

PUBLIC SCHOOL DARBHANGA



CLASS-8
Computer
Virus Alert

Computer Virus

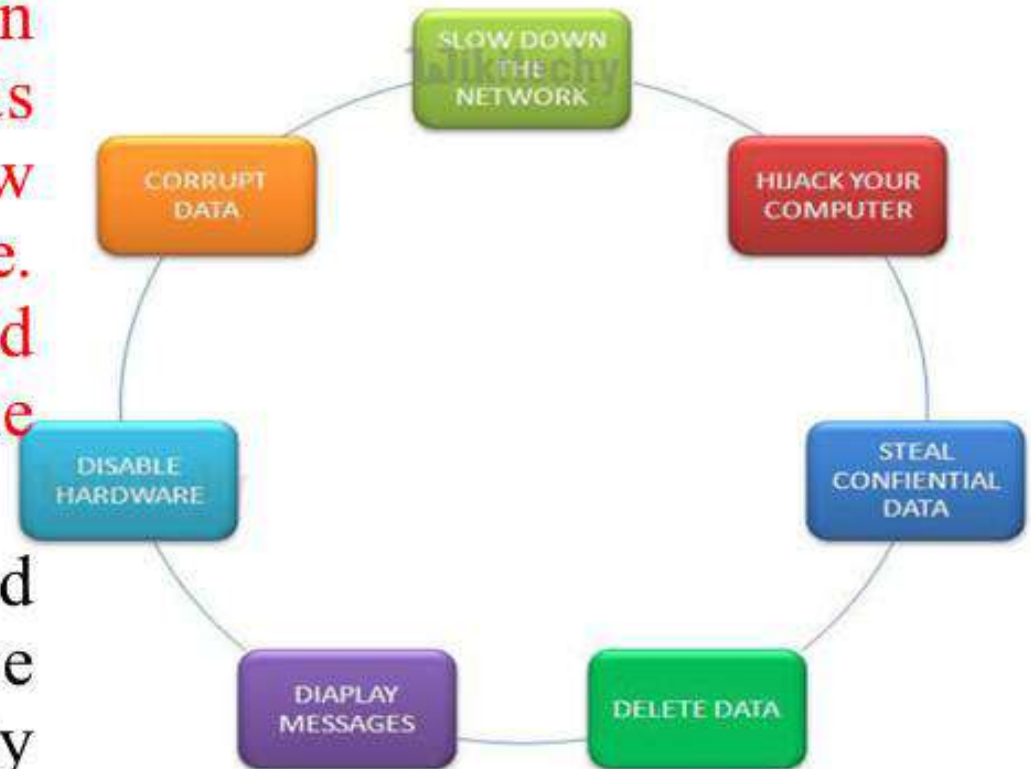
- ▶ A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. **Hackers** design computer viruses with malicious intent and prey on online users by tricking them.



How does a computer virus operate?


A computer virus operates in two ways. The first kind, as soon as it lands on a new computer, begins to replicate. The second type plays dead until the trigger kick starts the malicious code.

In other words, the infected program needs to run to be executed. Therefore, it is highly significant to stay shielded by installing a robust antivirus program.

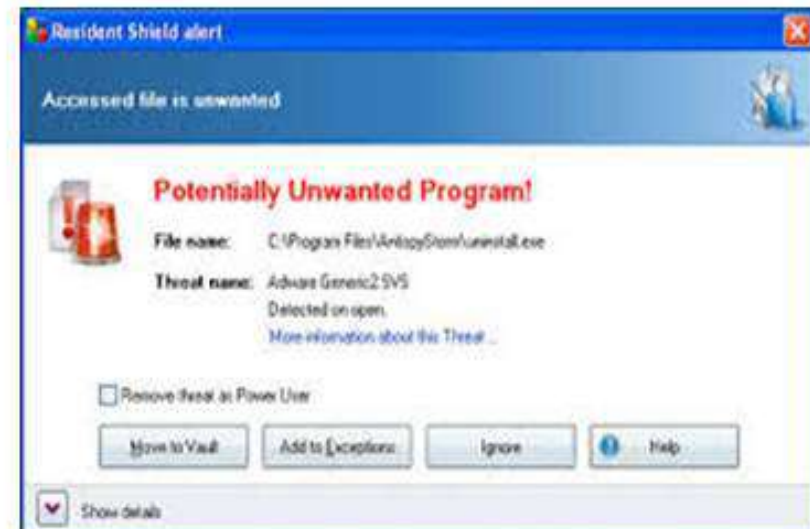


Types of Computer Viruses

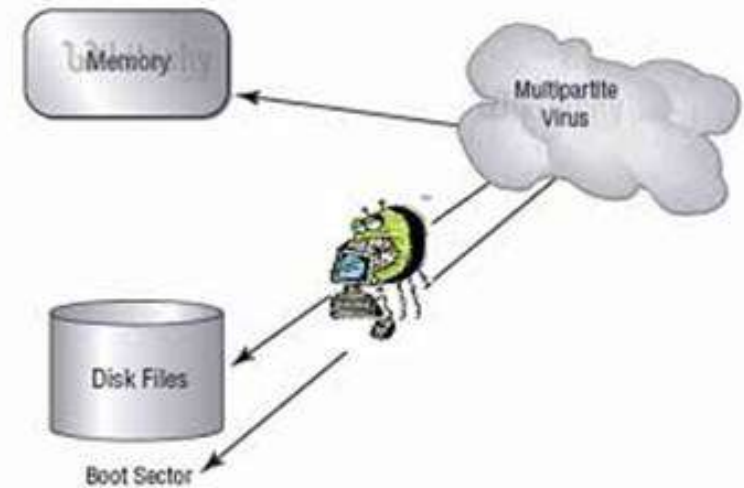
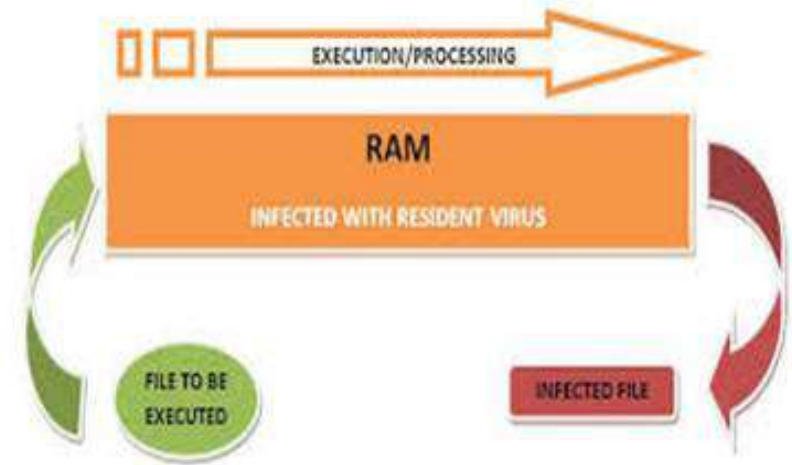
Computer viruses come in different forms to infect the system in different ways. Some of the most common viruses are,

1. Boot Sector Virus
 2. Direct Action Virus
 3. Resident Virus
 4. Multipartite Virus
 5. Polymorphic Virus
 6. Overwrite Virus
 7. Spacefiller Virus
- 

- ▶ **Boot Sector Virus** – This type of virus infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
- ▶ **Direct Action Virus** – This is also called non-resident virus, it gets installed or stays hidden in the computer memory. It stays attached to the specific type of files that it infect. It does not affect the user experience and system's performance.



- ▶ **Resident Virus** – Unlike direct action viruses, resident viruses get installed on the computer. It is difficult to identify the virus and it is even difficult to remove a resident virus.
- ▶ **Multipartite Virus** – This type of virus spreads through multiple ways. It infects both the boot sector and executable files at the same time.



- ▶ **Polymorphic Virus** – These type of viruses are difficult to identify with a traditional anti-virus program. This is because the polymorphic viruses alters its signature pattern whenever it replicates.
- ▶ **Overwrite Virus** – This type of virus deletes all the files that it infects. The only possible mechanism to remove is to delete the infected files and the end-user has to lose all the contents in it. Identifying the overwrite virus is difficult as it spreads through emails.
- ▶ **Spacefiller Virus** – This is also called “Cavity Viruses”. This is called so as they fill up the empty spaces between the code and hence does not cause any damage to the file.



PREVENTION A VIRUS INFECTION

- EVERY PC SHOULD BE EQUIPPED WITH SOME ANTI VIRUS PROGRAM
- ALWAYS SCAN THE PEN DRIVE BEFORE COPYING FILES
- DO NOT INSTALL PIRATED SOFTWARE
- SCAN THE HARD DISK TWICE A MONTH
- TAKE THE BACK UP OF IMPORTANT FILES EVERYDAY
- USE INTERNET AND E-MAIL ATTACHMENTS VERY CAREFULLY