Resource 1: Social Engineering Role Play Scenarios and Scripts

Scenario 1: Vishing Attack (Voice Phishing)

Overview: In this scenario, the attacker pretends to be a bank representative trying to steal personal information over the phone.

Attacker Script:
(Attacker calls the victim)
Attacker: "Good afternoon, this is John from [Bank Name]. I'm calling to alert you about a suspicious transaction on your account. There was a charge of £500 made this morning. Was this you?"
(Pause for victim's response)
Attacker: "We need to verify your identity to block the transaction. Can you please confirm your full name and account number?"

Victim Response (Guidance):

- Do not provide personal information.
- Ask for verification of the caller's identity.
- Suggest calling the bank back using an official number found on your bank card.

Observer's Role:

- Evaluate if the victim asked for proof of the caller's authenticity.
- Did the victim avoid giving away personal information?
- How assertive was the victim in managing the conversation?

Scenario 2: Smishing Attack (SMS Phishing)

Overview: The attacker sends a fake text message pretending to be from a delivery service to trick the victim into clicking a malicious link.

Attacker Script (Text Message):

Attacker: “Your parcel delivery has been delayed. Click here to reschedule: [malicious link]”

Victim Response (Guidance):

- Do not click the link.
- Research the sender's phone number.
- Call the delivery company directly using the official number found on their website.

Observer’s Role:

- Evaluate whether the victim identified the message as suspicious.
- Did they check the authenticity of the message?
- How effectively did they handle the situation?

Scenario 3: Pretexting Attack

Overview: In this scenario, the attacker pretends to be from the victim’s company IT department, attempting to gain access to sensitive information.

Attacker Script:

(Attacker sends an email or calls the victim)

Attacker: "Hi, this is Sarah from the IT department. We’re updating our system, and I need your username and password to verify your access. Could you provide those details?"

(Pause for victim's response)

Attacker: "This is a routine procedure, nothing to worry about. Without this update, you won’t have access to your email tomorrow."

Victim Response (Guidance):

- Refuse to provide login information over the phone or email.
- Ask for verification or follow up with the actual IT department through an official channel.

Observer’s Role:

- Did the victim refuse to provide login details?
- Did they question the authenticity of the request?
- Were they assertive and cautious throughout the conversation?

Resource 2: Feedback Form for Observers

Observer Feedback Form

(To be completed after each role play scenario)

- Scenario: ____
- Attacker Tactic: ____________________________________
- Did the victim identify red flags?:
  - Yes / No
  - If yes, what were the red flags?

    ____
- How effective was the victim's response?
  - Very Effective / Somewhat Effective / Ineffective
  - Provide feedback:

    ____

    ______
- Suggestions for improvement:

Resource 3: Group Reflection Questions

After each role play, each group should discuss and reflect on the scenario they acted out using the following questions:

1. What were the key warning signs in this social engineering attack?
2. How did the victim respond to the attack?

3. What could have been done differently to handle the situation more effectively?
4. What real-world implications does this type of attack have?
5. What steps can be taken to educate others on how to avoid falling victim to this kind of attack?

Resource 4: Role Play Evaluation Rubric

Criteria	Excellent (5)	Good (4)	Satisfactory (3)	Needs Improvement (1-2)
Identification of Red Flags	Identified all red flags	Identified most red flags	Identified some red flags	Did not identify any red flags
Response to Attack	Assertive and appropriate	Mostly appropriate	Somewhat appropriate	Ineffective response
Awareness of Social Engineering Tactic	Clearly understood the tactic	Understood most aspects	Some understanding	Limited understanding
Reflection and Analysis	Provided detailed analysis	Provided some analysis	Limited analysis	No analysis provided