

Topic 1.1: Understanding Social Engineering

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

Standards & Skills Map — Topic 1.1

CED-aligned reference: the LOs, EKs, and skill subskill this topic targets. For teacher use during planning, observation, and feedback.

Learning Objectives

- **LO 1.1.A** Identify common indicators of social engineering tactics.
- **LO 1.1.B** Explain how social engineering tactics influence victims to perform a desired action.
- **LO 1.1.C** Describe possible impacts for victims of social engineering attacks.

Essential Knowledge (8 EKs)

- **1.1.A.1** Social engineering uses psychological tactics to elicit info, trick into downloads, or trick into clicking malicious links. Often via email, text, or social media.
- **1.1.A.2** Two primary tactics: *intimidation* (threat-based) and *urgency* (time-pressure).
- **1.1.B.1** Tactics rely on common psychological principles that influence human behavior.
- **1.1.B.2** Intimidation exploits human aversion to negative consequences; fear drives action.
- **1.1.B.3** Urgency exploits the human reaction to time-sensitive needs; pressure prevents critical thinking.
- **1.1.C.1** Disclosed personal info (name, phone, address, workplace, pet names, birthdate) supports impersonation — often these double as identity-verification challenge questions.
- **1.1.C.2** Disclosed secure info like a one-time password (OTP) or auth code allows an adversary to log in as the victim.
- **1.1.C.3** Clicking a link or downloading a file may install malware, steal browser data, or redirect to a credential-capture page.

Suggested Skill

Skill 1.A — Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.

Unit Scenario cross-reference

Topic 1.1 connects to CED Unit Scenario **1A: Detecting Phishing Messages**. Our original Westbrook Gear case parallels the scenario theme without reproducing CB-authored content (per Trademark_Compliance.md).

Industry alignment

CompTIA Security+ (SY0-701) obj. 5.6: Explain types of social engineering attacks and motivations. Topics 1.1 + 1.4 together cover the AP-side material that students preparing for Security+ will see again in obj. 5.6.

NICE Workforce Framework: aligns with Cyber Defense Analyst work role (PR-CDA-001) competencies around recognizing common attack vectors.