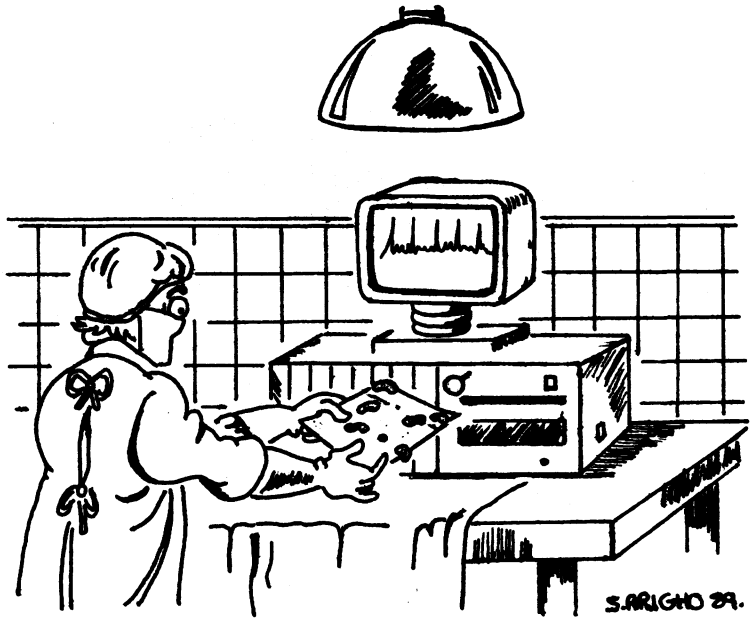
VIRUSES – HOW TO PREVENT INFECTION

Time was when the only bugs in a computer were the programmer's coding mistakes; and de–bugging, although difficult and often tedious, was one of the programmers chores.

These days, computer users have to worry about a more recent pestilience – the computer virus. Viruses are sophisticated programs written by practical jokers, malicious mischief makers, or 'hackers', and sometimes by saboteurs whose aim is to cause havoc to a computer system.

The programs are called viruses since they propagate in a similar manner to the biological kind. Generally, they surreptiously attach themselves to a host file (or reside in your computer's memory) and are activated when it is activated

Once a virus attaches itself to a target system or files on a disk (i.e. your personal computer) it becomes a carrier. Contacts with any other computer or media (e.g. host data communications or diskettes) used by your machine may also automatically become infected spreading the infection to the next computer and so on.



Often the virus remains dormant giving it time to be transferred numerous times before detection. When triggered by an event it creates mischief ranging from messages flashed across your screen to irretrievable destruction of data and irreparable damage to expensive devices and peripherals.There have been several attacks at major organisations throughout the world including NASA (Apple Macintosh Scores Virus), Lehigh University (PC Lehigh Virus), · US Department of Defence Arpanet Research Network (The Arpanet Virus), and Peace Virus which makes its way into distribution copies of Aldus Freehank, a graphics program for the Apple Mac.

Hence, viruses are a serious problem, and they have the potential to become even more troublesome. The threat of an attack should be considered and treated like any other disaster – it is unpredictable and potentially catastrophic. It is advisable to institute reasonable preventative measures of security relative to the risk of infection and sensitivity of your data.

In an office environment, a virus can be introduced in several ways:

- An infected diskette obtained from a doubtful source might be hand-carried to a workstation;
- Programs obtained by dialling into one of the many electronic bulletin boards and inadvertently transferred into a workstation might be infected; or
- A file received via host communications with a mainframe system or a Network and downloaded into a workstation can carry infected program code.

There is no 100% failsafe or guaranteed means of protecting your computer. Articles in the computer press and magazines have provided increased publicity to the serious dangers of business disruption and loss of data should such an eventuality occur to computer users.

Unfortunately, viruses are on the increase and dangers of infection are very real. However, experts caution against panic.

The software market is capitalising on offerings of anti–viral technical deterrents ("vaccine programs") to computer viruses, the latest "new and improved" security systems and virus recovery programs. Whilst these are highly specific and practical and may assist you before or after a virus attack, by nature they have a limited protection.

Preventative Measures

In general terms your most effective means of protection is good judgment and adherence to common sense procedures and policies. Reasonable protective precautions, for responsible computer users, to safeguard your systems include:

- Using only software obtained from reputable sources (avoid 3rd party software and unauthorised copies of games).
- Sensible and restricted use of 'bootable' diskettes (e.g. demonstration diskettes requiring you to start up or 'boot' your computer from them) – since diskette transfer is the commonest means of virus propagation.
- Being alert if you frequently receive data from external sources or have external communication links via dial–in facilities – these are the highest risk.
- Performing regular backups and archiving of important data – invaluable for restoration of a disabled system.
- Secure your computer and floppy diskettes from unauthorised access – (e.g. locking your office, PC etc. when not in use).

If your are vigilant, follow the do's and don'ts and remain alert to untoward behaviour on your computer your risk of contamination will be greatly diminished.

Finally, early detection of infection and containment if an outbreak does occur, is highly important. Prepare for what to do if your computer systems are compromised.

Given the lack of foolproof preventative measures a solid recovery plan is your best insurance against data loss!