**Computer viruses** are programs written by "mean" people. These virus programs are placed into a commonly used program so that program will run the attached virus program as it boots, therefore, it is said that the virus "infects" the executable file or program. Viruses work the same ways in Windows or DOS machines by infecting zip or exe files. A virus is inactive until you execute an infected program or application OR start your computer from a disk that has infected system files. Once a virus is active, it loads into your computer's memory and may save itself to your hard drive or copies itself to applications or system files on disks you use. Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files, or even erasing your entire hard drive.

Viruses begin to work and spread when you start up the program or application of which the virus is present. For example, a word processing program that contains a virus will place the virus in memory every time the word processing program is run. Once in memory, one of a number of things can happen. The virus may be programmed to attach to other applications, disks or folders. It may infect a network if given the opportunity.

Viruses behave in different ways. Some viruses stay active only when the application it is part of is running. Turn the computer off and the virus is inactive. Other viruses will operate every time you turn on your computer after infecting a system file or network.

Computer viruses are mysterious and grab our attention. On the one hand, viruses show us how vulnerable we are. A properly engineered virus can have an amazing effect on the worldwide Internet. On the other hand, they show how sophisticated and interconnected human beings have become.

When you listen to the news, you hear about many different forms of electronic infection. The most common are:

**Viruses** - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs).

**E-mail viruses** - An e-mail virus moves around in e-mail messages and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

**Worms** - 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.

A computer virus is most often defined as “a malicious code of computer programming”. What this means is that a computer virus is just another software – only written with not so very noble intentions. A computer virus is designed to install, propagate and cause damage to computer files and data without the knowledge and/or express permission of the user. A computer virus can only survive, attack and propagate in computer memory. Computer memory is usually the RAM (and all different variations of it) and disk storage (hard, floppy and everything in between). Besides this you will not find computer viruses in your monitor, keyboard.  
  
The first step in any virus attack is always the invasion. This is when the virus actually enters the computer system from an outside source. Much of the effort in preventing a virus attack lies in understanding what these virus entry points are and how best to monitor and block out any possible intrusion. All viruses enter the computer system through two main entry points: the disk drives and the network adapter cards. The disk drives may be any sort of disk drive (hard, floppy, CD, Zip). This makes any disks or CDs that you insert into these drives a possible source of virus infection. The network adapter card is most likely your computer network and/or modem card connected to the local Intranet and/or the Internet. Virus enters through the network card most likely disguised in the form of attachments in e-mails. These attachments are often program files and office documents containing macros. Besides this, certain web pages that we visit on the Internet may also contain harmful programming codes that might transfer virus or virus-like codes into our system. To guard our systems against virus intrusion from these sources, many good anti-virus programs allows users to completely scan all files read form disk drives or downloaded from the Intranet/Internet.

How do virus infections occur? The act of infection often begins with a harmless looking action such as opening a file (like a video game or a Word document) that one often gets in e-mail attachments or while accessing any disk in a disk drive. These actions inadvertently activate the virus lurking in these files and disks. The virus then installs itself into the computer’s memory.   
  
This is where things get nasty. After entering the computer memory, a virus often immediately sets out to multiply and spread duplicate copies of itself across the main data storage device (most often the hard disk drive). It does this by copying itself into as many files it can find on the disk drive. Later when users transfers or copies these files to their friends and colleagues, the virus gain entry into ever increasing number of systems. If the virus has found its way to this level of the user’s computer, the user runs a high risk of permanent damage to data and hardware. But such a level of infection only happens to two types of users. The first are those who do not employ any kind of anti-virus measures (or if they do, it obviously isn’t doing a good job). The second are those who do have good anti-virus programs installed and running but did not bother updating their software with the latest virus data files. As a result newer viruses can actually use the anti-virus programs to infect an even greater number of files. So we can see here that having good anti-virus software isn’t enough. One must constantly keep it updated (preferably on a monthly basis).   
  
If a virus were to just spread itself, users might not have much to worry about. But the worst is yet to come. Many viruses contain what is called a payload. This is the destructive sequence that is activated on a certain trigger. The trigger may be the arrival of a particular date or an action done by the user. The effect of the payload can be anything as benign as some harmless message appearing on screen to as frightening as the destruction of the disk drive’s boot record – making it completely unusable and in most cases completely irreparable. Indeed it is the later that causes permanent loss of data and hardware and which is responsible for the virus’ notorious reputation. If a virus is capable of unleashing its payload on the user’s system, this indicates a serious breach of security on part of the user. It’s time for the user to learn from the experience and never let computer virus have a second chance.   
  
A file [virus](http://stason.org/TULARC/security/computer-virus/4-How-do-viruses-work-Computer-virus.html) attaches itself to a file, usually an executable application (e.g. a word processing program or a DOS program). In general, file viruses don't infect data files. However, data files can contain embedded executable code such as macros, which may be used by virus or trojan writers. Recent versions of Microsoft Word are particularly vulnerable to this kind of threat. Text files such as batch files, postscript files, and source code which contain commands that can be compiled or interpreted by another program are potential targets for malware (malicious software), though such malware is not at present common.

The following virus types are more fully defined :  
  
**1) Boot sector viruses** alter the program that is in the first sector (boot sector) of every DOS-formatted disk. Generally, a boot sector infector executes its own code (which usually infects the boot sector or partition sector of the [hard](http://stason.org/TULARC/security/computer-virus/4-How-do-viruses-work-Computer-virus.html) disk), then continues the PC bootup (start-up) process. In most cases, all write-enabled floppies used on that PC from then on will become infected. Also sometimes called boot record infectors, [system](http://www.pcguide.com/care/data/virus/bgTypes-c.html) viruses, or boot viruses, these programs attack the vulnerable [boot program](http://www.pcguide.com/ref/hdd/file/struct_MBR.htm) that is stored on every bootable floppy disk or hard disk. This code is executed by the system when the PC is started up, making it a juicy target for virus writers: by installing themselves here they guarantee that their code will be executed whenever the system is started up, giving them full control over the system to do what they wish. They are spread most commonly through infected bootable floppy disks.

1. **Multipartite viruses** have some of the features of both the above types of virus. Typically, when an infected \*file\* is executed, it infects the hard disk boot sector or partition sector, and thus infects subsequent floppies used or formatted on the target system.  
   **3) Macro viruses** typically infect global settings files such as Word templates so that subsequently edited documents are contaminated with the infective macros. Macro Viruses are the newest type of virus, these clever programs make use of the built-in programming languages in popular programs such as Microsoft Word and Microsoft Excel. These programs allow users to create programs that automate tasks, called *macros*. As the macro languages have become more powerful, virus writers have created malevolent macros that, when opened unwittingly, duplicate themselves into other documents and spread just like a conventional virus would. These programs can cause just as much damage as regular viruses, despite the fact that they are very different: regular viruses are low-level machine language programs, while macro viruses are actually high-level interpreted BASIC programs! The most common type of macro virus right now infects Microsoft Word documents.  
   **4) STEALTH VIRUSES -** viruses that go to some length to conceal their presence from programs which might notice.  
   **5) POLYMORPHIC VIRUSES** - viruses that cannot be detected by searching for a simple, single sequence of bytes in a possibly-infected file, since they change with every replication.  
   **6) COMPANION VIRUSES** - viruses that spread via a file which runs instead of the file the user intended to run, and then runs the original file. For instance, the file MYAPP.EXE might be 'infected' by creating a file called MYAPP.COM. Because of the way DOS works, when the user types MYAPP at the C> prompt, MYAPP.COM is run instead of MYAPP.EXE.
2. **ARMOURED VIRUSES** - viruses that are specifically written to make it difficult for an antivirus researcher to find out how they work and what they do.
3. **File Infectors:** These viruses directly attack and modify program files, which are usually .EXE or .COM files. When the program is run, the virus executes and does whatever it wants to do. Usually it loads itself into memory and waits for a trigger to find and infect other program files. These viruses are commonly spread through infected floppy disks, over networks, and over the [Internet](http://www.pcguide.com/care/data/virus/bgTypes-c.html).

**Major Virus Types and How They Work**

Computer viruses work in the same way, including the way they tend to go around from PC to PC and then occasionally return to re -infect months or years later (in fact, there are viruses that have been circulating around since the early days of the PC that, thanks to backward compatibility, still "run" on the latest machines). Computer viruses however, differ from biological viruses in several ways: they are man-made for one thing, and they are easier to get rid of. Also, biological viruses cause symptoms as a side-effect, they do not exist to make people miserable. Most computer viruses *do* exist specifically to make people miserable.

There are three major types of viruses, each very different from the other. Of course, there are many subcategories within each group as well (and to make matters worse, there are [virus hoaxes](http://www.pcguide.com/care/data/virus/bgHoaxes-c.html) to confuse the issue):

As time goes on and virus writers get more clever, new strains and variations show up. For example, there are some viruses, termed *multipartite*, that infect both boot sectors *and* files. There are some things that are fairly universal, however: a virus is a program, and it therefore can only exist in a form that allows it to be executed as a program by the PC in some form. This means that, in general, viruses cannot exist in data files. There are a lot of myths about viruses that infect graphics pictures or email messages or recipe files. Just remember that a virus cannot do anything unless you run it, so unless you have a PC that can execute pictures or email messages somehow, it's doubtful that these can contain a virus. (Of course, you can have a virus in a program that is *attached to* an email message. But here again, this is a program, just in encoded form.)

There are also now viruses that target the BIOS program stored on the [motherboard](http://www.pcguide.com/care/data/virus/bgTypes-c.html), on systems that employ a [flash BIOS](http://www.pcguide.com/ref/mbsys/bios/comp_Flash.htm). These viruses can overwrite the system BIOS program and leave the PC in an unbootable state. (Some motherboards have jumpers that you can set to disable BIOS flashing except when you want to do it.)

Here is the general way that viruses work:

1. An infected program is run. This is either a program file (in the case of a file-infecting virus) or a boot sector program at boot time. In the case of a Microsoft Word document the virus can be activated as soon as the document that contains it is opened for reading within Microsoft Word. If the "NORMAL.DOT" document template is infected (and this is the most common target of these viruses) then the virus may be activated as soon as Microsoft Word is started up.
2. The infected program has been modified so that instead of the proper code running, the virus code runs instead. This is usually done by the virus modifying the first few instructions to "jump" to where the virus code is stored. The virus code begins to execute.
3. The virus code becomes active and takes control of the PC. There are two ways that a virus will behave when it is run: *direct-action* viruses will immediately execute, often seeking other programs to infect and/or exhibiting whatever other possibly malicious behavior their author coded into them. Many file-infector viruses are direct-action. In contrast, *memory-resident* viruses don't do anything immediately; they load themselves into memory and wait for a triggering event that will cause them to "act". Many file infectors and all boot infectors do this (boot infectors have to become memory resident, because at the time they are executed the system is just starting up and there isn't that much "interesting" for them to do immediately.)
4. What exactly the virus does depends on what the virus is written to do. Their primary goals however include replication and spreading, so viruses will generally search for new targets that they can infect. For example, a boot sector virus will attempt to install itself on hard disks or floppy disks that it finds in the system. File infectors may stay in memory and look for programs being run that they can target for infection.
5. "Malevolent" viruses that damage files or wreak havoc in other ways will often act on triggers. There are viruses that will only activate on particular days of the year (such as the infamous "Friday the 13th"), or act randomly, say, deleting a file every 8th time they are run. Some viruses do nothing other than trying to maximize their own infection to as many files and systems as possible.

As virus authors have become more "creative", they have devised increasingly more sophisticated viruses that work in different ways. In particular, newer viruses get smarter and smarter in avoiding detection. In most cases these viruses are not necessarily more hazardous than older ones, but they are harder to detect and remove using anti-virus software. Some of the tricks that authors use:

* **Polymorphing:** Some viruses are designed so that each time they infect, their appearance and size changes. These thwart simplistic virus scanners that look for predefined patterns and make detection much more difficult.
* **Stealth:** A stealth virus actively hides the changes it has made to the hard disk so that it appears that it has not infected the system. For example, a file infector might stay memory resident and misreport the size of infected files so they don't appear to be infected. Boot sector viruses can trap attempts to read the boot sector and return forged data that makes them appear to be "clean".
* **Disassembly Protection:** Many newer viruses are designed using programming tricks that make them hard to disassemble (the process of interpreting the code into a form that is easier to analyze so that the virus can be combated.)
* **Directory Viruses:** Some viruses now seek to avoid detection by avoiding modifying the file they infect directly. Instead, they change the cluster pointer in the directory entry of the file to point to the virus instead of the actual program. The virus runs its code and then executes the target program afterwards. The virus is thus able to "infect" the program without actually modifying it.

 Trojan Horses - A trojan horse is not a virus. It is a program that you run because you think it will serve a useful purpose such as a game or provides entertainment. Like a "trojan horse" it serves not as it claims, but to damage files or perhaps plants a virus into your computer. A trojan horse does not replicate or spread like a virus. Most virus checking programs detect trojan horses.

**Trojan horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your HDD). Trojan horses have no way to replicate automatically.

What has been attempted here is to give the reader a quick run down of how a virus attacks our systems. It is not meant to be exhaustive as the subject matter is very broad. In short the best cure for a virus attack is a good prevention plan coupled with knowledge, caution and good anti-virus software!   
How to Prevent a Virus Invasion!

1. Load only software from original disks or CD's. Pirated or copied software is always a risk for a virus.
2. Execute only programs of which you are familiar as to their origin. Programs sent by email should always be suspicious.
3. Computer uploads and "system configuration" changes should always be performed by the person who is responsible for the computer. Password protection should be employed.
4. Check all shareware and free programs downloaded from on-line services with a virus checking program.