

Spyware, Adware & Malware

1. **Malware**, short for *malicious software*, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of several U.S. states, including California. Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.
2. **Spyware** is a type of malware that is installed on computers and collects information about users without their knowledge. The presence of spyware is typically hidden from the user. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of internet or functionality of other programs. In response to the emergence of spyware, a small industry has sprung up dealing in anti-spyware software. Running anti-spyware software has become a widely recognized element of computer security practices for computers, especially those running Microsoft Windows. A number of jurisdictions have passed anti-spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.
3. **Adware** or advertising-supported software is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software. Adware can also download and install spyware. Advertising functions are integrated into or bundled with the software, which is often designed to note what Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. Adware is usually seen by the developer as a way to recover development costs, and in some cases it may allow the software to be provided to the user free of charge or at a reduced price. The income derived from presenting advertisements to the user may allow or motivate the developer to continue to develop, maintain and upgrade the software product. Conversely, the advertisements may be seen by the user as interruptions or annoyances or as distractions from the task at hand.

4. **Cookies** are text files used to track visitor information. Good Cookies save you time logging in next time you visit. Cookies are not Spyware. Information: <http://cookiescache.tripod.com>
5. **Online Tracking** - how to opt-out: www.selectout.org
6. **Phishing emails** are attempts to get you to give up personal information.
<http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp>
7. **Anti-malware programs** can combat malware in two ways:
 - 1) They can provide **real time protection** against the installation of malware software on a computer. This type of spyware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming network data for malware software and blocks any threats it comes across.
 - 2) Anti-malware software programs can be used solely for **detection and removal** of malware software that has already been installed onto a computer. This type of malware protection is normally much easier to use and more popular. This type of anti-malware software scans the contents of the windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.
8. **Free programs** - Many programmers and some commercial firms have released products dedicated to remove or block spyware.
 - 1) Lavasoft's Ad-Aware - <http://www.lavasoft.com/>
 - 2) Spybot - Search & Destroy - <http://www.safer-networking.org/en/download/>
 - 3) Malwarebytes - <http://www.malwarebytes.org/>
 - 4) Windows Defender is included as standard with Windows Vista and Windows 7 - <http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>
 - 5) Windows Security Essentials- http://www.microsoft.com/security_essentials/
9. All of the programs discussed, along with a list of free anti-virus programs and computer maintenance guidance, can be downloaded directly from a site developed by **Applications, etc.** a local father-son computer repair firm. <http://www.aehost.net/>
10. Additional copies of the **handout** may be viewed on the **Mission Oaks Computer Club's** website, www.missionoakscomputerclub.org/, on the Links page, under Education.
11. The Mission Oaks Computer Club meets on the 2nd Thursday of each month from 1-3 PM at the Mission Oaks Community Center, 4701 Gibbons Drive, Carmichael CA.