

Top 10 Ways to Fight Malicious Code

Top 10 tips for fighting malware

- 1. Get an antivirus tool. No, really get one. Don't just say you will.**

Antivirus tools remain one of the easiest and most comprehensive defenses against malicious code. You can purchase a commercial antivirus tool such as [Norton AntiVirus](#), [Trend Micro PC-cillin](#), or [ZoneAlarm](#). There are also free tools such as [Avast Home Edition](#).

When you first install an antivirus tool, run a complete sweep of your hard drive. Remember to keep your antivirus software current by running its update feature at least once a week. Don't hesitate to update more frequently if you're prompted by the tool!
- 2. Get a personal firewall.**

Again, really do it -- don't just pretend. [Personal firewall software](#) blocks incoming attacks. It also stops malicious code installed on your system from communicating across the network and revealing your secrets.
- 3. Keep your systems patched.**

Believe it or not, [Windows Update](#) is your friend (if you run Windows). New Windows vulnerabilities are discovered almost every day. By visiting Windows Update once a week and making sure you've got all the critical updates, you'll be far safer from attack. It's remarkably easy to do.
- 4. Keep your browser security settings at Medium or even High.**

The Medium security setting contains dozens of tweaks that block common malware-propagation techniques. The High setting goes even further, but it may keep legitimate applets and active scripts from running on your machine.
- 5. Never click 'Yes' when your browser asks if you want to install/run content from an organization you don't trust.**

Watch out for organizations with tweaked names such as "Micro\$oft" and "Paypa1" -- they're just imposters. If your browser pops up a "Do you want to install and run..." message, be afraid. Be very afraid. If you click "Yes," you may be inviting someone to have the same control over your computer that you have. The stakes are high, so don't be duped. Just say "No."
- 6. Install an anti-spyware tool to augment your antivirus protection.**

To seek out and delete adware and spyware, it's a good idea to run software such as Lavasoft's free [Ad-aware](#). Be very careful, however. There are Ad-aware imposters that are spyware-installing trojan horses. Download Ad-aware from Lavasoft's site and nowhere else!
- 7. Don't install a search-help bar in your browser unless it's from someone you trust.**

Google and Yahoo! search-help bars are fine. Many of the other search helpers are just plain evil.
- 8. Check to see which companies' software certificates you're configured to trust.**

Your browser will run code from sites in your trusted list without warning you, so make sure you trust every company on your list. In Internet Explorer, go to Tools > Internet Options > Content > Publishers to see which companies are on your good list. Delete the companies you don't trust.
- 9. Get a credit card to use solely for Internet purchases.**

That way you can carefully watch all charges on that card. Also, if by chance someone nabs that card number from a vulnerable e-commerce site, your physical life won't be impacted. By law your maximum liability for a stolen credit card is \$50. Never, ever, *ever* use a debit card for purchases on the Internet. The maximum liability you could suffer for a stolen debit card is the entire balance of your account. Ouch!
- 10. Don't run executable email attachments, even if sent by a friend.**

Most worms today spread by infecting a machine and launching a mass email attack. You can stop that attack vector and protect your friends by not running attachments. If you get an attachment you really want to open, don't double-click it. Instead, download it (save the file to your hard drive) and then open it from within the appropriate application, such as Word for .doc files or Acrobat for .pdf files. Be especially careful not to execute .exe, .pif, or .scr files!