

## **Protect Yourself Against SpyWare and Other Unwanted Programs**



The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

1. Only download programs from websites you trust. If you are not sure whether to trust a program you want to download, ask! Contact Computer Services or your building Lab Tech / Librarian.
2. Read ALL security warnings, license agreements and privacy statements for any software you download. Make sure you understand what they are doing with your information if they require any address or phone number info.
3. NEVER click "Agree", "Yes", "No", "Ok" or any other button on a pop up window. Even saying "No" can lead to spyware getting installed. This is usually a trick. Instead, click the uppermost X, (or press ALT + F4 on the keyboard) to close. Some will try to trick you by using two X's in the upper right hand corner, click the uppermost and to the right.
4. Be cautious of anything that's "FREE". This includes free music, movies, and other files. Programs like Bear Share, Napster, KaZaa and LimeWire to name a few are raging with all sort of viruses and spyware. DON'T use them (or allow your students to use them)!! Especially on school computers.
5. Those "free arcade" type websites the kids are always on too are places to pick up large amounts of spyware. Watch the kids in your room and kick them off websites where they are playing games or watching videos. They shouldn't be doing that in school anyway (unless it's for a class, in which case you should check the site first, then give the kids direct links to what you want them to use) and it makes for PC's that don't run correctly, thus causing other students and teachers not to be able to work.
6. Use AdAware and Spybot weekly if you are on the Internet a lot.
7. FOR HOME USERS, use a firewall if you are on a broadband connection such as Road Runner or DSL. A basic PC firewall acts as a barrier between your PC and the Internet. The firewall's goal: to prevent Internet threats from spreading to your computer. Remember, connecting to the Internet is like opening a door to your computer. Through that door, you can easily go online to shop, read the latest news, send e-mail, and more. But an open door also allows hackers to easily gain access to your PC. Windows XP Service Pack 2 has a built in firewall.
8. Run Windows Update regularly. Windows is full of programming holes that can allow a hacker to gain access to personal information, or even your PC. Running Windows Update will connect directly to Microsoft and download any fixes that are available to patch these programming holes that hackers use. It can also help guard against viruses.

9. Don't trust programs other than AdAware, Spybot, Microsoft's spyware cleaner, McAfee, Norton or TrendMicro. PLEASE CHECK WITH COMPUTER SERVICES BEFORE DOWNLOADING ANYTHING BUT THESE PROGRAMS. Some companies will advertise that they are anti spyware, but really ARE spyware. Ask before downloading anything that advertises they are anti spyware. A comprehensive list of rogue spyware programs to stay away from can be found here.

[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

We have had issues in school with people installing with many of the programs found on this list without checking with Computer Services first. Save yourself computer headaches by cross referencing this list and contacting us first. This page also has a reputable software list for trusted anti spyware software.

10. Use another browser such as Mozilla's FireFox or Netscape. While still targeted by spyware and viruses, they are LESS susceptible than Microsoft's Internet Explorer. These can be obtained from the following sites:  
Mozilla's FireFox: <http://www.mozilla.com/>  
Netscape: <http://browser.netscape.com/ns8/>
11. Don't click on links in spam that claim to offer anti-spyware software. Some software offered in spam actually installs spyware.
12. Minimize "drive-by" downloads. Make sure your browser security setting is high enough to detect unauthorized downloads, for example, at least the "Medium" setting for Internet Explorer. Keep your browser updated. For help on how to do this, please contact Computer Services.
13. When entering personal information (i.e. Credit Card info), always look for the web address to start with HTTPS://, or a little lock icon in the lower right hand corner of your web browser. In Internet Explorer it looks like this:  .  
In Mozilla it looks like this:  The lock being locked means the page is secure and thus the information being sent is encrypted.
14. Check out the following site for more info!  
<http://www.ftc.gov/infosecurity/>
15. ASK QUESTIONS!! That's what the Computer Services Staff is here for. One of us will either have an answer or we can find it.