Computer virus infections have reached epidemic proportions in the last few years. Although there are a number of maladies that can infect your PC, including viruses, worms and Trojan horses, we will concentrate on viruses here.

A **COMPUTER VIRUS** is a program that reproduces by attaching itself to another program or document, similar to a biological virus. The virus code is executed when the infected program is run.

Five most common types:

1). Macro virus - this type of virus usually comes as part of a document or spreadsheet, often in email. Microsoft provides a version of Visual BASIC in its Office product, (for example, in Word and Excel) to allow users to write custom routines. These routines are called macros. Many of the current macro viruses are written in this language and attached to Word documents. This capability is powerful, but allows viruses to be written and executed much more easily than by using other methods. Microsoft applications now have a feature called "Macro Virus Protection ," enabled by default that asks the user before automatically executing macros. The Melissa and ILOVEYOU viruses are examples of macro viruses.

2). Boot sector virus - this type of virus overwrites the boot sector on your hard drive or floppy drive. The boot sector holds information necessary for your PC to boot up, so the virus effectively disables your PC. Although floppy disk usage is diminishing, they are still the most common means by which these viruses spread. Boot sector viruses can also infect drives formatted with the NTFS file system. Examples of boot sector viruses are F-Prot and AVP (Kaspersky). There are similar viruses called Master Boot Record (MBR) viruses, which infect the MBR. Examples of these viruses are NYB, AntiExe, and Unashamed.

3). File infector virus - this type of virus attaches itself to executables, for example .com and .exe files. The virus spreads when the program is run, loading itself into memory and/or attaching itself to other programs on your system. It usually spreads to other computers when infected programs are shared. Examples of known file infectors include the Jerusalem and Cascade viruses.

4.) Stealth virus - this type of virus tries to fool antivirus software by catching its requests to the operating system (asking to open a file, for example). In this way, the stealth virus can provide its own clean version of the file to the antivirus software. The best way to defeat this type of virus is to boot from a known clean disk. The FRODO or 4096 virus is an example of a stealth virus, hiding changes in the file size of infectedfiles or directories, to try and avoid detection.

5). Self-modifying virus - this type of virus was designed to avoid detection by antivirus software by changing itself internally. There are two types of self-modifying viruses:

> Polymorphic virus - a polymorphic virus infects files with modified (usually encrypted) operational versions of itself, which it decrypts before executing. The virus and the decryption module are both modified on each execution, thus making it difficult to detect. The "Dark Avenger's Mutation Engine" (also known as MTE or DAME) has been released by virus writers to add this capability to any virus, but is now detectable by most antivirus tools.
>
> Metamorphic virus - a metamorphic virus rewrites itself completely each time it infects a new executable. This strategy requires the virus to include a metamorphic engine, making it large and complex, but also very difficult to detect. An example of a metamorphic virus is Win95.Zmist.A.