Activity

1) True and false activity: Read each statement carefully. Decide if it is True or False based on the provided reading.

a. Malware is created to improve computer performance and protect sensitive data.
b. Ransomware locks up networks and devices, demanding payment to release them.
c. Spyware operates openly on a computer and notifies users when collecting data.
d. Worms require host programs to spread across a network.
e. Adware can lead to system issues such as redirection to unsafe websites
f. Advanced malware protection uses multiple layers of defense to protect networks.
g. A Trojan virus is capable of self-replicating across multiple devices.
h. Fileless malware is harder to detect because it operates in the computer's memory.
i. Businesses rely solely on perimeter security to protect against malware.
j. Viruses can disrupt a system's functionality and cause significant data loss.

2) Video: *Different Types of Malware Explained | How does Anti-malware Detects them?*
https://www.youtube.com/watch?v=JZOLa7_LShk&ab_channel=MalwareFox

3) Based on the video "Different Types of Malware Explained | How Does Anti-malware Detect Them?", here is a multiple-choice activity to test your understanding:

1. What is the primary characteristic of a Trojan horse malware?
   - **a.** It self-replicates to spread across networks.
   - **b.** It disguises itself as legitimate software to deceive users.
   - **c.** It encrypts user data and demands a ransom.
   - **d.** It displays unwanted advertisements to the user.

2. How does ransomware typically affect a user's data?
   - **a.** It deletes all files permanently.
   - **b.** It encrypts files and demands payment for decryption.

c. It steals personal information without detection.
d. It slows down the computer's performance.

3. Which type of malware is known for recording keystrokes to capture sensitive information?

a. Adware
b. Spyware
c. Worm
d. Rootkit

4. What is a key feature of fileless malware?

a. It operates without leaving traces on the hard drive.
b. It requires user interaction to execute.
c. It displays pop-up advertisements.
d. It modifies system files to remain undetected.

5. How do anti-malware programs typically detect known malware?

a. By scanning for specific code signatures associated with malware.
b. By monitoring user behavior for suspicious activity.
c. By checking the authenticity of installed software licenses.
d. By analyzing the physical condition of hardware components.