

COMPUTER VIRUSES

Computer viruses are computer programs that silently replicate/reproduce themselves on a storage media without the computer user realizing it and negatively affect the functionality of your computer. Viruses are therefore malicious software programs (malware) that aim at damaging or interfering with regular performance of other programs in the computer.

A virus is a computer program that can copy itself and infect a computer without permission or knowledge of a user.

Most computer viruses will attach themselves to the RAM or boot sector of disks where crucial data/information for opening programs resides.

EXAMPLES OF COMPUTER VIRUS SCANNING SOFTWARE

These include;

- | | |
|--|---|
| <input type="checkbox"/> Norton Antivirus software | <input type="checkbox"/> Kaspersky Antivirus |
| <input type="checkbox"/> McAfee Virus Scan | <input type="checkbox"/> Avira Antivirus |
| <input type="checkbox"/> AVG Antivirus | <input type="checkbox"/> Bit Defender Antivirus |
| <input type="checkbox"/> Avast Antivirus | <input type="checkbox"/> Smadav Antivirus |
| <input type="checkbox"/> Panda Antivirus | <input type="checkbox"/> Thunder byte antivirus |
| <input type="checkbox"/> Dr. Solomon Antivirus Toolkit | <input type="checkbox"/> F-secure antivirus |
| <input type="checkbox"/> Web scan antivirus | <input type="checkbox"/> USB disk security |

TYPES OF COMPUTER VIRUSES

Viruses can be categorized in different ways, but mainly according to their behavior after execution. They include the following;

1. Resident Viruses; These load into memory on execution and hide in there and target a particular program that can affect other programs or files.

2. Non Resident Viruses; These viruses usually look for files which they infect and then search for other hosts that can be infected.

3. File Infector Viruses; These usually infect system executable files. A file infector virus attaches itself to a program file and is loaded into memory when the infected program is run.

4. Boot sector Viruses; These types of viruses execute when the computer starts up because they reside in the boot sector of a floppy disk or the master boot record of a hard disk. They infect boot sectors of disks where information that opens the disk and programs resides.

5. Multipartite Viruses; These are viruses that use a combination of techniques to infect the different executable files, boot sectors and/or partition sectors.

They are normally difficult to trap. They can therefore destroy the boot record or any other files accessed.

6. Macro Viruses; A macro virus uses the macro language of an application for example word processor or spreadsheet to hide the virus code. Macro viruses are automated tasks programmed by the user. When such tasks with viruses are created in the macro language, they will run whenever such automated tasks are run.

7. Script Viruses; These are programmed in the scripting language (e.g. Visual Basic Script, Java Script) and they may be more dangerous because they work within the operating system environment.

8. Worms; These copy themselves repeatedly in memory or on a disk drive until no memory or disk space remains which makes the computer to stop working. Worms use computer network security flaws to copy and replicate themselves over different computers on the network.

9. Trojan horse; This is a small program code hidden within legitimate software and can be triggered off immediately. It pretends to be doing something but when it is clicked or started, it may destroy computer resources.

10. Polymorphic virus; These modify their program code each time they attach themselves to another program so that even an anti-virus utility has difficulty in detecting them.

11. E-mail Viruses; These are transmitted by email addresses over the network and can append themselves to different addresses in one's mailbox so as to spread through other computer programs.

12. Logic/Time Bomb Viruses; These wait for a condition to occur which would trigger them off e.g. they wait for a particular date.

13. Partition Sector Viruses; These affect the partition sector which is the first sector on the hard disk that contains information about the disk specifications like the number of sectors and tracks in each partition where the operating system starts and so on.

14. Jockers; These are harmless programs that do amusing things on the screen (e.g. *your computer is about to explode in five minutes*).

15. Hoax; These come as e-mails with an attractive subject and launch themselves when the e-mail is opened.

16. Key loggers; Key loggers record the keys you use when using your keyboard and this can be used by hackers to monitor your actions.

17. Spyware; This is a program that can gather information from your computer and send it to someone without your concern. This program will behave like a virus on someone's computer but will not destroy his data but report his actions to another person.

SOURCES OF COMPUTER VIRUSES

- Contaminated storage devices** such as floppy disks, memory sticks, CDs, DVDs and other storage devices.
- Infected programs/software;** If the software to be installed on the computer is already infected with a virus.
- Downloading free programs;** It is not that every freeware and shareware has a virus; nevertheless, since they are of charge, programmers may use this chance to distribute their viruses.
- Updates of software distributed through networks** may also cause computer viruses.
- Sharing of infected storage devices** .This occurs when using a storage media in an infected computer which spreads the virus to the next computer.
- They can also be spread through **e-mail attachments**.
- Through infected web pages.

Qn. Discuss the ways through which viruses can be spread (Give ways of activating a computer virus).

- Through downloading email attachments.
- Through rogue websites; gambling websites and other less trustworthy sites.
- Through using infected boot disks; such as flash memory (flash disks, external hard disks, memory cards and other infected storage devices).
- Phishing schemes; a phishing scheme starts when you receive an e-mail from a website claiming to be your bank credit or credit card company. You are asked to click a link and log in; little did you know that you have given away your personal information.

- ☒ Through using infected software which comes as free games and free software applications.
- ☒ Through installing messaging sites; be careful of plug-ins to enhance service on instant messaging (IM) websites.
- ☒ Through using fake antivirus software; this is one of the most frustrating ways your computer becomes infected with a virus or worm.
- ☒ From mobile devices; a certain family purchased a digital picture frame from a local store and when they attempted to install the software that came with it, they inadvertently infected their computer with a virus.
- ☒ Through running an infected program.
- ☒ Through using removable storage device from an infected computer to another without scanning them.

SYMPTOMS OF COMPUTER VIRUSES

- ☒ Programs taking longer than usual to load.
- ☒ Programs and files disappearing mysteriously.
- ☒ Unusual error messages occurring more frequently.
- ☒ Abnormal functioning of the computer for example you may press the keyboard buttons and they produce nothing or funny characters like & .□ □ □
- ☒ Unfamiliar disk drives or labels and disappearance of some drive letters/labels.
- ☒ Executable files changing size for no obvious reasons.
- ☒ Computers indicating that the storage devices are full when there is still enough space or sometimes even when the storage device is empty.
- ☒ Slowing down of some programs that used to be fast when loading.
- ☒ Less memory available than usual.
- ☒ The computer may not start at all.
- ☒ Failure to respond to print jobs/tasks.
- ☒ Change of files and folder appearance.
- ☒ Computer programs opening without knowledge of the user.
- ☒ Access lights turning on for non-referred devices.

Preventing/Protecting computers from viruses (precautions to guard against computer viruses)

- ☒ Create back up copies of files so that they can be used when original copies get lost.
- ☒ Scan all external devices like diskettes, CDs, flash disks before using them in a computer.
- ☒ Avoid external storage devices as they may be carrying a virus. In other wards, limit the use of removable storage devices (you can install disk security software).
- ☒ Quarantine or isolate media or computers suspected of being infected.
- ☒ Always scan all in-coming e-mails and avoid opening attachments that look suspicious.
- ☒ Use firewalls to prevent hackers from accessing your computer.

NOTE: A firewall is a device or software that can be used to keep a network secure from illegal access.

- ☒ Install anti-spyware to provide protection against spying your computer (install AVG anti-spyware).
- ☒ Only download programs and other files from trusted websites. In other wards, avoid trusting free files.

- Remember to update your anti-virus software and scan the system regularly.
- Be careful when downloading programs from the internet.
- Use write protected disks and limit the exchange of files between computers.
- Do not allow people to load applications or use memory sticks on your computer.
- Be aware of how viruses can get into your computer.
- Never start a PC with a floppy diskette in the drives.
- Make sure that there is a policy to ensure the usage of computers and their protection and regulations.
- Install a trusted and updated antivirus and scan all removable devices before opening them. Antivirus software will also help to alert you when the virus has been discovered to remove or fix it.
- Do not use software that has been copied or pirated.

Qn. Give the disasters that are caused by a computer virus to a computer system.

When a virus infects the computer, it does the following;

- It damages programs.
- It deletes data on storage devices.
- It reformats the hard disk.
- It prepares a storage device by deleting (formatting) all the data that has been saved on it.
- Booting failure.
- It takes up computer memory and this may cause system crashes.
- It degrades efficiencies/performance of the computer.

NOTE: Troubleshooting: This is the process of identifying a problem that is causing a computer not to start normally.

Troubleshooting is a logical systematic search for the source of the problem so that it can be solved and the product or processor can be put into operation again.

Troubleshooting is used to fix problems with hardware, software and many other products.

An antivirus utility/software is a program that prevents, detects and removes virus from a computer memory or storage devices.

Qn. Briefly explain how you can troubleshoot a computer which is not working.

- If your desktop/monitor does nothing at all when you try to start it, first check whether the power cable is securely plugged in at the back of the computer as well as into a working outlet.
- Make sure that the computer components are connected to the computer system as well.
- If the computer is plugged into a surge protector, check whether the surge has a power switch that you can press.
- If you notice some indicator light on the main unit but the monitor stays down, make sure that the monitor is connected to a working power source and securely connect it to the computer via a video cable.
- If the monitor and the computer have power but the computer displays “non-system disk error” message, check to make sure that you did not leave a disk in drive A. If you did, eject it and restart the computer.

- ☐ If the computer system still does not start even when the above peripherals have power and are connected well, try to restart with the windows CD in the CD-ROM drive.
- ☐ If the operating system fails to start, your problem is probably with the start up drives or with the operating system installed on it.
- ☐ And if you cannot fix the drive, then you will have to replace it.

Reasons for creating computer viruses

- 1. Research;** Some viruses are written as research projects by students or academicians to find out the possible strengths, weaknesses, and effect to other programs.
- 2. Competition;** In a bid to show their strength, most virus programmers will always make viruses to out compete other viruses made by other programmers.
- 3. Business/money;** In most cases virus programs aim at destroying programs in other machines so that the creators can be called upon to repair.
- 4. Vandalism/Destruction;** Some viruses are created to strictly destroy other programs. These can be from rival companies targeting especially money making products from their rivals
- 5. Adventure;** Some viruses are made as works of art. They are made just to explore and be innovative and see what comes next.
- 6. Protection;** Some viruses are made as “**good viruses**”. They are made to improve on other products and disinfect the programs. In fact, these are more like anti-viruses.

EXERCISE

- Qn. 1
- a) Distinguish between computer repair and troubleshooting.
 - b) Differentiate between malware and computer virus.
 - c) Describe the stages of a computer virus.
 - d) Explain the different types of computer virus.
 - e) Give precautions of preventing a computer from being attacked by a virus.
 - f) How can you tell that a computer has a virus?
 - g) Give ways through which computer viruses can be spread.
 - h) Outline different virus scanning software that you know.
2. Clearly give the ways of troubleshooting a computer.