Cybersecurity Scenarios for Students

1. Social Engineering at CyberCafe

Scenario: Jennifer visits a popular CyberCafe in town. While sipping her coffee, she receives a call from someone claiming to be a tech support person from her company, asking her to confirm her login credentials as there's been a suspected breach.

Question: Should Jennifer provide her credentials? What steps should she take next?

2. The Mysterious Email Attachment

Scenario: Mark, an executive at a top firm, receives an email from a sender claiming to be from the HR department. The email contains an attachment titled "Annual Bonus Details". He wasn't expecting any such email.

Question: What should Mark do? If he wants to verify the authenticity of the email, what steps can he follow?

3. Unexpected WiFi Network

Scenario: Lucy is at an airport and searches for WiFi networks. She finds one named "Free Airport WiFi" but doesn't see any signs advertising free WiFi.

Question: Should Lucy connect to this network? Why or why not? What risks might she face if she connects?

4. A Generous USB Stick

Scenario: Kevin finds a USB stick in the parking lot of his office labeled "Company Salary Details". Curious, he considers plugging it into his office computer.

Question: Is it safe for Kevin to insert the USB stick? What are the potential threats, and what actions should he take regarding the found USB?

5. Shadow IT Concerns

Scenario: Sophia, from the marketing department, uses a cloud storage solution not approved by her company's IT department because she finds it more user-friendly. She starts storing company data on it.

Question: What are the potential risks of Sophia's actions? What policies can companies implement to prevent such behavior?

Instructor Answer Key

1. Social Engineering at CyberCafe

Answer: Jennifer should NOT provide her credentials. She should immediately report the call to her company's IT or security department. This is a potential social engineering attack.

2. The Mysterious Email Attachment

Answer: Mark should avoid opening the attachment. He should check the sender's email address for any discrepancies, avoid downloading any files, and immediately contact the HR department using known contact methods to verify the email's authenticity.

3. Unexpected WiFi Network

Answer: Lucy should avoid connecting to unverified or open networks, especially in public places. Risks include man-in-the-middle attacks, unencrypted traffic interception, and malware distribution.

4. A Generous USB Stick

Answer: Kevin should not insert the USB stick into his or any computer. It could be a baiting attack loaded with malware. He should hand it over to the IT department or, if not identifiable, destroy it to prevent potential misuse.

5. Shadow IT Concerns

Answer: Sophia's actions can expose company data to unauthorized access, potential data breaches, and data loss. Companies can prevent such behavior by implementing strict IT usage policies, educating employees on risks, and providing secure, user-friendly alternatives for necessary functions.