

Topic 1.1: Understanding Social Engineering

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

Application Worksheet — Topic 1.1

Complete all three parts. Use complete sentences in Parts 2 and 3.

Part 1 — Vocabulary match (5 points)

Match each term to its definition. Write the letter of the definition next to the term.

Term	Your answer	Definition
Phishing	D	Social engineering attack delivered by email.
Intimidation	B	Threat-based tactic that pressures the target with a negative consequence.
Urgency	E	Time-pressure tactic that prevents the target from taking time to think.
Elicitation	A	Casual conversation designed to draw out sensitive information.
Credential capture	C	Stealing a username and password by tricking a user into entering them on a fake page.

Part 2 — Red-flag identification (5 points)

Read the email below carefully. List **three** specific red flags that suggest this email is a social engineering attempt. For each one, write a short sentence explaining why it is a red flag.

Email Stimulus

From: alerts@my-bank-secure-portal.example.com
To: joelle.r@westbrookgear.com
Subject: ACTION REQUIRED: Account verification within 6 hours

Dear Customer,

Our automated system has flagged unusual login activity on your account. To prevent permanent suspension, please verify your account within 6 hours by clicking the secure link below and entering your full login details.

Verify now: <http://my-bank-secure-portal.example.com/verify?id=joelle>

Failure to act within 6 hours will result in immediate account closure and may affect your credit standing.

Sincerely,
My Bank Security Team

Model answers (any 3 of the following earn full credit):

- **Lookalike domain** — "my-bank-secure-portal.example.com" is not a real bank domain; legitimate banks use their official domain only.
- **Generic greeting** — "Dear Customer" instead of the recipient's real name suggests a bulk-sent attack.
- **Urgency + intimidation combo** — "within 6 hours" plus "permanent suspension" + "affect your credit standing" pressures the reader to act before thinking.
- **Unexpected link** — the URL goes to a non-bank domain; hovering would reveal a mismatched host.
- **Request for full login details** — legitimate institutions never ask for password verification via email.

Part 3 — Impact application (4 points)

Imagine the recipient of the email above did click the link and enter their username and password. In 2-3 complete sentences, describe two distinct categories of impact that could follow. Use vocabulary from this topic.

Model answer: First, this is a **credential capture** attack — the adversary now has the user's username and password and can log in as them. Second, the captured credentials can lead to **account takeover**: the adversary changes the password and locks the legitimate user out. If the user reused the same password elsewhere, the adversary can also take over those other accounts.