Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, spyware is designed to exploit infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

The more benign spyware and adware simply monitors and tracks your the sites you visit on the web so that companies can determine the web-surfing habits of their users and try to pinpoint their marketing efforts. However, many forms of spyware go beyond simple tracking and actually monitor keystrokes and capture passwords and other functions which cross the line and pose a definite security risk.

How can you protect yourself from these insidious little programs? Ironically, many users unwittingly agree to install these programs. In fact, removing some spyware and adware might render some freeware or shareware programs useless. Below are 5 easy steps you can follow to try to avoid and, if not avoid, at least detect and remove these programs from your computer system:

1. Be Careful Where You Download: Unscrupulous programs often come from unscrupulous sites. If you are looking for a freeware or shareware program for a specific purpose try searching reputable sites like tucows.com or download.com.
2. Read the EULA: What is an EULA? End User License Agreement. It's all of the technical and legal gibberish in that box above the radio buttons that say "No, I do not accept" or "Yes, I have read and accept these terms". Most people consider this a nuisance and click on "yes" without having read a word. The EULA is a legal agreement you are making with the software vendor. Without reading it you may be unwittingly agreeing to install spyware or a variety of other questionable actions that may not be worth it to you. Sometimes the better answer is "No, I do not accept."
3. Read Before You Click: Sometimes when you visit a web site a text box might pop up. Like the EULA, many users simply consider these a nuisance and will just click away to make

the box disappear. Users will click "yes" or "ok" without stopping to see that the box said "would you like to install our spyware program?" Ok, admittedly they don't generally come out and say it that directly, but that is all the more reason you should stop to read those messages before you click "ok".

4. Protect Your System: Antivirus software is somewhat misnamed these days. Viruses are but a small part of the malicious code these programs protect you from. Antivirus has expanded to include worms, trojans, vulnerability exploits, jokes and hoaxes and even spyware and adware.

5. Scan Your System: Even with antivirus software, firewalls and other protective measures some spyware or adware may eventually make it through to your system. There are now many free and commercial software packages available to scan your computer for spyware and other malicious programs. We have listed a few of them below.

- Lavasoft Ad-Aware
- Spybot Search & Destroy
- Microsoft AntiSpyware (beta)
- filehippo list of anti-spyware programs