

SCENARIO — WESTBROOK GEAR (TEACHER KEY)

Topic 1.1: Understanding Social Engineering

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

Teacher Key intro

Use the model responses below to guide the Day 2 case-debrief discussion. Don't simply read them aloud — prompt students to defend their own answers first, then validate or extend with the model. Look especially for students who can articulate WHY a red flag matters, not just identify it.

Scenario — Westbrook Gear Co. — The Saturday Afternoon Email (Teacher Key)

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 — Model Answers

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.

Model Response: Sample red flags (any 4 earn full credit):

(a) Lookalike sender domain — "trailco-supplies.tech" is not the real TrailCo domain. The unusual ".tech" TLD and the hyphenated name are spoofing red flags.

(b) Mismatched first-name greeting — the email opens with "Hi Marcia" but is sent to mpark@. Mrs. Park's first name is not Marcia; a real rep would know.

(c) Wire transfer request — legitimate B2B suppliers invoice through established billing systems, not surprise wire transfers to unfamiliar account numbers.

(d) Urgency + threat combination — "TODAY" + "by 5 PM" + "release your supply slot" is classic urgency-plus-intimidation. Genuine logistics problems rarely require same-day wire transfers.

(e) "Don't reply to this email" — legitimate vendors WANT a reply trail. Telling the recipient not to reply prevents verification.

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.

Model Response: Urgency — repeated time-pressure language: "TODAY", "by 5 PM Pacific", "three weeks for the next available shipment cycle." This is designed to make Mrs. Park act before she can verify.

Intimidation — threat of a negative consequence: "release your supply slot to the next account in queue" + "your store will have to wait three weeks." The fear of losing inventory pushes Mrs. Park to comply rather than question.

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

Model Response: Westbrook Gear loses \$4,800 to an adversary, with little chance of recovery once a wire transfer clears. The adversary may also follow up with additional "urgent" requests in the coming weeks, since the first attempt worked. This is primarily a **financial-loss** impact from social engineering, with a potential **credential-capture** follow-on if Mrs. Park clicks any later links in the same email thread.

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

Model Response: Joelle should suggest Mrs. Park do NOT wire the money and instead verify the request through a separate channel before doing anything else. Specifically: call TrailCo Supplies on the phone number listed on a recent legitimate invoice (NOT the number in the suspicious email) and ask whether Tom actually sent this request. If TrailCo confirms no such email was sent, Mrs. Park should report the email to her IT support and delete it without clicking any links or replying.