

Types of threat

- *Adware*
Programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purposes. This is often accomplished by tracking information related to Internet browser usage or habits.

Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger adware by accepting an End User License Agreement from a software program linked to the adware.
- *Dialers*
Programs that use a system, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.
- *Hack Tools*
Tools used by a hacker to gain unauthorized access to your computer. One example of a hack tool is a keystroke logger -- a program that tracks and records individual keystrokes and can send this information back to the hacker.
- *Hoax*
Usually an email that gets mailed in chain letter fashion describing some devastating, highly unlikely type of virus. Hoaxes are detectable as having no file attachment, no reference to a third party who can validate the claim, and by the general tone of the message.
- *Joke Programs*
Programs that change or interrupt the normal behavior of your computer, creating a general distraction or nuisance. Harmless programs that cause various benign activities to display on your computer (for example, an unexpected screen saver).
- *Remote Access*
Programs that allow another computer to gain information or to attack or alter your computer, usually over the Internet. Remote access programs detected in virus scans may be recognizable commercial software, which are brought to the user's attention during the scan.
- *Spyware*
Stand-alone programs that can secretly monitor system activity. These may detect passwords or other confidential information and transmit them to another computer.

Spyware can be downloaded from Web sites (typically in shareware or freeware),

email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.

- *Trojan Horse*
A program that neither replicates nor copies itself, but causes damage or compromises the security of the computer. Typically, an individual emails a Trojan Horse to you-it does not email itself-and it may arrive in the form of a joke program or software of some sort.
- *Virus*
A program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though, many do a large amount of damage as well.
- *Worm*
A program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.