When a Virus Strikes

Responding to a computer virus attack

As soon as you realize a computer virus is attacking your computer :

1. Turn the power off immediately ! Rebooting without switching the power off is not enough to kill viruses in memory.
2. Boot the system using a write-protected copy of your system diskette. This should leave the hard disk inactive.
3. Use an anti-viral program to scan and disinfect the hard disk. If you don't have a program handy, get one before you turn the computer on.
4. Once you have restored the hard disk using back-up files, systemat- ically work through your floppy disks, scanning and disinfecting them.

DO's of Computer Virus Protection

DO write protect all original commercial and shareware program diskettes, especially system diskettes, DOS or other. If you haven't done this yet, do it now.

On 5.25 inch diskettes use the little black or silver stickers that come with a package of diskettes to cover up the little notch on the side. On 3.5 inch diskettes open the little sliding window in the corner.

If you do get a virus infection you will need the original program diskettes to restore lost information and contaminated files. Write protecting them ensures that they will remain free of contamination.

If your hard drive is contaminated you will need to boot the system the old-fashioned way: by booting from a DOS or other operating system diskette in drive A: Write protecting the operating system diskette ensures this boot is possible. You will protect the diskette from contamination when it is inserted into the contaminated system.

DO make regular complete back-ups of your hard drive.

Backups are the best defense against all computer catastrophes. If a virus attacked some of the damage to data on your hard drive it may be irreversable. Only with a recent backup can the directory structure and all data be restored.

You might be backing up an unsuspected virus at the same time. But after an attack you will have a better idea where the virus is in the data structure. You could delete infected files right after restoring the hard drive from a backup, before running any other programs.

DO acquire software from a reputable, secure source.

Commercial shrink-wrapped packages or shareware direct from the author are safest. Shareware from mail-order houses or downloaded from major BBSes practising anti-viral security come second. Least safe is getting software on a disk from someone else, or from a BBS not practising anti-viral measures.

DO acquire at least one anti-virus package.

Nothing you do, short of never turning on your computer, can totally protect you. But using even one package will drastically reduce your risk level. When you first get your package, run it from a write-protected diskette, scanning computer's RAM and hard drive for inspection. Then use it to scan floppy diskettes.

DO use your anti-virus package to scan new diskettes & files for viruses.

No matter what the source, scan new material coming into your system. This includes programs used by service people, pre-formatted new diskettes, blank used diskettes, diskettes received in the mail, diskettes containing only text or data, and so on.

DO quarantine new software.

Run all new commercial and shareware programs for the first time from floppy diskettes. Unless a program is a hard disk utility, running it from floppy diskettes should leave the hard disk inactive. Sound and lights from the hard drive will warn you of virus activity, particularly Trojan Horse attacks.

DO prepare an emergency response diskette kit.

DON'Ts of Computer Virus Protection

DON'T swap diskettes carelessly between computers.
Boot sector viruses are the most common sort of virus. They are spread from computer to computer by the transfer of infected floppy diskettes.

DON'T use illegal copies of operating system files.
It may be tempting to upgrade to DOS 5.0 for nothing. But these files, COMMAND.COM and so on, are the targets of most file virus infections. Using non-secure copies leaves all your system resting on an unsafe foundation. If you must steal software, steal something else.

DON'T participate in a bootleg software market.
Attaching a virus to a desirable commercial product and then circulating copies is a favorite ploy for the rats who spread viruses.

DON'T leave diskettes sitting in disk drives if they aren't being used.
The best barrier against virus infection is the physical separation of disks. A computer virus can't leap through the six inches of empty space of a hard disk and a diskette case.

DON'T keep many files in the root directory of your hard drive.
The root directory is the target of many viruses because it contains main system files. Putting a lot of other files in the root directory makes it fertile soil for virus growth. In particular, don't put new software in the root directory. You might put a new virus right beside its target files.

DON'T trust hard disks loaded with software straight from the computer store.
Computer stores are vulnerable to virus infections too. Often they load up hard disks from copies of original diskettes. There have been cases of stores unknowingly including viruses with every package deal they sell.

DON'T trust packages with named system files, such as AUTOEXEC.BAT, in them.
In the 80's this was considered a convenient way to organize packages. Unfortunately, it is also a strategy for spreading viruses. Software developers have abandoned it.

DON'T take it for granted that new commercial software is virus-free. Scan it.
There has been more than one case of new commercial software being infected. In fact, contrary to popular opinion, it may be more likely to catch a virus from commercial software than shareware. Shareware vendors and BBSes practice active anti-virus security. Commercial vendors smugly assume they are immune.