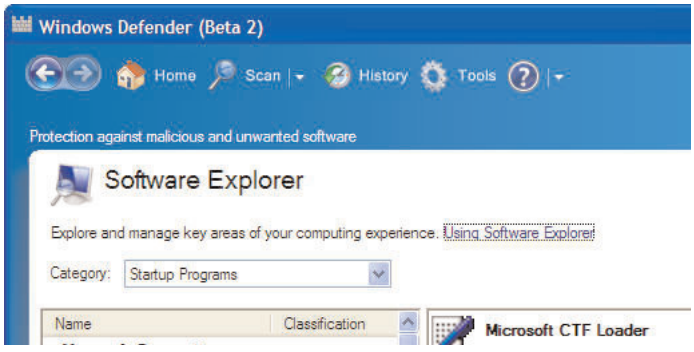
If you want to protect your PC against viruses, you have to pay for it...and pay for it...and pay for it. Anti-virus makers these days charge annual fees, rather than a one-time purchase price, so you'll end up paying hundreds of dollars to protect your PC against viruses during its lifetime.

That is, unless you know which applications to use. It's true that companies like McAfee and Symantec charge in this manner, but there are, in fact, two free anti-virus programs that do everything the big boys do: offer real-time virus protection, scan for viruses, and automatically download the latest anti-virus signatures for maximum protection.

One is Grisoft's AVG Anti-Virus Free, which has a companion anti-spyware program. Both are free for private, non-commercial, single home-computer use.

Another widely used free anti-virus program is Avast 4, free for home, non-commercial use. Avast even works with the beta of Windows Vista, something that few anti-virus programs are capable of doing.

As for anti-spyware tools, there are plenty of free ones out there. Ad-Aware Personal and Spybot Search & Destroy are excellent choices, as is Microsoft's Windows Defender. Anti-spyware programs don't always catch the same malware, so it's a good idea to scan your system regularly with at least two anti-spyware apps.



Windows Defender in action. The Software Explorer shows you all the programs running on your system and lets you eliminate any that might be malware.

2. Check Your Security Online

Just how secure are you, really, when you surf the Net? Find out with free online safety checks. To find out how vulnerable you are to online snoopers, hackers, and crackers, head to Shields Up, which

gives your PC a thorough analysis. It performs a series of tests, including checking every one of your Internet ports, and reports whether you're in "stealth" mode (the safest) and whether your PC responds to ping requests (for maximum safety, it shouldn't). It also gives you recommendations on how to close off your system if it's open to threats.

Symantec also offers an online safety check, but don't be surprised if the recommendations it offers are to buy Symantec security software. Similarly, McAfee has a free Wi-Fi scan that checks the safety of your wireless connection. Don't be shocked if it recommends that you buy McAfee Wireless Home Network Security to solve the problem. But there are other ways to protect yourself besides buying that particular product -- for example, checking out our next tip for free wireless protection.

3. Get Free Wireless Network Protection Software

Most home networks are vulnerable to passing "war drivers" who hack into unsuspecting wireless networks. There are plenty of ways you can muck around with your router settings to protect yourself, as we show you in 6 Steps To Protect Your Wireless Network.

But what if you don't want to fiddle around with filtering MAC addresses, changing your SSID (network name), and disabling SSID broadcast? You can get a free program that will do most of that for you. Network Magic comes in two versions, a free version and a for-pay version, but if all you want to do is configure your wireless network for maximum security, the free version will work just fine.

Install it, and it examines your router and entire network, and builds a network map of all of your connected devices. It examines your router's security settings and issues a report on what it finds. If, for example, it discovers that you're broadcasting your SSID, it will alert you. A single click of a checkbox, and Network Magic will stop the broadcasting for you.

The for-pay version includes other features, such as configuring folder and printer sharing, but if you're only interested in security, you don't really need it.

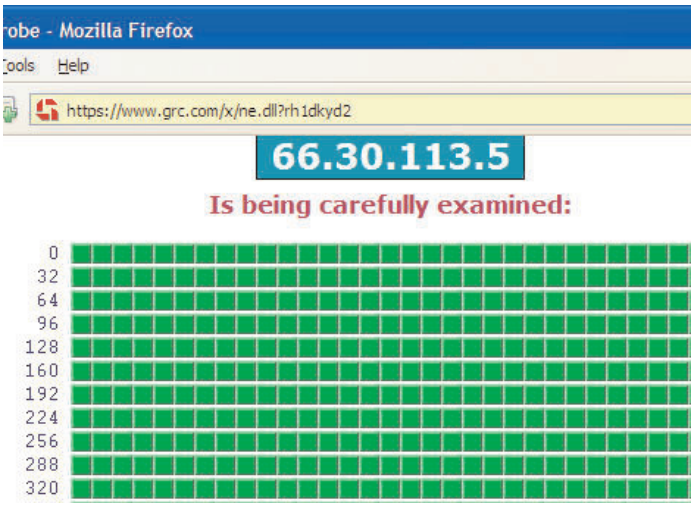
Note that there's not much this program can do that you can't do on your own, if you're willing to dig in and get your hands dirty. But if you'd like to keep them clean and still have a secure wireless network, you can't do any worse than free. 4. Use A Free Firewall

It's this simple -- you need a firewall. It's one of the best ways to protect yourself against Trojans, to keep your PC from becoming a zombie that obeys the commands of a distant hacker, and to stop attackers from worming their way into your PC.

If you have Windows XP Service Pack 2, you have a halfway useful firewall built in. (If you haven't installed SP2, immediately upgrade by going to Windows Update.)

By default, when you install SP2, the firewall is turned on. But if you suspect it's accidentally been turned off, you can check by clicking the Security Center icon in the system tray. The Security Center screen will pop up. (If the Security Center icon doesn't appear in your system tray or Taskbar, select Control Panel > Security Center.) Look at the top of the screen to make sure the firewall is turned on. If it's not, click the Windows Firewall icon at the bottom of the screen, select On, and click OK. The firewall will now be turned on.

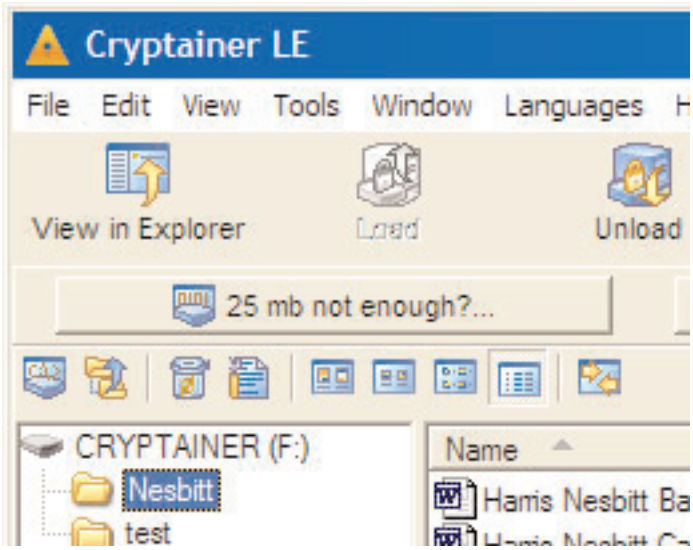
But the firewall built into XP only offers inbound protection -- in other words, it blocks unsolicited incoming connections, but not outbound connections. Spyware and Trojans often "phone home," making outbound connections from your PC without your knowledge. If you want to block outbound connections, you need a two-way firewall. The best free one you



Success! The green squares show that you've successfully blocked off your PC from hackers, crackers, and snoopers.

Network Magic will help you configure your wireless router for maximum security.

At the very least, make sure to turn on Windows XP's firewall.



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

can find is ZoneAlarm from Zone Labs. If you're only looking for a two-way firewall, there's no need to buy one of ZoneAlarm's for-pay versions, which offer extra features such as virus protection.

This is one area where users of older versions of Windows don't have much in the way of free options. ZoneAlarm no longer supports Windows 98 and ME, so if you're using one of those operating systems, you'll need to shell out for a commercial firewall such as Symantec's Norton Personal Firewall or Trend Micro's PC-cillin Internet Security.

Editor's Note: For reviews of five top software firewalls, see Safety First: Five Firewalls For Your Desktop PC.

5. Encrypt Your Data

No matter how good you are at making sure no one else has access to your PC, someone might be able to get in. It could be a hacker, or someone who is on the network you use. If you're at work, it might even be a co-worker who sits down at your PC when you're out of the office.

The solution? Encrypt data that you don't want others to see. Most encryption programs cost money, and many aren't particularly easy to use. But **Cryptainer LE** from Cypherix is both free and simple to use. Install it, and it creates a new, encrypted volume on your PC. Create files inside that volume, or move files into the volume, and they're encrypted on the fly. You can work with them as you would any other files, without having to use a password.

When you want any files or folders hidden from prying eyes, highlight them and click the Unload button in **Cryptainer LE**. They'll suddenly vanish. To make them appear, click the Load button, and they're back after you type in a password. Only those with access to the password will be able see them.

The software is also useful for those who use small USB flash drives to carry around data. You can encrypt the entire drive so that if you lose it, no one else can see the files on it. 6. Protect Yourself Against Phishers

Phishing is one of the most insidious and nastiest attacks out there. You get a legitimate-looking e-mail from your bank, eBay, PayPal, or other financial institution warning you that you must click a link to log into your account for some reason -- to update it, confirm your information, or even for protective purposes.

Click the link, and you go to a site that looks like the real thing, but isn't. Log in, and maybe be asked to provide additional information such as your social security number. Then kiss your money good-bye -- a scammer has sent the mail, and set up a false site, and uses the personal information you've entered to empty your account and steal your identity.

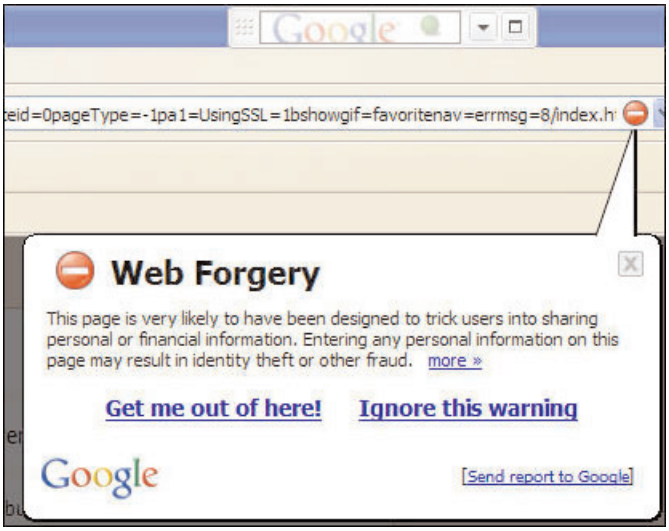
There are simple ways to thwart phishing attacks. Never click on a log-in link from an e-mail purporting to be from your financial institution, eBay, or PayPal, no matter how legitimate it looks. Instead, go to the site yourself and log in.

Second, use an anti-phishing toolbar, which will block you from visiting a phishing site or warn you when you're visiting one. There are plenty of good ones out there. The Google Toolbar includes an anti-phishing feature that will block you from visiting a phishing site and pop up a warning about it. After you install the toolbar, click on its "Options" button. Then, under the "Browsing" tab, check the box next to "Safe Browsing." Click the "Safe Browsing Settings" button and configure your level of protection. Click "OK."

Don't go there! The Google Toolbar includes an anti-phishing feature to protect you from phishing scams.

Another good anti-phishing toolbar is the Netcraft Toolbar, which offers similar protection.

Soon you won't need any anti-phishing toolbars, because both Internet Explorer 7 and Firefox 2.0 will include anti-phishing tools built right into the browser. In preliminary tests, the IE7 anti-phishing tools caught more phishing attacks than did Firefox 2.0, but both products are still in beta.



Don't go there! The Google Toolbar includes an anti-phishing feature to protect you from phishing scams.

7. Disable File Sharing

One of your biggest security dangers is sitting in plain sight, and you probably don't even know it. If you've set up your PC to share files and folders, it's exceptionally easy for people to look through all your files, grab personal information, and even delete files and folders as well. Odds

are, though, that you don't know if you're set up for sharing.

It's easy to find out, and then to turn off sharing. Open Windows Explorer and look at all of your folders. Any folder that has a small hand beneath it means that folder is being shared, and that anyone connected to your network can gain access to it. To turn off sharing, right-click the folder, select Sharing and Security, click the Sharing tab, select "Do not share this folder," and click OK.

By the way, when a folder is shared, all the subfolders beneath it are automatically shared as well. But those subfolders won't show the small hand beneath the folder or indicate that it's shared in the Sharing tab. So be careful to look at all top-level folders to see if they're shared. And you should always check to make sure that your root drives aren't shared, because if they are, others have access to all the folders and files on your system. 8. Surf The Web Anonymously

Toss your cookies by opting out of advertising networks.

When you surf the Web, your life is an open book. Web sites can track your online travels, know what operating system and browser you're running, find out your machine name, peer into your clipboard, uncover the last sites you visited, examine your history list, and delve into your cache. They can also examine your IP address to learn basic information about you, such as your geographic location. Pretty scary stuff.

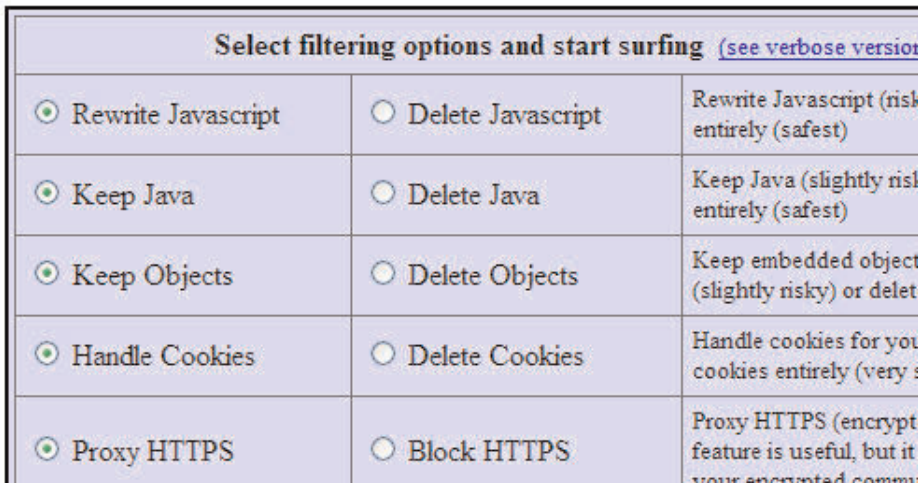
But if you'd like, you can browse in perfect anonymity. There's plenty of software you can buy that will do this for you, but you can do it for free by using an anonymous proxy server that sits between you and the Web sites you visit. When you use an anonymous proxy server, your browser doesn't contact Web sites directly -- the proxy server acts as a buffer, which means the sites see the IP address of the proxy server, not your PC's IP address. Web sites can't read your cookies, see your history list, or examine your clipboard and cache because your PC is never in direct contact with them. You can surf without a trace.

One way to do it is to head to the free site The Cloak. Click the "Surf" link on the left. From there, type in the URL you want to visit, and the site acts as your proxy, with all your information hidden.

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

Then, in Internet Explorer, select Tools > Internet Options, click the Connections tab, and click the LAN Settings button. Check the "Use a proxy server for your LAN" box. In the Address field, type in the IP address of the proxy server. In the Port field, type in its port number. Check the "Bypass proxy server for local addresses" box; you don't need to remain anonymous on your local network. Click OK twice to close the dialog boxes.

In Firefox, select Tools > Options > General > Connection Settings, click the "Manual proxy configuration" button, enter your proxy information, and click OK twice.



Surf anonymously without paying a penny, by using The Cloak.

9. Say No To Cookies

Online ad networks have the potential to create in-depth profiles of your Web travels and personal interests. The trick? They place cookies on your hard disk that track you across multiple sites.

You can fight back by placing an opt-out cookie -- provided by the ad network -- on your hard disk that will tell sites to keep their mitts off your surfing habits.

To opt out of the massive DoubleClick online advertising network, go to its opt-out page and click on the "Ad Cookie Opt-Out" button at the bottom of the screen.

Some other advertising networks let you opt out as well. For details, go to the Network Advertising Initiative site, check the Opt-Out box next to any ad networks you want to opt out of, then click Submit.

10. Protect Yourself Against eBay "Nigerian Scams"

E-mail "Nigerian scams" are among the oldest and well-known on the Internet, in which you're sent an unsolicited e-mail asking for help to

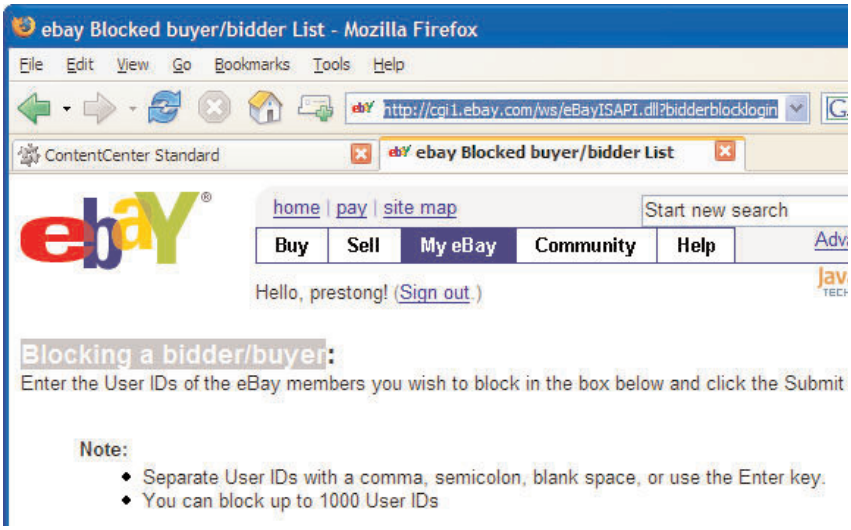
transfer millions of dollars out of Nigeria -- but somehow, it's your bank account that gets emptied.

Well, the scam has morphed, and Nigerian scams are now rife on eBay. This time around they're often pointed at sellers of items, not buyers.

Here's how it works. You put an item up to bid. At the end of the auction, the winning bidder gets in touch with you and asks that you ship the item to Nigeria, or somewhere else overseas. Often, there's a strange story attached -- a common one is that the bidder lives in the U.S., but has just adopted a child in Nigeria, and wants the item sent directly to the child there.

The winning bidder sends you what appears to be a PayPal notification, saying that the item has been paid for. Or else he sends you an e-mail saying that as soon as you send him a confirmation that you've shipped the item, he'll pay you via PayPal.

Ship the item, and you've been scammed. The PayPal notification was in fact a forgery, and, of course, if you first ship it before getting payment, you'll never get paid.



Block suspected scammers from bidding on your items.

How to protect against it? First, never ship an item until you confirm that you've been paid. Don't trust an e-mail from a bidder, or from PayPal itself, that appears to say a payment has been made. Instead, log into your PayPal account and see if there has in fact been a payment.

Second, only sell items to people who have already bought items at other auctions. Scammers often set up new accounts for scams, and these accounts have zero activity. If you see a high bidder on an item of yours with zero activity, go to the Canceling bids placed on your listing page and fill out the form for canceling a bidder.

By the way, some scammers recognize that zero activity may work against them. So some of them look for 99-cent "Buy It Now" items and buy a number of those, building up solid buying activity. So you should also look at the details page of any potential bidder -- if all the items are of the 99-cent Buy It Now variety, there's a good chance he's a scammer.

If you know or suspect that a particular user is a scammer, you can also block him from ever making future bids on anything you sell. Go to the Blocking a bidder/buyer page and fill out the form.