

Topic 1.1: Understanding Social Engineering

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

Guided Notes — Topic 1.1

Fill in the blanks during the slide presentation. Use exact terms from the slides.

Section 1 — What is social engineering?

Social engineering is an attack that uses **psychological** tactics — not technical exploits — to manipulate a target into revealing sensitive information, downloading a malicious **file**, or clicking a malicious **link**.

It is most often delivered by **email**, by **text** message, or through **social media** messages.

Section 2 — Two psychological tactics

Intimidation: the adversary **threatens** the target with a negative consequence if they do not comply. Example: "Your account will be suspended."

This tactic works because it exploits the natural human **aversion** to negative consequences — in other words, it uses **fear** to incite action.

Urgency: the adversary creates a reason the target must act **quickly**. Example: "You have 24 hours to verify."

This tactic works because feeling time pressure prevents the target from taking the time to consider whether the action is **reasonable** or **safe**.

Section 3 — Three impacts of a successful attack

1. Impersonation. Personal information disclosed — like name, phone, address, pets' names, or **birthdate** — often matches **challenge questions** used by websites to verify identity, so the adversary can reset accounts and impersonate the victim.

2. Account takeover. A disclosed **one-time password** (OTP) or login code allows the adversary to log in as the victim with full account access.

3. Malware or credential capture. Clicking a malicious link can install **malware** on the device, steal browser-stored credentials, or redirect to a fake **login** page that captures the password.

Quick check

The first thing to do when you suspect social engineering is to **not click anything**. The second thing is to verify the message via a separate **channel**.