



Rotary Club of Sedona

District 5490, Club #1230
PO Box 2170
Sedona, Arizona 86339
www.sedonarotary.org

Service Above Self

January 15th Meeting
Rob Adams, Problems Facing the Next Mayor

Upcoming Meetings:

January 22nd Board Meeting, 11:00 A.M.

Computers today, when connected to the Web, frequently have severe problems. Spyware, Worms, and Virus's are each a very a very serious and real threat to all users. The following is presented for your information (HL). Avoiding these problems requires the installation and use of Anti-Virus, and Anti Spyware programs. Avoid infection, removal after infection can not restore the destroyed information. Computers with more than 6,000 infections are common.

Spyware From Wikipedia, the free encyclopedia

Spyware is [computer software](#) that is installed [surreptitiously](#) on a [personal computer](#) to intercept or take partial control over the user's interaction with the computer, without the user's [informed consent](#).

While the term *spyware* suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of [personal information](#), but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting [Web browser](#) activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of [Internet](#) or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term [privacy-invasive software](#).

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](#) best practices for [Microsoft Windows desktop computers](#). A number of jurisdictions have passed anti-spyware laws, which usually target any software that is [surreptitiously](#) installed to control a user's computer.

History and development

The first recorded use of the term [spyware](#) occurred on [October 16, 1995](#) in a [Usenet](#) post that poked fun at [Microsoft's business model](#).^[1] *Spyware* at first denoted [hardware](#) meant for [espionage](#) purposes. However, in early 2000 the founder of [Zone Labs](#), Gregor Freund, used the term in a [press release](#) for the [ZoneAlarm Personal Firewall](#).^[2] Since then, "spyware" has taken on its present sense.^[2] According to a 2005 study by [AOL](#) and the National Cyber-Security Alliance, 61 percent of surveyed users' computers had some form of spyware. 92 percent of surveyed users with spyware reported that they did not know of its presence, and 91 percent reported that they had not given permission for the installation of the spyware.^[3] [As of 2006](#), spyware has become one of the preeminent security threats to computer systems

running Microsoft Windows [operating systems](#). In an estimate based on customer-sent scan logs, Webroot Software, makers of [Spy Sweeper](#), said that nine out of ten computers connected to the Internet are infected.^[4] Computers where [Internet Explorer](#) (IE) is the primary [browser](#) are particularly vulnerable to such attacks not only because IE is the most widely-used,^[5] but because its tight integration with Windows allows spyware access to crucial parts of the operating system.^{[6][5]}

Before Internet Explorer 7 was released, the browser would automatically display an installation window for any [ActiveX](#) component that a website wanted to install. The combination of user naiveté towards [malware](#) and the assumption by Internet Explorer that all ActiveX components are benign, led, in part, to the massive spread of spyware. Many spyware components would also make use of flaws in [Javascript](#), Internet Explorer and Windows to install without user knowledge or permission.

The [registry](#) also contains numerous locations that allow software to be executed automatically when the operating system boots. Spyware often exploits this design to help it circumvent attempts at removal. The spyware typically will link itself from each of location in the [registry](#) that allows execution. Once running, the spyware will periodically check if any of these links are removed. If so, they will be automatically restored. This ensures that the spyware will execute when the operating system is booted even if some (or most) of the registry links are removed.

Spyware, adware and tracking

The term [adware](#) frequently refers to any software which displays advertisements, whether or not the user has consented. Programs such as the [Eudora](#) mail client display advertisements as an alternative to [shareware](#) registration fees. These classify as "adware" in the sense of advertising-supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and provides the user with a specific service.

Although most adware is *spyware* in a different sense for a different reason: it displays advertisements related to what it finds from spying on you. [Claria Corporation](#)'s Gator Software and Exact Advertising's BargainBuddy are examples. Visited Web sites frequently install Gator on client machines in a surreptitious manner, and it directs revenue to the installing site and to Claria by displaying advertisements to the user. The user receives many [pop-up advertisements](#).

Other spyware behavior, such as reporting on websites the user visits, occurs in the background. The data is used for "targeted" advertisement impressions. The prevalence of spyware has cast suspicion upon other programs that track Web browsing, even for statistical or research purposes. Some observers describe the [Alexa Toolbar](#), an Internet Explorer plug-in published by [Amazon.com](#), as spyware, and some anti-spyware programs such as [AdAware](#) report it as such. Many of these adware distributing companies are backed by millions of dollars of adware-generating revenues. Adware and spyware are similar to viruses in that they can be malicious in nature, however, people are now profiting from these threats making them more and more popular.

Similarly, software bundled with free, advertising-supported programs such as [P2P](#) act as spyware, (and if removed disable the 'parent' program) yet people are willing to download it. This presents a dilemma for proprietors of anti-spyware products whose removal tools may inadvertently disable wanted programs. For example, [recent test results](#) show that bundled software (WhenUSave) is ignored by popular anti-spyware program [AdAware](#), (but removed as spyware by most scanners) because it is part of the popular (but recently decommissioned) Edonkey client. To address this dilemma, the [Anti-Spyware Coalition](#) has been working on building consensus within the anti-spyware industry as to what is and isn't acceptable software behavior. To accomplish their goal, this group of anti-spyware companies, academics, and consumer groups have collectively published a series of documents including a [definition of spyware](#), [risk model](#), and [best practices](#) document.