

Topic 1.1: Understanding Social Engineering

LO: 1.1.A, 1.1.B, 1.1.C | Skill: 1.A | Scenario: 1A: Detecting Phishing Messages

Exit Ticket — Topic 1.1

5 minutes. Read the scenario, then answer all three items.

Scenario. A high-school junior, Devon, gets a text message from an unknown number: "This is Mom's coworker Linda. Mom's car broke down and she lost her phone. She needs you to send her bank login code that just came to your phone so she can pay for a tow. Hurry, she's stuck on the highway." Devon's phone just showed an SMS with a 6-digit code from his mom's bank.

1. Which psychological tactic is the text message PRIMARILY using?

- (A) Elicitation through casual conversation.
- (B) Urgency — the code is needed immediately. **(correct)**
- (C) Authority by impersonating a bank employee.
- (D) Scarcity by saying the offer is limited.

2. If Devon sends the 6-digit code, which impact category is most likely?

- (A) Malware installs on his device.
- (B) His personal info is used as challenge questions on another website.
- (C) The adversary takes over his mom's bank account using the OTP. **(correct)**
- (D) Devon's mom is charged for the tow but cannot recover the money.

3. In 1-2 sentences, what specifically should Devon do BEFORE responding to the text? Name the action.

Model: Call his mom directly on her real phone number (or a known family member) before responding — if the text is real she'll answer; if she doesn't, it is almost certainly social engineering and Devon should share the OTP with no one.