

Topic 1.1: Understanding Social Engineering

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

Collaboration Activity — Phishing Triage Team

Suggested skill: **Skill 4 — Collaborate** (subskills 4.A team objectives, 4.B roles, 4.D complete assigned work).

Goal

In teams of 3-4, act as the security team at a small business. Your team's job: triage a reported phishing email and produce a 1-sentence guidance note for the rest of the staff. (15 minutes total.)

Roles (choose before starting)

Role	Responsibility
Analyst	Identifies at least 3 specific red flags in the email and writes them down.
Writer	Drafts the 1-sentence staff guidance note based on the analyst's findings.
Verifier	Checks the analyst's red flags against the topic vocabulary; pushes back if any are weak.
Spokesperson	Presents the team's findings to the class in 30 seconds at the end.

Your email to triage

Email reported by an employee

From: it-helpdesk@centraltech.support
To: all-staff@centraltech.com
Subject: Mandatory password update — complete by end of day

Hello team,

Our records show your password expires today. To avoid losing access to company systems, please update your password by 5 PM by clicking the secure link below and entering your CURRENT password, then your new password.

Update now: <http://centraltech-portal.password-reset.example.test/update>

Note: this is a mandatory IT compliance task. Failure to update will result in your account being locked out of email, file shares, and the VPN.

Thank you,
IT Help Desk

Deliverables (submit one per team)

- List of at least 3 specific red flags + a one-line reason each.
- Which psychological tactics are at work (intimidation, urgency, or both)?
- One-sentence staff guidance note ("If you receive this email, do X.").
- 30-second spokesperson presentation to the class.

Reflection (individual, written, 2 min)

One thing your team caught that you might have missed working alone:

One thing you contributed to the team: