Lesson 12: Network Security

In this lesson, students will explore the importance of network security and learn about different forms of attacks on networks, including social engineering and malicious software. They will engage in various activities, such as a bell-ringer activity to discuss the types of data that could be stored on school networks, a quiz to assess their understanding of network security concepts, and a simulation activity using Packet Tracer software to simulate a pharming attack. Additionally, students will play a network security game to identify and protect against various threats. The lesson will conclude with an exit ticket and closure, emphasizing the need for network security in today's digital world and encouraging students to be proactive in protecting their own networks and personal information.

## **Objectives:**

- Students will determine the need for and importance of network security.

- Students will identify different forms of attacks on networks, including social engineering and malicious software.

- Students will explain network security methods to protect against attacks.

## **Materials:**

- Whiteboard or projector

- Computer with internet access and Packet Tracer software installed

- Handouts with network security game instructions

- Pen/pencil and paper for each student

## **Bell-Ringer Activity (5 minutes):**

1. Ask students to think about the data that might be held on them in school.

2. In pairs or small groups, have students discuss and make a list of the types of data that could be stored, such as grades, attendance records, personal information, etc.

3. After a few minutes, ask students to share some examples with the class.

4. Transition to the introduction by asking students why it is important to keep that data safe.

## **Introduction (10 minutes):**

1. Explain to students that today's lesson will focus on network security and the importance of protecting networks from cyber attacks.

2. Discuss with students why it is important to keep data safe, especially personal data stored on school networks.

3. Emphasize that network security is crucial to protect against cyber crime and maintain the privacy and integrity of data.

4. Introduce the two main types of attacks on networks: social engineering and malicious software.

5. Explain that social engineering involves manipulating people to gain unauthorized access to information, while malicious software (malware) is designed to harm or exploit computer systems.

6. Provide examples of social engineering attacks, such as phishing emails or phone scams, and examples of malicious software, such as viruses or ransomware.

## **Direct Instruction (20 minutes):**

1. Use a whiteboard or projector to present information on social engineering and malicious software.

2. Define social engineering as the manipulation of individuals to disclose sensitive information or perform actions that may compromise a network's security.

3. Discuss common social engineering techniques, such as phishing, pretexting, and baiting.

4. Define malicious software (malware) as any software intentionally designed to cause damage or gain unauthorized access to computer systems.

5. Explain different types of malware, including viruses, worms, Trojans, and ransomware.

6. Provide real-life examples and case studies to illustrate the impact of social engineering and malicious software attacks.

## **Guided Practice (25 minutes):**

1. Divide students into pairs or small groups.

2. Instruct each group to use Packet Tracer software to simulate a pharming attack on a network.

3. Provide step-by-step instructions for setting up the simulation and guide students through the process.

4. Encourage students to discuss and analyze the consequences of the attack on the network.

5. Facilitate a class discussion to share observations and insights from the simulation.

## **Independent Practice (25 minutes):**

1. Distribute handouts with instructions for a network security game.

2. Explain the rules of the game, which involve identifying and protecting against various network security threats.

3. Instruct students to play the game individually or in pairs, using their knowledge of network security methods.

4. Monitor students' progress and provide assistance as needed.

5. After the game, ask students to reflect on the threats they encountered and the methods they used to protect the network.

## **Exit Ticket (5 minutes):**

1. Ask students to write a brief response to the following question: "Why is network security important in today's digital world?"

2. Collect the exit tickets to assess students' understanding of the importance of network security.

## **Closure (5 minutes):**

1. Recap the main points of the lesson, emphasizing the need for network security and the different forms of attacks on networks.

2. Ask students to share some examples of network security methods they learned during the game.

3. Remind students to be vigilant and proactive in protecting their own networks and personal information.

4. Encourage students to continue exploring the field of cybersecurity and its importance in today's digital world.

**Common Core Standards:**

- CCSS.ELA-LITERACY.RI.9-10.1: Cite strong and thorough textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text.

- CCSS.ELA-LITERACY.RI.9-10.2: Determine a central idea of a text and analyze its development over the course of the text, including how it emerges and is shaped and refined by specific details; provide an objective summary of the text.

- CCSS.ELA-LITERACY.RI.9-10.3: Analyze how the author unfolds an analysis or series of ideas or events, including the order in which the points are made, how they are introduced and developed, and the connections that are drawn between them.

- CCSS.ELA-LITERACY.RI.9-10.7: Analyze various accounts of a subject told in different mediums (e.g., a person's life story in both print and multimedia), determining which details are emphasized in each account.