

How Can I Prevent My Computer from Becoming Infected by Spyware?

By Shawn Hatcher

Source: *The LogicForce Letter*, Fall 2004

How Can I Prevent My Computer from Becoming Infected by Spyware?

By Shawn Hatcher

Spyware is an ever-increasing problem, creating security risks on your company's network by collecting information about users and using that information to send advertising content to users. The main source of spyware is users' downloading unnecessary and suspect software such as screensavers, games, wallpaper, weather reporting tools, Internet clock sync and shopping software.

The following is a list of guidelines, which should help in keeping your computer spyware-free.

1. **Pay attention.** When you're browsing a website, don't just click 'Yes' to see what's next, especially if the website is not a reputable organization. Examples of reputable organizations include Wal-Mart, Outback Steakhouse, eBay, banks, Hallmark, Barnes & Noble, your workplace or your church.
2. **Don't visit online pharmacies, gambling, explicit or hack sites.** Of course, if you feel the organization offering these services are reputable, such as Walgreens.com, then you are probably OK. These sites will attempt to have you install a program on your machine that you probably do not need in order to use their service. The bottom line here is that if they want you to install it, DON'T, because it will probably be spyware.
3. **Install a free program such as Ad-Aware or Spybot.** These programs can be downloaded from <http://www.download.com>. Install one of these programs, and when you feel you're having problems with your computer, update the program and scan. Be sure you remove everything, reboot, and then scan again to make sure there are no lingering spyware applications.
4. **Make sure you have an anti-virus program.** Many people subscribe to an anti-virus service such as Norton or McAfee. If you are unable to subscribe, try installing AVG free anti-virus from <http://free.grisoft.com/freeweb.php>. You may also try using McAfee's Stinger app to scan for common viruses. It does not protect as well as AVG; but if you'd like to scan for recent viruses, go to Google.com and type Stinger. You should see a link to download this anti-virus tool.
5. **Delete Cookies often and modify your cookie policy in Internet Explorer.** Internet Explorer 6 offers extra features to deal with cookies. While in IE6 click on 'Tools' and go to 'Internet Options.' There is a 'Delete Cookies' button here. If you

would like to change your cookie policy, click the 'Privacy' tab at the top. Halfway down the page, click 'Advanced'. Here you may want to select to block third-party cookies. Be careful, though—many websites will not let you browse if you disable cookies completely.

6. **Don't read e-mails from strangers or that are unsolicited.** Everyone knows which e-mails we are talking about here. Those that are from someone with a name that is spelled in an odd manner or the subject is something you really don't care about. Turn off the preview pane in Outlook to delete messages without opening them.

7. **Don't install any Internet toolbars without knowing the company thoroughly.**

8. **Install a firewall on your home computer.** This step is not necessary for most computers on a corporate network because most of these networks already have firewalls installed. On home computers and computers not part of a corporate network, Windows XP Service Pack 2 comes with a great firewall. If you have another version of Windows, consider going to <http://www.download.com> and searching for 'Zone Alarm'. Having a firewall, a virus scanner and an anti-spyware program on your computer will provide the best possible protection against spyware and other security threats.