Activity 12-2: Ransom Crisis Simulation

Big Idea

This activity is designed to simulate a real-life ransomware attack scenario, enabling participants to understand the severity and complexities involved in such cyber threats. The core concept is to educate participants on how ransomware works, the potential impacts on organizations, and the importance of having effective response plans.

Materials

Computer/Tablet with Internet Access
Materials linked below in the activity section
Optional: Expert guest speaker or cybersecurity professional to provid insights

Vocabulary

Ransomware
Malware
Encryption
Decryption
Cybersecurity

Background

In the background portion of the Ransom Crisis Simulation, designed for students, we'll introduce the basics of ransomware. Imagine ransomware as a type of computer bully that locks away all your files and demands money to give them back. We'll explore how it sneaks into computers, often through tricky emails or weaknesses in the computer's defense. The session will also cover simple yet powerful cybersecurity steps, like using strong passwords, keeping programs up-to-date, and understanding the role of protective software like firewalls and antivirus programs. Another key point will be the importance of regularly saving copies of your files elsewhere (backups), so you're not at a loss if something goes wrong. This knowledge is crucial for students to grasp the real-world scenario in the simulation, helping them think about how to respond effectively if their virtual system gets hit by ransomware.

Activity Directions

1. **Introduction to the Simulation:**
    a. Brief students on the scenario: their school's computer network has been hit by a ransomware attack.
    b. Divide students into teams, each representing a different department (IT, administration, communications, etc.).
2. **Initial Response Phase:**
    a. Teams receive an initial briefing about the attack's impact (e.g., locked files, ransom notes).
    b. Each team discusses and decides on their immediate response actions (e.g., isolating infected computers, informing authorities).
3. **Malware Identification Activity:**
    a. Teams analyze clues and data (provided in their briefing packs) to identify the type of ransomware.
    b. They research the specific ransomware to understand its characteristics and potential weaknesses.
4. **Decision-Making Exercise:**
    a. Teams must decide whether to pay the ransom, seek external help, or attempt to recover the files using backups.
    b. Each decision comes with its own set of consequences and further developments in the scenario.
5. **Recovery Plan Development:**
    a. Teams develop a recovery plan to restore services and secure the network, regardless of their previous decision.
    b. They must consider aspects like system restoration, data recovery, and future prevention measures (RPD Template).
6. **Reflection and Discussion:**
    a. Teams present their response strategies and recovery plans.
    b. Facilitators lead a discussion on the real-life implications of ransomware attacks and the importance of cybersecurity.
7. **Guest Speaker Session:**
    a. If possible, invite a cybersecurity expert to talk about real-world experiences with ransomware and answer student questions.
8. **Wrap-Up Quiz or Assessment:**
    a. Conclude with a quiz or assessment to reinforce key learnings from the simulation.