10 Computer Virus

LEARNING OUTCOMES

After this lesson, students will be able to:

- Identify and give examples of malware.
- State reasons why people create malware.
- List the different types of malware.
- Define virus and give examples.
- List types of virus.
- Define worms and give examples.
- Define Trojan horse and give examples.
- Define adware.
- Define spam.
- List sources of malware.
- Describe the effects of malware on a computer.
- List the methods of protecting a computer from malware.
- Define and give examples of antivirus software.

WARM UP

Why do you think some people would want to steal data from someone else's computer?

Ans. This can be done by the student after a discussion in the class and with guidance from the teacher.

CHAPTER NOTES

- Malware is a piece of software that causes harm to your system or network.
- Malware has the ability to spread itself in the network, remain undetected, cause changes/damage to the infected system or the network.
- A computer virus is a malicious software program loaded into the computer without the user's knowledge and performs malicious actions.
- A computer virus has the ability to replicate itself.
- A virus can self-replicate, inserting itself onto other programs or files, infecting them in the process.
- Trojan horse is a program that appears harmless, but is malicious.
- Unexpected changes to a computer's settings and unusual activities even when the computer is idle are strong indications that a Trojan is residing on the computer.
- Typically, the malware programming in a Trojan is hidden inside an e-mail attachment or as a free downloadable program.
- A computer worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.
- Spyware is a threat to businesses and individual users, as it can take sensitive information and harm your network.
- Spam is electronic junk mail or any unsolicited or undesired e-mail.
- Some common symptoms that a computer virus attack can produce are: Slow computer performance; unknown programs starting up when you turn on the computer; password changes which could prevent you from logging into your computer; unexpected pop-up windows.
- A boot sector virus can take control when you start or boot your computer.
- A web scripting virus exploits the code of web browsers and web pages.
- A resident virus is a general term for any virus that enters into a

computer system's memory. The virus can execute at any time when an operating system loads.

- A polymorphic virus changes its code each time an infected file is executed. It does this to escape antivirus programs.
- A file infector virus inserts malicious code into executable files, used to perform certain functions or operations on a system.
- Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through e-mail attachments.
- The main causes of a computer virus are infected flash drives or disks, infected files using flash drives and disks, e-mail attachments, infected websites, infected networks and pirated software.
- An illegal copy of software is called pirated software.
- To avoid contact with a virus, it's important to be careful while surfing the net, downloading files, and opening links or attachments.
- To stay safe, never download unexpected text or e-mail attachments, or files from websites you don't trust.
- Avoid clicking on any pop-up advertisements.
- Always scan your e-mail attachments before opening them.
- Use a trusted, latest and updated version of antivirus, such as Norton Antivirus, and keep it updated with the latest virus definitions.
- USB drives should be scanned for viruses, and should not be used on infected computers.
- Spam or unknown e-mails should not be opened and must be deleted without opening.
- Unauthorised or pirated software should not be installed on the computer.
- Always keep a backup of your data on a regular basis. The backup is used in case the virus deletes the data or modifies it. There are some great software that can back up your data automatically.
- Never download songs, videos or files from suspicious websites.
- Never share your personal data with people you don't know over the Internet.

- Antivirus software is a program designed to detect, prevent and remove malware infections on individual computing devices, networks and IT systems.
- Antivirus software can also protect against a wide variety of threats, including other types of malicious software.
- Antivirus software runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware.
- Some of the popular antivirus software are Avast, Norton, McAfee, Adware, etc.

DEMONSTRATION

Demonstrate the use of antivirus software.

LAB ACTIVITIES

Make a PowerPoint presentation on the topic 'Computer Malware'.

ASSESSMENT

Teacher can have an oral quiz in the class on viruses and their types, how they infect and protection against them.