**Malware, Spyware, Adware & Viruses**

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software

Spyware is any software that covertly gathers user information through the user’s Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. However, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about E-mail addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that users can unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are readily available on the internet. But more and more, users can be infected with spyware simply by surfing the internet. Many times spyware objects are invisibly and unethically embedded into web pages by the webmaster. And by simply visiting one of these websites, the user is unsuspectingly infected.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer’s memory resources and also by eating bandwidth as it sends information back to the Spyware’s home base via the user’s Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising, and/or marketing purposes, or sell the information to another party.

Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers

Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.

Viruses, Worms and Trojan Horses:

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".[1][2][3] Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent

A Worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well. The term worm was coined by John Brunner, a science fiction writer, in his 1975 novel Shockwave Rider. The hero, a talented programmer, created self-replicating computer programs that tunneled their way through a worldwide network.

A Trojan horse is simply a malicious computer program that damages your computer system upon installation. The program claims to do one thing, such as pretending to be a game, but instead do something else when you run them. Some nasty Trojans will actually attempt to erase your hard drive. They were originally named after the historic Trojan horse used by the Greeks to conquer Troy because the first Trojan horse programs pretended to be innocent games or applications. Trojan horses have no way to replicate themselves automatically.

**References**:

1. "Malware definition" - techterms.com
2. "Spyware, Adware and Malware”— http://en.wikipedia.org/wiki/Adware
3. “Computer virus” - Encyclopedia Britannica. Britannica.com
4. "Viruses and other forms of malicious software". Princeton University Office of Information Technology