

Protecting Your Home PC

Brought to you by Ziff Davis Media

The more we make home PCs a daily part of our lives, the more attractive they become to spammers, hackers, phishers, and other Internet malcontents who see your PC as little more than a billboard or a launching pad for insidious attacks. We're concerned about security here at work (you may have noticed!), but a protected PC at home is important, so we thought we'd pass along these security tips for home systems.

The first step in implementing an effective home-security solution is psychological: resign yourself to the fact that protecting your PC involves not one product but many, and that the price of security, to paraphrase Thomas Jefferson, is eternal vigilance: you need to keep your security applications up-to-date.

Every PC needs effective firewall, antivirus, antispam, and antispyware protection. Here are the steps you should take to make your home PC or network about as safe as it can be.

1. **Upgrade to Windows XP.** This may sound like a dramatic change if you're running an earlier operating system, but XP offers the strongest security of any Microsoft OS.

2. **Download Service Pack 2.** A key part of XP's security is Service Pack 2, which gives you:

- An improved (though still flawed) firewall. The firewall's now on by default and it loads earlier in your PC's boot process. Unfortunately, it still doesn't prevent outbound connections, stopping malware from phoning its author and spilling your PC's secrets, for example.
- Windows Security Center. This nice new addition lets you see at a glance that your firewall and antivirus programs (even third-party antivirus programs) are running and up to date. (It also recognizes some, though not all, third-party firewalls.)
- Vestigial antivirus protection. Microsoft has just started integrating antivirus protection into its OS (after buying antivirus technology from GeCAD in 2003). The company recently released, via its Web site and Windows Update (for XP users only) its Malicious Software Removal (MSR) Tool—you'll get this tool when you make the SP2 upgrade. Even Microsoft, however, stresses that MSR *complements* a full antivirus app rather than replaces it. The company has also released a public beta of Microsoft AntiSpyware, based on Giant AntiSpyware (Microsoft acquired Giant Software last year). You can download it at <http://www.microsoft.com/athome/security/spyware/default.mspx>. If you're not willing to spend the money on the full-blown solutions we recommend below, at least install SP2 and Microsoft AntiSpyware.
- Internet Explorer improvements. IE now blocks most pop-up ads (they can contain links that install malware) and usually asks permission before installing ActiveX controls (they provide entrée to your system's OS).

To download SP2, go to the Windows Update site

(<http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>), download the (small) program that checks your PC for current installations, and follow the step-by-step instructions. Before you do that, however, since upgrading means getting on the Net and you're currently unprotected, turn on XP's firewall by going to XP's Control Panel, double-clicking on Windows Firewall, and turning it on.

3. **Enable Automatic Updates.** While you're at the Microsoft Windows Update site, click on the "Turn On Automatic Updates" button on the left of your screen so that XP automatically checks for security updates (don't worry, you can make sure XP asks you before it installs anything).

4. **Upgrade Office applications.** Once you've got Microsoft's operating system under control, it's time to tackle any security leaks in your Office applications. Go to the Microsoft Office Update site (<http://office.microsoft.com/officeupdate/maincatalog.aspx?lc=en-us>) and follow the same procedure as you did for Windows Update: download the checker program and install any available updates. While you're there, turn on Office Update as well.

5. **Go the suite route.** Even with their improvements, SP2 and the Office updates are no security solution. You still need firewall, antivirus, antispyware, and antispam applications, and if you have kids to rein in, you should have parental controls and content filtering as well. Buying all these bits of protection individually can be expensive. In addition, if you try to piece together a security solution with components from different companies, you run the risk of the applications clashing with one another. A security suite is a much more sensible approach and, on average, suites cost only about 50 percent more than an antivirus program alone. *PC Magazine* reviewed nine security suites at <http://www.pcmag.com/article2/0,1895,1761716,00.asp>. All of them contain firewall, antivirus, and at least one other form of protection, such as antispyware, antispam, Internet filtering, identity protection, or instant-messaging security.

6. **Update your suite.** Once you've selected and installed your suite, don't forget to go to the manufacturer's site and update their set of programs.

7. **Toughen your passwords.** Any word in the dictionary makes for a poor password. Password crackers, the clever programs that hackers use to gain access to your system and accounts, use dictionaries, too, and they're fast at trial-and-error. A good password contains at least 8 characters consisting of letters, numbers, and symbols.

8. **Layer security.** Two firewalls or antivirus utilities will step on each other, but it's okay—even wise—to have two antispysware apps, because their accuracy isn't yet up to snuff. Set only one to scan files on-access; that's how programs end up fighting.

9. **Beware ActiveX.** ActiveX controls execute cool interactive elements on Web pages, but they provide access to the local Windows OS—highly risky. In Internet Explorer, click on Tools/Internet Options and go to the Security tab. The Custom Settings button takes you to Security Settings. Choose Prompt for Download signed ActiveX controls and Disable for Download unsigned ActiveX controls.

10. **Know what you're running.** If the kids insist on using P2P apps, use ones without spyware, such as Shareaza, and don't share your entire hard drive. Also, look through your Program Files directory—you may be surprised to find what's on your machine.

11. **Avoid foreign objects.** Your kid's friend could show up with a CD or USB key with a downloaded game on it and inadvertently install spyware on your PC. Or he could do so on purpose.

12. **Prepare for the worst.** Store sensitive data off your hard drive, preferably encrypted. Invest in system-recovery software against the day Windows becomes a total loss, either from hackers or from bit rot and Registry bloat.

13. **Turn it off.** There's no point in offering your PC's ports to the Internet while you're sleeping or at work.

Security for Your Wireless Home Network

If you have a wireless LAN at home, and more and more people do, security is important there, too. Encryption is a vital component of wireless network security—after all, you don't want someone standing outside your den window and accessing your PC and all its contents. If you leave your wireless connection unsecured, the very least you can expect is a hitchhiker or two on your connection.

You have two choices in wireless security standards, WEP and WPA. Engineers designed wireless's first encryption scheme to provide the same level of security as wired LANs, so it goes by the name Wired-Equivalent Privacy (WEP). It turns out, however, that WEP encryption wasn't all that secure, and a second standard evolved that bolstered wireless security in a number of ways--by restricting access to authenticated users only, for example, and by using stronger encryption schemes. This newer standard goes by the name WiFi Protected Access, or WPA (WiFi—wireless fidelity--is the protocol for wireless networks). If you're still

deciding on a wireless protocol for your home LAN, spend the extra money and go with the sturdier WPA solution.

(If you decide to switch to WPA from WEP, be aware that it's an all-or-nothing proposition: every wireless device on your network must have WPA capabilities, including any wireless bridges you use for your Microsoft Xbox (or other gaming device), digital camera, home audio gateway, and print server.)

If you've got a wireless LAN at home, follow these steps (in addition to the steps outlined above) to bolster its security:

1. **Update your firmware.** Make sure the firmware on both your router/access point and your network cards is up to date with the latest security patches. Download them from the manufacturer's Web site.
2. **Set limits.** Limit the number of IP addresses your router can assign.
3. **Restrict MAC access.** Restrict access to your computers' MAC addresses only. Go to each machine you want to allow on your wireless network, open a command prompt, and type `ipconfig /all`. Copy down the physical addresses, then use the access point's configuration options to limit connection to only these addresses.
4. **Banish defaults.** Never use the default SSID, administrator password, or WEP key; set all of these using criteria for tough passwords (see "Toughen Your Passwords" above).
5. **No SSID broadcasts.** Disable SSID broadcasting.
6. **WEP security.** If you're on a WEP-based WLAN, set your router/access point and wireless cards to the highest level of encryption that both allow.

Copyright © 2005 Ziff Davis Media Inc. All rights reserved. You may customize this document for use within your organization. Any other reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. The information contained herein has been obtained from sources believed to be reliable. Ziff Davis Media does not make any representation or warranty of any kind, whether express or implied, concerning the document or the use, accuracy, completeness, or reliability of the information contained herein or for interpretations thereof. Without limiting the foregoing, Ziff Davis Media expressly disclaims any warranty of merchantability or fitness for a particular purpose. Ziff Davis Media TIPS-IT.com and TIPSheet are trademarks of Ziff Davis Publishing Holdings Inc. All other trademarks and trade names used on the TIPS-IT Web site and in its publications are the property of their respective owners.