

Topic 1.1: Understanding Social Engineering

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

Scenario — Westbrook Gear Co. — The Saturday Afternoon Email

Original case for AP Cybersecurity Topic 1.1. Not based on any real company.

Background

Westbrook Gear Co. is a small, three-store outdoor sporting-goods chain in the Pacific Northwest. The North Lake location keeps a small staff: a store manager named Mrs. Park and two part-time weekend stockers. One of them is Joelle, a high-school junior who has worked at Westbrook for nine months.

The situation

It is a quiet Saturday afternoon. Joelle is reorganizing the climbing-gear wall when Mrs. Park calls her over to the back-office computer. Mrs. Park looks worried. "Joelle, you're better with computer stuff than I am. Can you look at this for me?" She turns the screen toward Joelle. There is an email open in her inbox.

The email

Email on Mrs. Park's screen

From: tom.fielding@trailco-supplies.tech
To: mpark@westbrookgear.com
Subject: URGENT - Lost shipment - wire \$4,800 today or lose your supply slot

Hi Marcia,

Tom here from TrailCo. Bad news — the truck carrying your Saturday harness and rope shipment was hit on I-5 this morning. Everything's a loss.

We can rush you a replacement shipment on Monday morning, BUT our system requires payment confirmation before we can release product to a re-ship.

I need you to wire \$4,800 to the account below TODAY. If we don't see it by 5 PM Pacific I will have to release your supply slot to the next account in queue and your store will have to wait three weeks for the next available shipment cycle.

Wire instructions: Bank of Cascade Crest, Acct #88712-3401, Routing 113-009-441

Don't reply to this email — the rep mailbox is full. Call me direct at 555-0119 if you need to (but please just wire so we can keep moving).

-- Tom

What happens next?

Mrs. Park is reaching for her phone to call the bank. "I don't want to miss our shipment slot," she says. "But four thousand eight hundred dollars is a lot. Joelle, what would you do?"

Application Questions

1. Identify at least **four red flags** in this email that suggest it is a social engineering attempt rather than a real message from a TrailCo Supplies representative. For each red flag, write one short sentence explaining why it is suspicious.

2. Explain which two psychological tactics from this topic are at work in this email. Quote specific words or sentences from the email as evidence.

3. Describe what could happen to Westbrook Gear if Mrs. Park wires the \$4,800. Identify which category of impact this falls into.

4. Determine what Joelle should suggest Mrs. Park do next. Give a specific, concrete action — not a general principle.