



PUBLIC SCHOOL DARBHANGA
COMPUTER
CLASS 7

COMPUTER VIRUSES

- a. A computer virus is a program which is designed to perform undesired and malicious actions by replicating and attaching itself to other programs. Viruses are created in order to gain an illegal entry into a computer and obtain or destroy some vital information.
- b. The various ways through which a computer virus enters a computer system are listed below.
 - Viruses can enter the system when the system is booted with an infected pen drive.
 - Some viruses infect the system when a file is copied from an infected disk or a pen drive.
 - Some viruses infect even when there is an attempt to erase the contents of an infected disk or a pen drive.
 - Viruses can also be passed from one computer to another when data or programs are accessed on a network or a file is downloaded from the Internet.
 - If a virus is in the network, it tries to locate the computers that are prone to virus attacks.
- c. After entering a system, a virus tries to take control of the system. It replicates by making copies of itself and also tries to carry out the harmful tasks written in its program.
- d. Some of the preventive measures which should be undertaken to avoid a virus infection are listed below.
 - Avoid booting the computer with a pen drive. If it is required to boot from a pen drive, use a virus free pen drive.
 - Do not exchange the disks or pen drives with others. If it is required to do so, always scan the disk or pen drive with an antivirus software before using it.
 - Do not use pirated software. If the software has been obtained illegally, it may contain a virus.
 - Always keep at least one set of backup copies of all original disks.
 - Always keep the Auto-Protect, Internet-worm Protection and E-mail scanning features of an antivirus software on to prevent downloading of the infected files.
 - Update the antivirus software frequently so that it can detect and delete new viruses.
 - Always check if the computer demonstrates any strange behavior like slowing down or disappearance of files.
- e. Antivirus software is an application program which is designed to detect and remove viruses, worms and Trojan horses from a computer system. The different scanning options provided by Quick Heal Total Security antivirus program are as follows.
 - Full System Scan: This option checks all boot records, drives, folders and files on the computer.
 - Custom Scan: This option checks the specific drives, folders or files on the

- Memory Scan: This option checks the memory of the computer.
 - Boot Time Scan: This option restarts the system for scanning the boot sector.
 - Mobile Scan: This option checks the mobile phone when connected to the computer.
- f. (i) Worms are the programs designed to find their way into the data processing programs and alter or destroy the data. They often use networks such as the Internet to spread from one computer system to another, thus attacking systems that are linked through communication lines.
- (ii) A Trojan horse is a program which performs similar destructive activities. It is not a virus since it does not replicate or spread like a virus. However, it can damage files, place a virus on a computer or break passwords. These programs enter into a computer through an e-mail or through free programs downloaded from the Internet.
- g. The various types of viruses are listed below.
- Boot sector virus: This type of virus hides in the boot sector of a hard disk or a pen drive and infects the start-up instructions required to boot the system. It overwrites the original boot record with the infected one.
 - Program virus: This is the most infectious type of computer virus. It usually resides inside the memory. It infects the executable files such as .COM and .EXE files by attaching its copy to them and hence, is also known as the file virus.
 - Stealth virus: This type of a virus attempts to hide its presence. Some of the simple techniques include hiding the change in date and time and hiding the increase in the file size.
 - Multipartite virus: This type of virus can infect both the boot sector of a disk as well as the executable files. It is the worst virus because it can combine a lot of techniques to prevent its detection.
 - Macro virus: This type of virus infects data files. For example, this virus can attach itself to a word processing or a spreadsheet file as a macro. Once the file is accessed, it replaces one of the Word or the Excel standard macros with an infected version, which can then infect all subsequent documents.