COMPUTER VIRUSES

What is a computer Virus?

A computer virus is a program designed specifically to damage, infect and affect other programs or data or cause irregular behavior of the computer without the permission of the user.

BEHAVIOR OF A COMPUTER VIRUS.

- It replicates itself from one computer system to another.
- It destroys program and data files by interfering with the normal processes of the operating system.
- The spread of the virus is accelerated by the increased use on networks, internet and e-mail.

The risks or threats posed by viruses and the primary impact of a virus can be broadly classified into:

1. **Destructive Viruses**

Type of Destruction	**Symptoms**
Massive Destruction	Attacks the format of disks whereby any program or data damage will be unrecoverable.
Partial Destruction	Erasure and modification of the specific portion of disk affecting any files stored in the location.
Selective Destruction	Erasure and modification of specific files or file groups.
Random Havoc	Randomly changing data on disk or in memory during normal program execution, or changing key stroke values, or data from other input/output devices.
Network Saturation	Systematically using up computer memory or space to impede performance

	or cause the system to crash.

2. **Non-Destructive Viruses**

These viruses do not cause any destruction, but are annoying. They usually display messages, change display messages, change display colors, change key stroke values (e.g. changing the effect of the SHIFT/UNSHIFT keys) and delete characters displayed on a visual display.

Sources of Virus (Spread)

Research has shown that viruses can be introduced into computer systems from a variety of sources. Some of the most common sources are the following:

1. **Contact with contaminated systems**
   Any diskettes used on a contaminated system could become contaminated. If the same diskettes are used on another system, then the virus will spread.

2. **Pirated Software**
   The use of pirated software introduces the risk that the software may be contaminated by the virus code or amended to perform some other destructive function which may affect your system.

3. **Infected Proprietary Software**
   There have been instances of virus programs being introduced and contaminating software under development in laboratories and then being installed onto diskettes containing the finished software product. The number of recorded instances of this is still very low, but the possibility that cellophane wrapped diskettes bought from an approved supplier could be contaminated still exists.

4. **Fake games**
   Many people like playing games on the computers and for the same reason games programs spread very fast. It can take less than two years for a game program to spread to Australia, South America, Africa and Europe.

5. **Freeware and Shareware**
   Freeware is any copyrighted software, application or program that may be freely downloaded, installed, used and shared. Such programs are available for use at no cost to general end users.
   Whereas **Shareware** is software that is distributed free on a trial basis with the
   understanding that the user may need or want to pay for it later.

6. **Updates of software distributed via Networks**
   Software distributed vial networks are fairly obvious targets for virus programmers, as they provide a built in method for widespread and anonymous propagation.

How are viruses activated?

Viruses are activated in three ways. These are:

1. Opening an infected file
2. Running an infected program
3. Starting up the computer with an infected disk.

Types of Viruses include the following:

Boot Sector Virus

Is a virus which executes when a computer starts up because it resides in the boot sector of the floppy disk or the master boot record of the hard disk (MBR).

A File Virus

This attaches itself to program files, and is loaded into memory when the infected program is run.

Macro Virus

A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel or word processors such as Microsoft Word.

Logic Bomb

Is a malicious program timed to cause harm at a certain point in time, but is inactive up until that point.

Time Bomb

A malicious program that is programmed to "detonate" at a specific time and release a virus onto the computer system or network.

Worm

is a malicious, self-replicating program that can spread throughout a network without human assistance.

Trojan horse

Is the program that hides within or looks like a legitimate program, but executes when a certain condition or action is triggered.

Polymorphic Virus

Is a harmful, destructive or intrusive type of malware that can change or "morph," making it difficult to detect with antimalware programs.

VIRUS SYMPTOMS

The presence of a virus can be indicated if one or more of the following symptoms appear on your computer. Any evidence of these or similar events should be an immediate cause for concern to isolate the PC at once and investigated.

1. Unfamiliar graphics or quizzical messages appearing on screens.
2. Programs taking longer than usual to load
3. Disk accesses seeming excessive for simple tasks
4. Unusual error messages occurring more frequently.
5. Less memory available than usual.
6. Access lights turning on for non-referenced devices.
7. Programs or files mysteriously disappearing.
8. Executable files changing size for no obvious reason.
9. Changes to disk volume IDs

DETECTION AND REMOVAL OF VIRUSES.

To prevent infection of your computer system, Antivirus software is used.

An antivirus utility/Software is a program that prevents, detects, and removes viruses from a computer's memory or storage devices.

Software antivirus guards include the following:

i) Norton antivirus software
ii) F-Secure antivirus software
iii) MacAfee antivirus software
iv) Dr.Solomon's kit antivirus software
v) AVG antivirus software
vi) Penicillin antivirus software
vii) Kasperskey antivirus software
viii) Avila antivirus software
ix) Symantec antivirus software

An antivirus utility scans for programs that attempt to modify the boot program, the operating system, and other programs that are normally read from but not modified.

Antivirus programs normally look for virus signatures to identify a virus.
A virus signature or virus definition is a known specific pattern, of virus code.

Users of antivirus utilities must update the virus definition files as often as possible to ensure that such files have patterns of newly discovered viruses.

However a polymorphic virus modifies its program code each time it attaches itself to another program or file, so that even an antivirus utility cannot detect it by its virus signature.
Antivirus utilities may also detect viruses by inoculating existing program files.

To inoculate a program file, the antivirus utility records its file size and file creation date in a separate inoculation file, and uses this information to detect if a virus has altered the inoculated program file.

However a stealth virus infects a program file, but still reports the size and creation date of the original, uninfected program.

If an antivirus utility cannot remove the virus, it often quarantines the infected file in a separate area of a hard disk until the virus can be removed.

Most antivirus utilities can create a recovery disk to remove or repair the infected programs and files. E.g. boot sector virus.

In extreme cases a hard disk may need to be reformatted to remove a virus.

A backup is a duplicate of a file, program, or disk that can be used if the original is lost, damaged or destroyed.

Files can be restored by copying the backed up files for their original location on the computer.

Backup copies should be kept in a fireproof and heatproof safe or offsite.

Precautions that should be taken to guard against computer viruses.

1. Ensure that there is a policy to ensure the usage of computers and their protection and regulations.
2. Ensure that the e-mail is from a trusted source before opening or executing any e-mail attachment.
3. Install an antivirus utility and update its virus definitions frequently for detecting and removing viruses.
4. Never start up a computer with a floppy disk in a floppy drive.

5. Scan all floppy disks and files for possible virus infection before opening them.
6. Set the security level for macros in an application so that the user can choose whether or not to run potentially unsafe macros.
7. Write protect the recovery disk before using it.
8. Back up important files regularly.
9. sharing of diskettes

<u>Steps taken if a virus attack is detected:</u>

1. Identify and isolate PCs and disks which could be affected.
2. Seek the advice of a specialist to perform the following tasks
    a. Identification of virus code on affected disks.
    b. Removal of virus code from all affected disks
    c. Evaluation of the security procedures to ensure that the future virus attacks are minimized.
3. Determine how the virus was introduced to the system
4. Look out for any infected disks that may have left the site.