

UNIT 37

HACKERS AND VIRUSES

Objectives: at the end of the lesson, students will be able to:

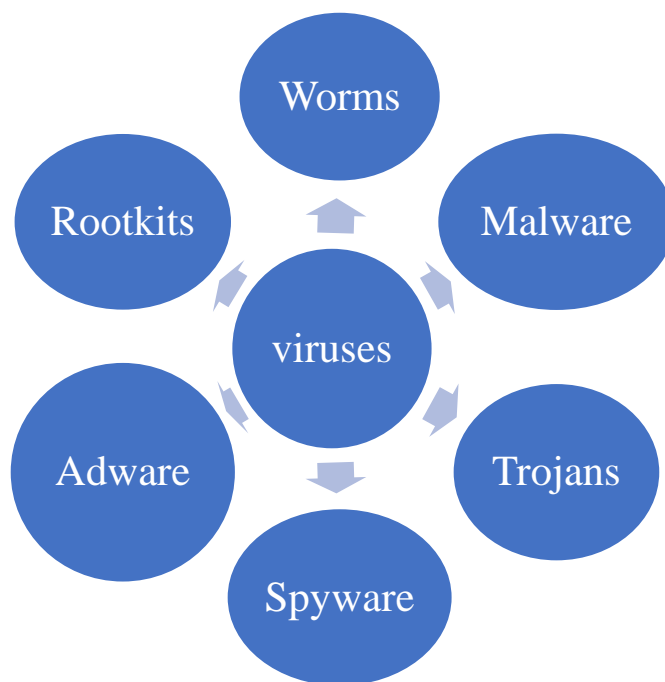
1. memorize key terms related to hackers and viruses, such as "malware," "phishing," and "cyberattack.";
2. understand the impact of hackers and viruses on daily life and the importance of online security;
3. participate in group discussions or role-plays about staying safe online.

Lead-in: Guess the topic

Look at the picture and guess the theme of today's topic.



1. What are some common types of viruses?
2. What are some other kinds of harmful programs?



Vocabulary Building

Key Terms

Hacker – a person who exploits computer hardware and software for their own purposes

Host computer – a computer that provides or receives data or software on a network

Piggyback – to transfer by attaching to another file

Log in – to provide a computer security system with the proper identification to use the computer

Overwriting virus – a computer virus that copies its code over and destroys the files of the original data

Anti-antivirus viruses – is a computer virus that attacks and often disables anti-virus software

Resident virus – a computer virus that becomes part of a file or disk drive but does nothing until activated by a trigger event

Resident extension – an add-on to a computer virus that causes it to become part of the host computer's operating system

Replicate – to make copies

Infect – to infect a computer is to contaminate it with a computer virus

Activity: Choose the correct answers:

1. A “**Resident virus**” can hide in the computer's memory and remain active even after a restart.

- A. True
- B. False

2. “**Replicate**” means to delete a virus from a computer.

- A. True
- B. False

3. A “**Host computer**” is a computer that is used to spread a virus to other computers.

- A. True
- B. False

4. “**Piggyback**” refers to the process of making a copy of a virus.

- A. True
- B. False

5. A “**Hacker**” is someone who helps protect computers from viruses.

- A. True
- B. False

Reading

Viruses 101

The fear that a virus may infect your computer is a familiar one for many. These viruses not only spread malicious code, they also replace the information contained in other programs. They erase important information, sometimes rendering a computer entirely unusable.

Another common virus is a resident virus. They stay dormant until a particular event activates them. If your computer harbors resident viruses, you may not discover them until the damage is done. These and other viruses often install themselves in the resident extensions of other programs.

A Trojan horse is another destructive type of program. It's not technically a virus, because it doesn't replicate, but it's still dangerous. A Trojan Horse looks like an ordinary, useful file or program. However, it has destructive programming embedded in it. This programming may also piggyback onto beneficial files.

Lastly, unlike viruses and Trojan horses, a worm does not need to attach itself to another program. It is particularly troublesome because it attacks computers directly.

Activity: Choose the correct answers.

1. What is the main purpose of the article?

- a. to describe the types of viruses and other harmful programs
- b. to explain how to avoid viruses
- c. to stress the importance of having anti-virus software
- d. to alert readers to the existence of a new virus type

2. Which of the following is NOT a threat to computers?

- a. a resident virus
- b. an overwriting virus
- c. a worm

d. a resident extension

3. How is a Trojan horse different from a virus?

- a. It attaches to another program.
- b. It is harmful to your computer.
- c. It does not replicate itself.
- d. It spreads within a network.

Speaking

Activity: Role - Play

Use languages such as:

I hope ...

Maybe it was ...

At least ...

Student A: You are an IT employee. Talk to Student B about:

- a co-worker's computer problems
- what might have caused the problem

Student B: You are an IT employee. Talk to Student A about how to solve the problem.

- I'm afraid it's probably a virus.
- Yes, but it could be a worm.
- Has anyone else been having problems?
- Maybe it was a Trojan horse.

Continue a role-play with the following scenario:

Scenario 1: Jamila is implementing new security policies at work, including mandatory password changes and multi-factor authentication. Anvar has concerns and questions about these changes.

Scenario: Jamshid receives an email that looks like it's from his company's IT department. The email asks him to click a link and enter his login credentials to update his account information.

Group Work Activity: Case Scenarios

Have students in small groups find real-life examples of famous hackers and viruses, along with brief explanations.

Example: Virus – “ILOVEYOU”

Background: Released in 2000, the ILOVEYOU virus was a computer worm that spread via email with the subject line "I love you." It appeared as a love letter but contained a malicious attachment.

Impact: The virus caused widespread damage by overwriting files and sending copies of itself to everyone in the infected user's address book. It led to an estimated \$10 billion in damages worldwide.

Home assignment

Write a summary of how viruses impact our daily lives. (Words 100-150)