

Computer Viruses: Answers for Class 8

1. Very Short Answer Questions

(i) What is a computer virus?

A computer virus is a malicious program or code that can replicate itself and spread from one computer to another, typically damaging data or system performance.

(ii) Mention a cause of virus infection in a computer.

A common cause is downloading infected files from the internet, especially from unverified sources, or using infected USB drives/external media.

(iii) Write any two examples of computer viruses.

Two examples are Trojan Horse and Worm.

(iv) Write a symptom of a computer infected with a virus.

A symptom is the computer operating much slower than usual.

(v) Suggest a preventive measure of virus infection.

A key preventive measure is to install and regularly update reliable antivirus software.

(vi) List out any three antivirus programs.

Three antivirus programs are Norton Antivirus, McAfee Total Protection, and Avast Antivirus.

2. Short Answer Questions (4 Marks Each)

(i) List out the type of computer viruses.

Computer viruses are classified based on their behavior and where they hide. The main types include:

- **Boot Sector Virus:** Infects the master boot record (MBR) and loads when the computer starts.
- **File Infector Virus:** Attaches itself to executable files (like those ending in .exe or .com).
- **Macro Virus:** Infects files created by applications like Microsoft Word or Excel (documents/spreadsheets).
- **Polymorphic Virus:** Changes its own code whenever it replicates, making it hard for antivirus programs to detect.
- **Stealth Virus:** Tries to hide its presence from the operating system or antivirus programs.

(ii) "Polymorphic virus is dangerous." Justify this statement.

Polymorphic viruses are dangerous because they are very difficult to detect and eliminate.

- **Code Change:** A polymorphic virus **changes its programming code** (or signature) every time it infects a new file or system.
- **Evasion:** This constant change makes it hard for traditional **antivirus software** that relies on matching a known virus signature to identify and block it.
- **Replication:** They can replicate rapidly and effectively, staying hidden and causing widespread damage before being noticed.

(iii) Distinguish between computer virus and anti viruses.

Computer Virus	Antivirus Software
To damage files, slow down the system, or steal data (Malicious).	To detect, prevent, and remove viruses and other malware (Protective).
A malicious program/code that replicates itself.	A utility program designed to safeguard the computer.
Causes harm, data loss, or system instability.	Provides security, system stability, and data protection.

Computer Virus	Antivirus Software
Trojan, Worm, Boot Sector Virus.	Norton, Avast, McAfee.

(iv) How can you say a computer is virus-infected?

You can suspect a computer is virus-infected if you observe several unusual symptoms:

- **Slow Performance:** The computer runs extremely slow or takes a long time to start or open files.
- **Unexpected Pop-ups:** Strange messages, windows, or pop-up ads appear randomly on the screen.
- **Missing/Corrupt Files:** Files disappear or become corrupt, or their content changes without your input.
- **System Crashes:** The computer frequently freezes or restarts unexpectedly.
- **Unusual Activity:** Programs launch by themselves, or the hard drive shows excessive activity when the computer is idle.

(v) What do you mean by boot sector virus?

A boot sector virus is a type of virus that specifically targets the boot sector of a hard disk or any storage device (like a floppy disk or USB drive).

- **Infection Spot:** The boot sector is a specific area on the disk that contains the small program needed to start the operating system boot up the computer.
 - **Activation:** The virus copies itself into this boot sector. When the computer is started, the virus loads into the computer's memory before the operating system, allowing it to control the system from the very beginning.
 - **Impact:** They can prevent the system from booting up correctly or damage the entire file system.
-

■ 3. Long Answer Questions (6 Marks Each)

(i) Explain the computer virus with its types.

A computer virus is a type of malware malicious software that attaches itself to legitimate files or programs and is designed to replicate itself and spread to other computers. Viruses typically cause harm by corrupting files, consuming system resources, or gaining unauthorized access to private information.

Key Types of Computer Viruses:

- **Boot Sector Virus:** This virus infects the Master Boot Record (MBR) of a hard disk or storage device. It becomes active when the computer is powered on and the system attempts to read the MBR, often preventing the machine from starting up.

- **File Infector Virus:** This is the most common type. It attaches itself to executable program files like .exe, .com, or .dll files. When the user runs the infected program, the virus executes and then looks for other files to infect.
- **Macro Virus:** These viruses are written in a programming language like VBA associated with applications like Microsoft Word and Excel. They infect the data files (documents, spreadsheets) themselves. When an infected document is opened, the macro virus runs and spreads.
- **Polymorphic Virus:** This virus is designed to change its signature or code every time it replicates. This makes it extremely difficult for traditional antivirus scanners to detect because the virus's "look" is always different.
- **Stealth Virus:** A stealth virus attempts to hide its presence from the operating system and antivirus software. It achieves this by intercepting system requests and presenting the system with an uninfected version of the file or boot sector.

(ii) What are the effects of computer viruses? Also recommend measures to prevent computers from viruses?

Effects of Computer Viruses

Computer viruses can have a range of negative effects, including:

- **Data Loss and Corruption:** Viruses can delete or corrupt files, making your valuable documents, photos, or school projects unusable.
 - **System Slowdown:** They consume significant CPU power and memory, causing the computer to run very slowly, freeze, or take a long time to start up.
 - **System Instability:** Frequent and unexpected **computer crashes or restarts** are a sign of a severe virus infection.
 - **Hard Disk Damage:** Certain viruses, like the boot sector virus, can damage the integrity of the disk structure, sometimes making it impossible to access data.
 - **Privacy and Security Breach:** Some viruses like Trojans are designed to steal personal information, such as passwords, banking details, and other sensitive data, and transmit it to hackers.
 - **Unwanted Advertisements:** Displaying numerous annoying **pop-up ads** and redirecting your browser to suspicious websites.
2. **Be Careful with Downloads:** Never download files, programs, or games from unknown, untrusted, or suspicious websites.
 3. **Scan External Media:** Always scan any external devices like USB drives, external hard drives with your antivirus software before opening files from them.
 4. **Practice Email Safety:** Do not open attachments in emails from unknown senders. Even if the sender is known, be cautious if the email content seems suspicious or out of character.
 5. **Keep Software Updated:** Regularly update your operating system like Windows and other major software. Updates often include security patches that close vulnerabilities viruses can exploit.
 6. **Use a Firewall:** Activate a Firewall either hardware or software-based to monitor and block unauthorized network traffic, preventing virus entry from the internet.

Measures to Prevent Computer Viruses

Protecting your computer involves a combination of software and safe computing habits:

1. **Use and Update Antivirus Software:** Install a reliable and reputable antivirus program like Norton, McAfee, etc. Ensure the program and its virus definitions are always up-to-date to recognize the latest threats.