

Computers get sick

by Bernie Wieser

There is no question that today we live in an information society. Computers are an integral part of our every day lives. As students, many of us rely heavily on computers to do our homework. Writing a term paper is cheap and easy using a word processor.

We put our trust in these machines to keep our information safe. "Computers are reliable. They don't need coffee breaks or sleep. They can work twenty-four hours a day, seven days a week. Computers do not make mistakes." These statements are not true. Computers can get sick, just like people, and when they do it affects you.

The term "computer virus" has been in the air lately. But what is a computer virus? Webster's dictionary defines a virus as "any group of microscopic infective agents that cause various diseases; capable of multiplying in connection with living cells." The

computer virus is much the same. But unlike a people virus, which is usually a complex protein foreign to the body, a computer virus is a program created by a person and executed on a system like any other program. Its purpose is to hide in the computer system and attach itself to healthy files or to install itself onto disks.

When a computer virus attacks it usually attaches itself to "system" or "command" files. These are the programs which the user executes to start (boot) the program and do the work. When the infected program is requested, instead of getting down and doing what it is supposed to, the virus is executed first. It usually relocates itself somewhere in the computer's memory and will run along side the host program, spreading itself to any new files or disks that the user puts into the system.

Some viruses don't even bother attaching themselves to files. They insert themselves right into the "boot track" on a disk. A computer usually

can't do anything for anybody unless it has a way of communicating with the person using it. When you turn on your machine at home it usually wants you to put a disk into the disk drive. It can then load something called the "Operating System" (OS) into the machine and execute it. The OS is the program which allows the user to talk to the computer. The boot track is the first thing the computer sees when you put in your disk, and the information on it is what tells the computer to load the OS. Usually there is not too

the OS. On some systems when the virus "gives" itself disk space, it will tell the OS that the sectors taken are "bad" and can't be used for anything else.

Unfortunately most people do not know that they have a virus until the symptoms come out. At this point it is usually too late! The symptoms vary depending on the degree of perversity of the virus' creator. Some are relatively harmless. For example, on the Apple MacIntosh computer there is a virus which will send the message "Remember Hiroshima" drifting across the

modify themselves directly whenever they are used. They use data files instead.

If you think that you have been hit by a virus then stop and get help. If you continue using your system you may be condemning other programs and data to destruction, as well as any chance you might have at recovering what was lost. However, just because there is a glitch in your system does not necessarily mean you have a virus. That is why you should get help. It is not too hard to find someone who knows

"A virus is a type of lie. There is really no one person or group to blame; it is an ethical problem."

much room in the boot track, so a virus might look for empty spaces (sectors) on the disk and copy itself onto them. Instead of the boot track loading the OS, it will load and install the virus first which in turn loads

screen whenever the internal clock points to August sixth.

Some virus' are not so nice. There are a few that will insult you and then hang your system. These are actually the good ones in this category because you know exactly when you've been hit. The bad ones will change or destroy the information on your disks without saying anything, and in this case you may not notice until all your hard work is gone.

Programs that wait for a specific time or event are called Trojan Horses, after the Greek myth in which the city of Troy was destroyed when the Trojan citizens accepted the gift of a huge wooden horse from their Greek enemies. Programs which destroy information have been affectionately called worms. A worm in an apple will eat through the flesh, destroying the integrity of it. A worm in a computer will destroy the integrity of your information. Of course, a virus does not necessarily have to have the symptoms of a Trojan Horse or a worm. It can do anything the creator has programmed it to do, and it can be as inconspicuous as possible.

So how does a user detect a virus before it is too late? As with some diseases there may be early warning signs. For example, watch the sizes and dates of creation of your command and system files. If a virus is present these should change. Most programs do not

something about the equipment you are using, so get an expert opinion before doing anything. You might even be able to get your files back.

Most of all, do not get paranoid. Some programs will update data files every now and then. Know what is going on before jumping to conclusions. Read your program manual or ask someone who uses the same programs that you do. The best place to get help is your local computer users' group.

As with all things, the best protection is prevention. Software companies were quick to jump on the virus band wagon and there are many inoculation programs available. These can be found at the local software store. There are alternatives to paying for a cure you might not need. Your local users' group may have free public domain programs which check for and remove viruses. The best way to protect yourself is to be careful.

Careful computer use is comprised of several things, most of which is common sense. Have master copies of programs which are vital to your work. Devote a disk to this copy and write protect it. The disk drive can not write to a disk which has a write protect. A virus can not spread if it has nowhere else to go.

Scrutinize all untested software. Chances are if you buy

