

Session 3: Computer Security & Viruses

1. What is a Computer Virus?

Ans- A computer virus is a harmful program which attaches itself with the computer files and infects them. It is capable of making its copies. The ability to copy itself makes virus capable of spreading from one file to other and even to other computers over a network.

2. How many types of computer virus are there? Explain.

Ans- Depending on the way they function; viruses are of following types:

1. **Boot Sector Virus** – Replaces the boot sector program of hard disk; activates at start-up. Prevents OS from loading if corrupted. Examples: Form, Disk killer, Cascade.
2. **File Virus** – Hides in files; activates when file runs; spreads to other files in memory. Examples: Jerusalem, Invader.
3. **Stealth Virus** – Avoids detection by reducing file size or changing structure (polymorphic). Examples: Whale, Frodo.
4. **Macro Virus** – Hides in macros of word/spreadsheet files; activates when file opens. Examples: Melissa, Wazzu.

3. What are computer virus symptoms that we see upon being infected?

Ans- The symptoms that we see if a virus has infected our computer is-

- Computer starts and runs slower than before.
- It hangs or crashes, needing forced restart.
- Pop-ups and notifications appear unexpectedly.
- Hard disk light blinks even when no program is running.
- Available disk space becomes low, and memory usage is high in Task Manager.
- Unwanted or unknown files get created.
- Files don't open properly or crash after opening.
- System restarts by itself suddenly.
- Programs take more time to load and work.
- Strange error messages or dialog boxes appear.

5. What are other Malware Programs and how they affect a computer?

Ans - There are other malware programs also which infect computers and user data in different ways.

- **Worm:**
Copies itself without a host file; spreads through networks and slows data transfer.
Some use email to spread.
Examples: MSBlast, ILOVEYOU.
- **Trojan Horse:**
Looks like useful software but causes harm when run.
Users install it unknowingly.
Examples: Zelu, Rootkit.
- **Spyware/Adware:**
Installs secretly, tracks keystroke, takes screenshots, reads chats, and steals user data.
Can lead to identity theft.

6. How to do protect our computers from Spyware or Adware?

Ans – These are the ways to protect our computers from Spyware or Adware: -

- Install an effective spyware detecting software.
- Keep your operating system and browser updated.
- Check if any unnecessary software is being installed. It is often during the installation steps and in the User Agreement.
- Be careful while installing free programs, games or shareware. Free programs may contain spyware.

7. What is an Antivirus Software?

Ans- An anti-virus software detects the virus threats, scans files for viral infection and removes the viruses. An anti-virus needs to be installed on the computer to prevent, detect and remove viruses. It is necessary to update anti-virus at regular intervals of weeks or months to keep it aware of new threats.

8. How Anti-virus Works?

Ans- An anti-virus detects viruses by their signature or behaviour. A virus signature is the unique structure of a virus program which anti-viruses are aware of. Anti-viruses have a list of known virus signatures with which they can identify the possible virus. That is why anti-viruses need regular updates. Anti-viruses also detect behaviour of the programs on the computer to detect any unusual action such as accessing a file which is not meant for them. In case of any suspicious activity, it scans the program for virus.

9. What is Spam?

Ans- Spam is unsolicited or undesired junk email usually a promotional material. Senders of such emails are called spammers. Spams have a link that lures the user into clicking it. This confirms user's email ID and that brings in more spam in future.

10. What is a Firewall?

Ans- A firewall is a security combination of hardware and software that is used to protect a server and network resources from unauthorized access and intrusion. Firewall checks the incoming data packets over the networks and filters out which do not have suitable and sufficient permission to access the network. This way an extra level of protection is created right at the gates of the network.

11. What is Phishing?

Ans- Phishing is a scam where someone tries to steal your personal info, like passwords or bank details. They send fake emails or make fake websites that look real, pretending to be a trusted company to trick you into giving your information.

12. What is Pharming?

Ans- Pharming is a type of online scam where attackers secretly redirect you from a real website to a fake one, even if you type the correct web address. The fake site looks real and tricks you into entering personal details like passwords or bank info.

13. Define the term operating system. List its 3 major functions.

Ans- An **Operating System (OS)** is system software that acts as an intermediary between computer hardware and the user. It manages hardware resources and provides services for computer programs, allowing users to interact with the computer efficiently and safely.

Three Major Functions of an Operating System:

- i) Resource Management involves allocating and managing hardware resources such as the CPU, memory, and input/output devices.
- ii) File Management is responsible for organizing, storing, retrieving, and protecting data in files on storage devices.
- iii) Process Management controls the execution of programs by managing running processes and handling multitasking.

14. What is the use of disk defragmenter and disk clean up utilities?

Ans- The use of disk defragmenter and disk clean up utilities are -

Disk Defragmenter utility reorganizes fragmented data on a hard disk so that related pieces of files are stored closer together. It helps to improve the speed and efficiency of file access and overall system performance.

Disk Cleanup utility scans the hard drive for unnecessary files such as temporary files, system cache, and items in the recycle bin, and then deletes them. It frees up disk space and helps the computer run more efficiently.

15. Why are regular backups of data important?

Ans- Regular backups of data are important because they help protect against **data loss** caused by events such as hardware failure, accidental deletion, software corruption, cyberattacks, or natural disasters. Backups ensure that important files and system information can be **restored quickly**, minimizing downtime and preventing permanent loss of valuable information.

16. What do you mean by the terms Icons, Desktop and Taskbar?

Ans- The terms icons, desktop and taskbar means:-

- i) Icons are small graphical symbols on the computer screen that represent programs, files, folders, or functions. Clicking an icon usually opens or activates what it represents.
- ii) Desktop is the main screen area that appears after the computer starts. It serves as a workspace where icons, files, and shortcuts can be placed for easy access.
- iii) Taskbar is a horizontal bar (usually at the bottom of the screen) that shows open applications, system notifications, and provides quick access to system tools like the Start menu and clock.

17. What is the use of Computer icon and Recycle Bin.

Ans- The use of Computer icon and Recycle Bin are:-

- i) Computer Icon (also called *This PC* or *My Computer*) allows users to access and manage the computer's storage devices (like hard drives, USBs, and CD/DVD drives), view system properties, and navigate files and folders.
- ii) Recycle Bin temporarily stores deleted files and folders. Users can restore accidentally deleted items or permanently remove them to free up space.