1. Introduction to the Escape Room Challenge

Before diving into individual station resources, it's essential to provide an overview of how the Escape Room works. Below are the general instructions:

Escape Room Overview:

- Title: Cybersecurity Escape Room Challenge
- Objective: Collaborate with your team to solve a series of cybersecurity puzzles and challenges across multiple stations.
- Time Limit: 45 minutes to complete all stations.
- Rules:
    - Teams must rotate through four stations.
    - Each station has its own set of cybersecurity challenges.
    - You will earn points based on the time taken and accuracy of the solutions.
- Stations:
    - Station 1: Identifying Malware
    - Station 2: Securing a Network
    - Station 3: Detecting Phishing
    - Station 4: Social Engineering Role Play

Teacher Dialogue: "Today, you'll be working in teams to complete a Cybersecurity Escape Room challenge! You'll rotate through different stations, solving puzzles that will test all the cybersecurity knowledge you've gained throughout this course. Remember, teamwork and communication are key!"

Resource 1: Station 1 – Identifying Malware

- Instructions: Each group will receive a set of malware clues based on suspicious files, and they must determine the type of malware.
- Materials:
    1. Printed sample malware descriptions (below).
    2. Answer sheet for identifying malware types.

Malware Files (Clues):

1. File: Financial_Records.exe
    - Clue: This is an executable file disguised as a financial record. It is commonly used to distribute trojans.
2. File: Photos.zip
    - Clue: The zip file contains a batch script that auto-executes spyware when extracted.
3. File: Project_Summary.pdf.locked
    - Clue: The file has been encrypted, likely by ransomware.
4. File: Holiday_Photos.png.scr
    - Clue: Appears to be a photo but uses a .scr extension, suggesting it's a disguised screensaver that may carry malware.

Answer Key:

- Financial_Records.exe: Trojan
- Photos.zip: Spyware
- Project_Summary.pdf.locked: Ransomware
- Holiday_Photos.png.scr: Worm

Teacher Dialogue: "Your task here is to identify the type of malware based on the clues given. Think back to our previous lessons—what tells you if it's ransomware, spyware, or a trojan? Discuss with your team!"

Resource 2: Station 2 – Securing a Network

- Instructions: Students are tasked with configuring a network's security settings. They must choose between different firewall options, user permissions, and antivirus statuses.
- Materials:
    1. Printed network setup sheets (below).
    2. Answer key for correct network configuration.

Network Setup Sheet:

1. Firewall Settings:
    - Option 1: Allow all traffic to pass.
    - Option 2: Block all incoming traffic except trusted IP addresses. (Correct)
    - Option 3: Disable the firewall to test network speed.
2. User Permissions:
    - Option 1: Allow all users to access critical files.
    - Option 2: Restrict admin rights to network engineers. (Correct)
    - Option 3: Allow everyone access to modify system files.
3. Antivirus Status:
    - Option 1: Disable antivirus during updates.
    - Option 2: Keep antivirus active at all times. (Correct)
    - Option 3: Remove antivirus to improve system performance.

Answer Key:

- Firewall: Block incoming traffic except trusted IP addresses.
- User Permissions: Restrict admin rights.
- Antivirus: Keep antivirus active.

Teacher Dialogue: "In this station, you need to secure the network. Make sure you’re setting up the firewall, antivirus, and user permissions correctly. Talk it out—what is the safest configuration for each setting?"

Resource 3: Station 3 – Detecting Phishing

- Instructions: Students will examine sample phishing emails and determine the red flags that indicate it's a phishing attempt.
- Materials:
    1. Printed phishing email templates (below).
    2. Red flag checklist to help identify phishing.

Phishing Email Templates:

1. Email 1:
    - Subject: Your account has been locked.
    - Body: "Click here to reset your password immediately. [Suspicious link]."
    - Clue: Urgency and suspicious link.
2. Email 2:
    - Subject: Important message from your bank.
    - Body: "Please download the attached document for details on your account."
    - Clue: Unfamiliar sender and suspicious attachment.
3. Email 3:
    - Subject: You've won a prize!
    - Body: "Claim your $1,000 prize by clicking here."
    - Clue: Too good to be true, unsolicited message.

Answer Key:

- Email 1: Urgency, phishing link.
- Email 2: Suspicious attachment.
- Email 3: Unsolicited message, too good to be true.

Teacher Dialogue: "These emails are designed to trick you into giving away sensitive information. Look carefully for red flags like urgency, suspicious links, and attachments. How can you tell these are phishing attempts?"

Resource 4: Station 4 – Social Engineering Role Play

- Instructions: Students will act out social engineering scenarios to practise their responses. One student plays the attacker, another the victim, and others observe and provide feedback.
- Materials:
    1. Scenario cards for role play.
    2. Feedback forms for observers.

Scenario 1: Vishing (Voice Phishing)

- Attacker: Pretend to be a bank official asking for login details.
- Victim: A student who must decide whether or not to give personal information.
- Clue: The attacker uses urgency and authority to pressure the victim.

Scenario 2: Smishing (SMS Phishing)

- Attacker: Send a fake SMS stating the victim has won a prize.
- Victim: The student must determine whether the message is legitimate.
- Clue: The message is unsolicited and promises a large reward.

Scenario 3: Pretexting

- Attacker: Pretend to be a colleague needing the victim's login details for an urgent project.
- Victim: The student must determine whether the request is valid.
- Clue: The attacker creates a false sense of urgency to gain access.

Feedback Form:

- What worked well?
- What could be improved?
- How effective was the response?

Teacher Dialogue: "Social engineers rely on psychological manipulation to trick their victims. Let's see how well you can respond in these scenarios—what should you say if someone asks for sensitive information? Observers, make sure you're noting what works and what doesn't!"

Resource 5: Reflection Sheet

Objective: After completing all stations, students will reflect on what they learned and how they can apply it in real-life cybersecurity situations.

Reflection Questions:

1. What was the most challenging station, and why?
2. What strategies helped you solve the cybersecurity problems?
3. How can you apply these strategies to protect yourself in real life?
4. What did you learn about teamwork and collaboration during the Escape Room?

Teacher Dialogue: "Let’s take a few minutes to reflect on what you’ve learned. Think about what challenges were hardest for you, what strategies helped, and how you can apply these lessons to protect yourself from cybersecurity threats."

Other Resources:

1. Team Instruction Sheets: Outlining the rules and time limits for each station.
2. Timers for each station, ensuring that teams rotate on time.