Activity Title: Role Play – Responding to a Digital Threat

Objective:

To help participants recognize a phishing attempt, understand why it's dangerous, and demonstrate the appropriate response.

Duration:

15-20 minutes

Materials Needed:

- **Printed copies** or a **digital display** of the phishing email scenario for each group.
- **Notepads and pens** (optional) for taking notes during the discussion.

Instructions:

1. **Group Formation**:
    - Split participants into **pairs**.
2. **Scenario**:
    - You receive an email that looks like it's from your bank. The email asks you to verify your account details by clicking on a link.
      Example email text:
    - **Subject**: **"Important: Verify Your Account Information"**
    - **Message**:
      "Dear Customer,
      We have noticed unusual activity on your bank account. To protect your account, we need you to verify your details.
      Please click on the link below and log in to your account.
      [FakeBank.com Login Link]
      Thank you for banking with us.

Best regards,
Customer Support Team"

---

3. **Role Assignment**:
    - **Participant 1**: Plays the role of the user who received the phishing email.
    - **Participant 2**: Plays the role of the cybersecurity expert advising the user on how to handle the situation.

---

4. **Task**:
    - **Participant 1** should explain how they would initially react to the email, considering whether they suspect it's a phishing attempt or not.
    - **Participant 2** will provide expert advice on:
        - Why the email is likely a phishing attempt.
        - The specific **red flags** (e.g., unusual language, urgent requests, suspicious link).
        - The correct steps to take (e.g., not clicking the link, contacting the bank directly).

Steps to Follow in the Role Play:

1. **Identify the Digital Threat**:
    - Discuss why the email is dangerous:
        - Suspicious link (e.g., hovering over the link to check the actual URL).
        - Urgent language meant to induce panic.
        - Lack of personal details (no mention of the user's actual name).
2. **Response Strategy**:
    - Participant 2 should guide Participant 1 on the following:
        - **Do not click on any links** or download attachments.

        - **Report the email** as phishing to the email provider.
        - **Contact the bank directly** using official communication channels to verify whether the request is legitimate.
        - **Delete the email** after reporting it.

Debrief:

- After completing the role play, each pair should briefly present:
    - The **red flags** they identified in the phishing email.
    - The **steps** they took to handle the situation and protect their digital identity.
- Facilitate a **group discussion** on:
    - **What makes phishing emails effective?**
    - **What are some other examples of phishing attempts** participants have encountered?

Facilitator Role:

- Ensure participants understand the purpose of the exercise.
- Encourage the cybersecurity "expert" to clearly explain how to recognize phishing attempts and guide the user.
- Wrap up by reinforcing best practices for **digital safety** and **how to respond to phishing threats**.

🎯 **Activity Objective:**
The goal of this activity is to help participants make more informed decisions to protect their digital data.