Computer Viruses

While viruses have been around almost as long as the PC, they have only recently changed from a minor inconvenience to a serious menace. There are several reasons why they are now much more of a problem … many more computers are in use and there are many more ways of sharing information between them.

-- PC Guide

What is a 'Virus'?

A computer virus is a program or piece of code that operates by attaching itself to some other program or downloaded file. When this program starts, the virus code unintentionally runs, replicates itself and infects other programs or documents on the PC. A computer virus spreads mainly via e-mail attachments, downloadable files from the Internet or floppy disks. Virus infection can be prevented by installing (and maintaining) anti-virus software, among other strategies, some of which are outlined in this advice sheet.

A computer virus can seriously damage or completely destroy files or software on a computer. The result is that files may be lost permanently, educational programs may not function correctly or the overall performance of a computer may be slowed down. The process involved in repairing the damage can be time consuming and expensive.

How Does a Virus Work?

There are two ways in which a virus behaves when activated.

- **Direct Action** – the virus is activated immediately, frequently relying on other programs to infect and carry out specific behaviour encoded by the author of the virus.
- **Memory Resident** – the virus is loaded into the computer's memory and is activated by a triggering event. A triggering event can be either a date or a certain combination of keystrokes.

The damage caused by computer viruses varies from poor computer performance to erasing the hard drive.

Types of Virus

Boot Sector Infectors
These viruses infect the **boot sector** on floppy disks and hard drives. The boot sector is a small program that initialises the operating system. By placing its virus code in the boot sector, a virus is guaranteed to be executed. It can load itself into the memory immediately and it is able to run whenever the computer is on, infecting the entire system. Boot sector infectors are spread through infected bootable floppy disks (or other removal media) and can damage the entire computer system from the moment the computer is switched on.

Macro Viruses
These viruses function by relying on the built-in (internal) programming languages used in popular applications, such as Microsoft Word and Excel, which allow users to create macros. Macros are very simple programs that automate tasks. Virus writers have created macros that, when opened unknowingly, replicate themselves and spread into other documents. These can subsequently be spread via e-mail attachments, floppy disks or other removal media.

File Infectors
These viruses function by modifying specific program files, such as .EXE or .COM files (the file that starts Microsoft Word, for example, is **winword.exe**). When the program runs, the virus executes by loading itself into the memory and later infects and corrupts other files. These viruses are usually spread via infected floppy disks or other removal media, over networks or the Internet.

Preventing Virus Infection

- Install and regularly update anti-virus software. This, in conjunction with good housekeeping, can greatly reduce the threat caused by computer viruses.
- All floppy disks or other removal media, should remain within the confines of the computer room. It is not advisable to let students bring them home or return with them to school. However, if this occurs they should be scanned immediately using anti-virus software. Floppies should also be write-protected.
- Files should be saved to a designated hard drive where incoming files can be scanned automatically by anti-virus software.
- When the sender of an e-mail is not known to the recipient, avoid clicking on attachments containing an executable file.
- Creating back-ups of files won't directly prevent virus infection, but it may speed up the recovery process in the event of a virus erasing or damaging files.

Why Prevent Virus Infection?

School computers contain a wealth of data ranging from student- and teacher-created documents to confidential administration files. Here are just a few reasons why prevention of virus infection is important to schools:

- In order to protect the school's educational and administration software
- In order to avoid huge investments of time and money repairing hardware, reinstalling software and retrieving backed-up documents
- In order to protect students' project work and teachers' class notes

Purchasing Anti-Virus Software

Commercial Programs: Anti-virus software can be purchased on the Internet or from reputable software retailers.

Shareware or Demos: There are a number of Web sites that offer anti-virus software for a nominal charge (shareware). Demo versions of anti-virus programs are also available free of charge.

Ensure that any anti-virus software obtained includes an update facility. It is important that schools are continuously protected against newer viruses as they emerge.

How Does Anti-virus Software Work?

- It scans the computer for viruses and deletes infected files.
- It monitors all incoming files and deletes any viruses contained in these files.
- It places suspect files in quarantine.
- Updates to the software are produced by the program developers in order to address new viruses as they emerge. The software can be set to check for updates at regular intervals.

Relevant Web sites

NCTE Anti-Virus Information
www.ncte.ie/NCTEInitiatives/TechnologyIntegrationInitiative/SchoolsAnti-Virus

Symantec Anti Virus website- Virus threats and definitions

http://www.symantec.com/business/security_response/index.jsp

Symantec anti-virus website which highlights the most active viruses in circulation at present

Note: While the advice sheets aim to act as a guide, the inclusion of any products and company names does not imply approval by the NCTE, nor does the exclusion imply the reverse. The NCTE does not accept responsibility for any opinions, advice or recommendations on external web sites linked to the NCTE site.

This Advice Sheet and other relevant information are available at:
www.ncte.ie/ICTAdviceSupport/AdviceSheets