

# Topic 1.1: Understanding Social Engineering

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

## Mini-FRQ — Westbrook Gear Phishing Review

Two weeks after the wire-transfer email incident, Westbrook Gear's IT volunteer Sam Ortega is investigating another suspicious email reported by Mrs. Park. Use the two sources below to answer Parts A and B.

Total points: 5. Use evidence from the sources. Allowed task verbs: **Describe** · **Determine** · **Explain** · **Identify** · **Write**.

### Evidence Sources

#### Source 1 — Reported phishing email

**From:** billing-security@westbrook-gear-billing.help  
**To:** mpark@westbrookgear.com  
**Subject:** Final notice: your store will be disconnected within 2 hours

Dear Westbrook Gear,

Our payment-processor records show your North Lake store has an outstanding balance of \$312.49. To avoid having your point-of-sale system disconnected within the next 2 hours, please click the link below and update your billing card. Disconnection will block all sales until reactivation, which can take 5-7 business days.

Update billing: <http://westbrook-gear-billing.help/update?store=northlake>

Failure to act may also affect your business's standing with our processor.

Sincerely,  
Billing Security Team

#### Source 2 — Westbrook Gear Email & Communication Policy (excerpt)

##### Required

- Staff must update their email password every 90 days.

##### Permitted

- Staff may click links in emails from senders whose domain matches westbrookgear.com or one of our listed suppliers.
- Staff may share login credentials with the store manager when troubleshooting.

## Prohibited

- Staff may not install software on store computers without IT volunteer approval.

## Questions

**Part A.** Consider the email in Source 1.

**i. Identify** two specific elements of the email that indicate it is a social engineering attempt. (1 point)

**Model Response:** (a) The sender domain "westbrook-gear-billing.help" is a lookalike spoof — it is not the real westbrookgear.com domain. (b) The 2-hour deadline + threat of POS disconnection combine urgency and intimidation in classic phishing fashion.

**ii. Describe** how the email uses BOTH the urgency and intimidation tactics to influence Mrs. Park's behavior. Cite specific words from the email as evidence. (2 points)

**Model Response:** Urgency: "within the next 2 hours" + the 5-7 business-day reactivation delay both create time pressure to act before verifying. Intimidation: "point-of-sale system disconnected" + "affect your business's standing with our processor" both threaten negative consequences. The combination is designed to short-circuit critical thinking so Mrs. Park clicks the billing-update link before checking whether the sender is legitimate.

**Part B.** Consider the policy in Source 2.

**i. Explain** one weakness in the policy that makes Westbrook Gear MORE vulnerable to social engineering. Include a specific example of how an adversary could exploit it. (1 point)

**Model Response:** Allowing staff to share login credentials with the store manager when troubleshooting is the major weakness. An adversary impersonating the store manager (or claiming to be "IT support") could elicit a staff member's password under the cover of a fake troubleshooting request, and the staff member would believe they are following the policy.

**ii. Determine** one specific change to the policy that would reduce risk from social engineering attacks like the one in Source 1. (1 point)

**Model Response:** Add a Prohibited rule that staff may not share login credentials with anyone — including the store manager — under any circumstance. Pair with a Required rule that any link in an email claiming an urgent action (billing, password, account suspension) must be verified by phone with a known contact before clicking.