Stop hostile apps

Cookies aren't inherently malicious, but the ubiquitous little files inhabit your hard drive (if you use Internet Explorer, for instance, the cookies reside inside your C:\Windows\Cookies folder) and identify you via a string of numbers and letters (called a unique identifier) to the Web site or company that placed the cookie there. For instance, companies such as DoubleClick, Adbureau.net, or LinkExchange that provide advertising to Web sites can plant a cookie on your hard drive when you are reading one site (for example, Amazon.com) and then read that same cookie when you surf to a different DoubleClick-served site (for instance, CNN.com). That's how the company tracks you across multiple sites.

Take a bite out of cookies

Fortunately, your browser makes it easy to disable cookies: In Internet Explorer 5.*x,* click Tools > Internet Options, then choose the Security tab. Click the Earth icon labeled Internet, then click the Custom Level button near the bottom of the window. In the Security Settings window that opens, scroll down to the section labeled Cookies. To keep your browser from automatically planting cookies on your PC, select the Disable or Prompt option next to "Allow cookies that are stored on your computer" (in other words, the persistent cookies we mentioned earlier). It's generally OK to leave the per-session cookies enabled; these are the cookies that remember what's in your shopping cart when you use a Web store.

In Netscape, click Edit > Preferences and select the Advanced item in the left pane. Here, you can opt to block all cookies or to decide on a site-by-site basis. We recommend that you pick the second option and allow your browser to use cookies for some sites. That way, you can exercise a measure of control over your information and still take advantage of the cookie conveniences. If you're truly paranoid, however, you may want to disable all cookies even if it prevents you from, say, shopping efficiently online.

If you're curious about how many sites set cookies, check the "Warn me before accepting a cookie" box, and Navigator will pop up a dialog box each time a site tries to set a cookie. (Internet Explorer still lacks such an option.) We recommend that you try this for only a short time; the sheer volume of cookie request dialogs will likely drive you batty.

Be selective

Simply disabling cookies may not work for you, however. Internet Explorer doesn't let you block cookies sent to advertising companies while permitting cookies from the site you're visiting; it's all or nothing. Blocking all cookies eliminates the timesaving benefit of user preferences on free customizable news sites such as My Yahoo. If you use IE and want to pick and choose which sites are allowed to plant cookies on your hard drive, try the handy freeware CookieWall from AnalogX. CookieWall runs in your System Tray, silently monitoring your Internet Explorer cookie file every minute or so and allowing you to pick and choose which cookies to permit. When the program encounters a cookie that it hasn't seen before, a dialog box pops up to ask you what to do with cookies from this site--handy if, say, you register to use My Yahoo and don't want to have to enter your username every time you load the page.

Antiviral warfare

If you don't have antivirus software on your computer, get with the program! Every day your PC goes without proper protection is another day it risks infection--and infecting others. Viruses don't just wipe out your hard drive; some can steal your entire e-mail address book or implant programs on your hard drive (such as SubSeven or BackOrifice) that hackers can later use to break in to your computer. For $20, eTrust Antivirus software provides virus protection nearly as good as the big guns from Symantec or McAfee. Best of all, you can try it free for two months. For a more comprehensive antivirus program, however, you may want to shell out a few bucks for Norton AntiVirus.

Connection protection

If you use a high-speed connection such as DSL or cable, consider downloading ZoneAlarm, CNET's favorite free personal firewall. Firewalls not only keep hostile apps from entering your PC from the outside, they also block hidden or unknown software on your PC (the sort a virus could install) from connecting to the Internet without your knowledge and giving away your valuable information.

To find out how secure your connection is, go to Steve Gibson's Shields Up site and get a free test of your security. Shields Up performs many of the same tests hackers use to probe your computer for vulnerabilities and provides you with a summary assessment of your PC's security and what you need to do (if anything) to make yourself less vulnerable. Gibson's scan can tell you if the back door program is running but not if it has been (or is being) used. But a little information goes a long way. If you know the Trojan is there, you can work to get rid of it. Again, the price is right, so what are you waiting for?