

The Ten Commandments of PC Security

Fight off nasty viruses, worms, and Trojan horses by following these simple rules.

Daniel Tynan

Contributing editor and award-winning journalist Daniel Tynan writes PC World's monthly Gadget Freak column.

And it was written (by Bill Gates, et al): Thou shalt use a Windows PC to do thy work and it will be good.

But Windows computers are vulnerable to plagues of biblical proportions: viruses that bring down entire networks, e-mail worms that replicate at lightning speed, Trojan horses that hide inside otherwise innocent programs, hackers that take over computers, and more.

Fortunately, archeologists have recently unearthed two stone tablets from a garage near Cupertino, California that can help deliver us from such evils. We present their guidelines here, along with interpretations from our brothers and sisters in the PC security choir.

I. Remember thy antivirus software and keep it updated.

It's not enough to have the software installed (if you don't have an antivirus package, stop reading right now and get one); you also need to keep up with new viruses as they emerge.

"Your antivirus software is only as good as your latest virus definitions set," says Kelly Martin, senior product manager for Symantec's Norton AntiVirus. Programs like Symantec's Norton AntiVirus (\$50) and Network Associates' McAfee VirusScan (\$35 to \$60) can automatically update their virus signature databases, but it costs an additional \$20 to \$35 for ongoing annual subscriptions.

II. Thou shalt not covet thy neighbor's attachments.

You get a message you think is from a friend with what looks like a cool file attached, so you click on it. Next thing you know, you're Typhoid Mary, spewing out infected e-mails to everyone in your address book. That's how the Sobig.F worm spread--and it happened so quickly that millions of copies got out before the antivirus companies could update their databases.

"Never trust an e-mail 'from' address," adds Chris Wysopal, director of research for security consultants @Stake. "And never open an attachment without verifying it was sent by a trusted person, and they meant to send it to you."

III. Avoideth bogus file downloads. Be wary of any Web site that requires you to download software to view a page, unless it's something familiar like a Flash plug-in or Acrobat Reader. The file may contain a virus, a Trojan horse, or some auto-dialer that calls pay-per-minute numbers via your modem and racks up huge charges.

"Do not install software via the Web unless you are absolutely sure what it is and that you trust the company you are downloading it from," warns @Stake's Wysopal.

IV. Smite spyware and pop-ups. Like Trojan horse programs,

spyware secretly installs itself when you download software like file-swapping applications; it tracks your movements online and delivers ads based on where you surf. Pop-up ads can also exploit security flaws in Internet Explorer, like the recent Qhost Trojan that hijacked users' browsers after they viewed an ad on the Fortune City Web site. Fortunately, there are tools that can protect you: For example, Ad-aware (free) blocks spyware and StopZilla (\$30) takes care of pop-up ads. Some antivirus software and security suites also stop spyware and pop-ups in their tracks.

V. Thou shalt foil spammers. Unsolicited commercial e-mail is more than just a nuisance; it's also a major source of virus infections. In fact, some versions of Sobig are designed to turn infected PCs into zombie machines that can be used to send spam. A good filter like Symantec's Norton AntiSpam 2004 (\$40), Network Associates' McAfee SpamKiller 5 (\$40 to \$50), or Sunbelt Software's IHateSpam (\$20) help trap the nasties your antivirus software might miss.

VI. Keep thy operating system patched. E-mail-borne worms and other scourges like to exploit security holes in your software--namely Windows and other Microsoft programs. These days Microsoft issues so many critical updates to fix these flaws that many users ignore them. Don't. Last January, the Slammer worm exploited a vulnerability that Microsoft had fixed more than six months before. But thousands of infected computers--including some at Microsoft--didn't have the patch installed. Run the Windows Update program once a week and whenever Microsoft issues a warning.

"Until we see automated patch management software, users will simply have to stay up to date," says Thor Larholm, senior security researcher at PivX Solutions.

VII. Maketh a rescue disk and keep it handy. When things go bad, a boot or rescue disk is your first step to recovery. At minimum, you'll want to put the basic elements of your operating system on a floppy disk or Zip media, so you can bypass the hard disk at start-up. To find out how, read "Hardware Tips: Create Your Own Emergency Boot Disk." A better idea: Use your antivirus program to create a rescue disk you can use when your system gets infected. Label it with a date and store it near your system where you won't lose it.

VIII. Be not taken in by false claims. There are more hoaxers than hackers on the Internet, and more bogus "e-mail virus alerts" than actual viruses. Even real virus threats are typically blown out of proportion by the media. A phony warning could cause you to delete harmless files and then forward the message to others, clogging e-mail servers and causing virus-like damage in the process. When you get one of these e-mails (or see yet another breathless news story), check it out first. Type the name of the alleged virus into a search engine to see if any of the major security vendors have issued an alert, and visit the virus hoax pages at F-Secure and Hoaxbusters.

IX. Honor thy firewall. A firewall is like a bouncer for your computer--it checks every ID at the door and won't let anything in or out until you give the thumbs up. So a hacker can't access personal information on your hard drive, and a Trojan horse keystroke logger (a stealth program that monitors the characters you type) can't steal your passwords and transmit them over the Net. Symantec and Network Associates both offer personal firewall packages for \$35 to \$50, while Zone Labs offers a no-frills version of its ZoneAlarm software firewall for free. But a better deal is an Internet security suite that combines antivirus, firewall, ad blockers, spam fighting, and other useful apps; most cost between \$60 to \$80. For a review of suites from Symantec and Network Associates, read "Extra-Suite Virus and Spam Protection."

X. Maketh backups and keep them holy. Simply put: Back up your data files at least weekly (daily and if you're running a business). Even if you fall victim to a virus or hacker attack, you'll escape with only minor damage. Fail to keep a recent backup though, and you'll go straight to hell--at least, that's how it will feel.