

[Workers' Edge](#)

May 7, 2009 9:00 AM PDT

Five simple PC security tips

by [Dennis O'Reilly](#)[Font size](#)[Print](#)[E-mail](#)[Share](#)[Yahoo! Buzz](#)

The list of PC security products never ends. For every name that drops off, two more jump on. In fact, determining the best security hardware and software is a full-time job. Sometimes, you just want to throw up your hands and take your chances.

Maybe I'm just a cockeyed optimist, but I think you can stay safe without spending all your spare time doing research, installing updates, and generally becoming a PC-security expert. Here are five relatively easy ways to improve your security.

Use the firewall that's closest at hand

In the computer industry, the reputation of a product, service, or Web site is just about worthless. Yesterday's best firewall, ad blocker, spam buster, virus spotter, or spyware cleaner is today's bust.

Maybe the product got bought and the new owners aren't as conscientious about updates as the previous ones. Or the service's management team decides to go for profits and skimp on support, updates, and enhancements. There are lots of reasons why a good product goes sour, and the computer industry has seen nearly all of them.

So if you can't go by reputation, how do you choose a security product? One way is to go with the tools you've already got. Windows' security is roundly criticized, but the fact is, it's better than it used to be, and third-party security products have their own shortcomings.

Last February, I recommended that you [use a third-party firewall](#) rather than the one built into Windows. Six months earlier, I suggested that you pass on the third-party tools and [stick with the Windows Firewall](#) despite its shortcomings.

So which side of the fence am I on now? The simple side. The fact is, any third-party security tool complicates your setup. It's not difficult to find weaknesses in the Windows Firewall, but it's safe enough for most PC users, and it's much better than using no software firewall at all.

My previous post included links to information on Microsoft's TechNet site providing [technical details](#) of the Windows Firewall, tips for [customizing the Windows Firewall](#), and help troubleshooting the firewall in [XP](#) and [Vista](#).

Don't hesitate to try another free antivirus program

Just last week, I switched antivirus programs on my XP test system--for the umpteenth time. Something was slowing the system down, and after defragging the hard drive and doing other standard maintenance tasks, the machine's performance didn't improve as I expected it to.

Rather than go through a bunch of diagnostic tests, I simply uninstalled the system's antivirus tool and downloaded a competing package. The old and new programs were both free, and the switch didn't take much time to complete. The topper? The XP machine's performance perked up immediately.

Two antivirus programs that are free for home use and that are currently highly rated are [Avast Home Edition](#) and [Avira AntiVir](#). You'll find a list of dozens of antivirus programs for Windows on this [Download.com page](#).

Change your password...again

I hate those "your password will expire in x days" warnings as much as you do, but one of the simplest ways to protect yourself is by keeping your passwords fresh. Last year, I described the [Ten Password Commandments](#), one of which was to devise a password-creation strategy that's all your own.

Just two months ago, I complained about the [shortcomings of passwords](#) as our primary security option, though I concluded that there's nothing better, for now. Lots of people swear by password managers such as [RoboForm](#), but then you have yet another third-party app complicating matters.

For me, it's simpler just to devise a new password based on my unique, inimitable

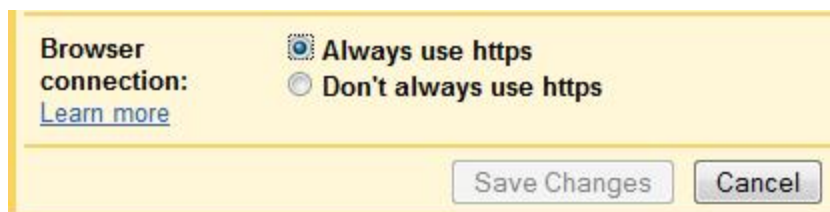
password-creation system, which I share with no one. No need to write it down, enter it in an online form, or encrypt it in a master-password file. Temporary amnesia, well, that's another matter.

For secure e-mail, use encryption

You would think that encrypting e-mail would be a breeze, but doing so is anything but. You and the recipient have to deal with digital certificates, public and private keys, and any number of other time-eating preparations and precautions.

The simplest way I know of to encrypt your e-mail is by using the Mozilla Foundation's [Thunderbird](#) with the [Enigmail](#) extension. Jason Thomas provides step-by-step instructions in this [tutorial](#) on the Lifehacker site.

Gmail users can secure their e-mail communications by enabling the service's built-in encryption. To do so, click the Settings button at the top-right of the main Gmail screen, scroll to the bottom of the General tab, select "Always use https," and click Save Changes.



Select "Always use https" under the General tab in Gmail's Settings to encrypt your messages.

(Credit: Google)

Keep your browser up-to-date

Most people will tell you that the Mozilla Foundation's [Firefox](#) browser is the safest way to surf, but a recent [report](#) from Google Switzerland and the Swiss Federal Institute of Technology found that "(u)sing the most recent version of a browser will lower the risk associated with drive-by-downloads and other Web-based attacks, which start by targeting the browser."

The report cites [Google Chrome's](#) silent updates as the best way to ensure that your browser is protected. The researchers also laud Chrome's lack of a way for users to disable its silent-update feature. Some people will object to software being downloaded

to and installed on their system without their knowledge, but the fact is, these behind-the-scenes updates are the best way to keep you safe from the Internet bad guys.

Personally, I'm starting to rethink my choice of default browser. But as I mentioned earlier, you can't put any faith in a computer security product's reputation. And you can't be afraid to switch.



Dennis O'Reilly has covered PCs and other technologies in print and online since 1985. Along with more than a decade as editor for Ziff-Davis's Computer Select, Dennis edited PC World's award-winning Here's How section for more than seven years. He is a member of the CNET blog Network, and is not an employee of CNET.

Topics: [Security](#), [Internet tips](#), [E-mail tips](#)

Tags: [Encryption](#), [E-mail security](#), [Passwords](#), [Browser security](#), [Windows Firewall](#), [Antivirus software](#)

Share: [Digg](#) [Del.icio.us](#) [Reddit](#) [Yahoo! Buzz](#) [Facebook](#)

Related

From CNET

[The iPhone's secret silicon: A need to know?](#)

[UC Berkeley computers hacked, 160,000 at risk](#)

[Prediction: Apple will recommend security software](#)

From around the web

[Hotels: Hyatt is the latest chain on sal...](#) Budget Travel

[The Caps' Keys to Victory](#)
Washington Post Blogs - D.C. S...

[More related posts](#) powered by
 Sphere