



# Digital Cowboy Computers

www.digitalcowboycomputers.com

Microsoft Certified  
Professional

John Wheeler  
(937)672-3403

## RE: Malicious software (“spyware”, “adware”, “malware”)

**Malicious Software Explained:** One of the biggest threats to computer users on the Internet today is malicious software. It can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up. Malicious software programs usually cause your computer to become unbearably slow and unstable in addition to their specific malevolent mission. Many of them will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean.

You can get infected by malicious software in several ways. Malicious software often comes bundled with other programs (Kazaa, iMesh and other file sharing programs, typically seem to be the biggest bundlers). These malicious programs, usually pop-up ads, send revenue from the ads to the program's authors. Others are installed from websites, pretending to be software needed to view the website. Still others, most notably some of the CoolWebSearch variants, install themselves through holes in Internet Explorer like a virus would, requiring you to do nothing but visit the wrong web page to get infected. Finally, the remainder must be installed by the user (typically done when they use shareware or “free” downloaded programs from the Internet).

Unfortunately, getting infected with malicious software is usually much easier than getting rid of it. Once you get malicious software on your computer, it tends to multiply as it redirects you to other websites that install more malicious software on your machine.

Although there is no official breakdown, we can divide malicious software into several broad categories: adware, spyware, hijackers, toolbars and dialers. Most, malicious software programs will fit into more than one category. Most products that call themselves spyware or adware removers will actually remove almost all types of malicious software. The descriptions of each category are listed below.

**Adware:** Adware is the class of programs that place advertisements on your screen. Adware (also called advertising-supported software) is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. Typically this installation is performed without the user's explicit consent (they do not let you know exactly what you are installing) and is not announced at the time of the installation.

These advertisements may be in the form of pop-ups, pop-unders, advertisements embedded in programs, advertisements placed on top of ads in web sites, or any other way the authors can think



# Digital Cowboy Computers

Microsoft® Certified  
Professional

[www.digitalcowboycomputers.com](http://www.digitalcowboycomputers.com)

**John Wheeler**  
**(937)672-3403**

of showing you an ad. The pop-ups generally will not be stopped by pop-up stoppers and often are not dependent on your having Internet Explorer open. They may show up when you are playing a game, writing a document, listening to music or anything else. Should you be surfing, the advertisements will often be related to the web page you are viewing.

**Spyware:** 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 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.

Programs classified as spyware send information about you and your computer to somebody else. Some spyware simply relays the addresses of sites you visit or terms you search for to a server somewhere. Others may send back information you type into forms in Internet Explorer or the names of files you download. Still others search your hard drive and report back what programs you have installed, contents of your e-mail client's address book (usually to be sold to spammers), or any other information about or on your computer – things such as your name, browser history, login names and passwords, credit card numbers, and your phone number and address.

Spyware often works in conjunction with toolbars. It may also use a program that is always running in the background to collect data, or may integrate itself into your Internet browser, allowing it to run undetected whenever your Internet browser is open.

**Malware:** Malware (the slang for "malicious software") is a type of software designed to take over and/or damage a computer user's operating system, without his or her knowledge or approval. Once installed, it is often very difficult to remove, and depending on the severity of the program installed, its handiwork can range in degree from the slightly annoying (such as unwanted pop up ads while a user is performing regular computing tasks on or offline), to irreparable damage requiring the reformatting of one's hard drive. Examples of malware include viruses and trojan horses, website redirection, simple pop-up advertisements and items listed below:

- **Hijackers:** Hijackers take control of various parts of your web browser, including your home page, search pages, and search bar. They may also redirect you to certain sites should you mistype an address or prevent you from going to a website they would rather you not, such as sites that combat malicious software. Some will even redirect you to their own search engine when you attempt a search.



# Digital Cowboy Computers

Microsoft Certified  
Professional

[www.digitalcowboycomputers.com](http://www.digitalcowboycomputers.com)

**John Wheeler**  
**(937)672-3403**

- **Toolbars:** Toolbars plug into your Internet browser and provide additional functionality such as search forms or pop-up blockers. The Google and Yahoo! toolbars are probably the most common legitimate examples, and malicious software toolbars often attempt to emulate their functionality and look. Malicious software toolbars almost always include characteristics of the other malicious software categories, which is usually what gets it classified as “malware”. Any toolbar that is installed through underhanded means falls into the category of malicious software.
- **Dialers:** Dialers are programs that set up your modem connection to connect to a 1-900 number. This provides the number's owner with revenue while leaving you with a large phone bill. Most dialers, however, are installed quietly and attempt to do their dirty work without being detected. This is a relatively new concept and many people find it very hard to convince the phone company to cancel the large bill.

**The short summary on “adware”, “spyware” and “malware”:** It is not uncommon for people to confuse "adware" with "spyware" and "malware", especially since these concepts overlap. For example, if one user installs "adware" on a computer, and consents to a tracking feature, the "adware" become "spyware" when another user visits that computer, and interacts with and is tracked by the "adware" without her consent. “Spyware” can quickly become “malware” when a URL redirection directs the user to a website that automatically downloads a piece of software which infects the user’s computer. Whatever you want to call them (“adware”, “spyware” or “malware”), 99% of the time, the user does not need nor want these malicious software packages installed on their computer.

**Why does adware exist?** Adware helps some developers recover programming development costs, and it may allow the software to be provided to the user of the application free of charge or at a reduced price: due to the advertising, the programmer may still profit from the wide use of their work, motivating them to write, maintain, and upgrade the software product.

Some adware is also shareware, and as such, it may be used as term of distinction used to differentiate between types of shareware software. What differentiates adware from other shareware is that it is primarily advertising supported. Users may also be given the option to pay for a "registered" or "licensed" copy, which typically does away with the advertisements. However, most users do not opt to pay the fee required to get a “licensed” or “registered” copy of the software. Thus, they continue using the “free” version which contains the adware programs. Some common examples of this are “free” games people download from the Internet.

**How does malicious software spread?** The most important aspect is the initial installation of “adware” may be fairly harmless to the computer. However, during one of the pop-ups, the user may be redirected to a website that installs another malicious software package. The next round of



# Digital Cowboy Computers

Microsoft® Certified  
Professional

[www.digitalcowboycomputers.com](http://www.digitalcowboycomputers.com)

**John Wheeler**  
**(937)672-3403**

redirects can cause the same issue. This is how malicious software is able to spread itself across the Internet. As the computer is redirected to more websites by the malicious software, there are more opportunities for malicious software to install itself.

Imagine if the user is using two (2) illegal song download programs, has three (3) “free” web games and visits a “questionable” website. That is six (6) opportunities for malicious software to install itself on the computer. It is easy to see how malicious software is able to infect and dominate a user’s computer in a short period of time.

**How to prevent malicious software from infecting your machine:** Malware is responsible for slowdowns and crashes. Besides hurting the productivity and patience of those using infected PCs, it is a productivity waster — a problem which takes time away from other issues. The best method of protection is abstaining from visiting sites that you do not fully trust. Never accept or OK any windows dialogue box without first reading it and understanding what it is telling you. Be careful when pop-ups and advertisements appear, they can lead you to worse infections just by clicking a simple Yes or OK button. Surf carefully, pay attention to what you are clicking and do not be afraid to say NO, CANCEL or to click the X in the top right corner of the screen (to close the window out). Finally, keep your computer’s operating system up to date. Many exploits may be eliminated by your operating system being up to date.

**How to remove malicious software from your machine:** Download and install AdAware and Spybot from the Internet. Both are “freeware” programs designed to specifically find and eliminate malicious software from your computer. Always make sure you update both programs right before you run a scan on your system. Do the scans at least one time every week or two (more often if you like). Finally, if something feels “wrong” with your computer (running slow, doing something “weird”, etc), do the scans and see if it is a malicious software program.

If you need assistance with determining if your machine(s) are infected with malicious software, please feel free to call Digital Cowboy Computers. We specialize in finding and removing malicious software while protecting your valuable data.

John Wheeler  
937-672-3403  
[www.digitalcowboycomputers.com](http://www.digitalcowboycomputers.com)