

# 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 \_\_\_\_\_ tactics — not technical exploits — to manipulate a target into revealing sensitive information, downloading a malicious \_\_\_\_\_, or clicking a malicious \_\_\_\_\_.

It is most often delivered by \_\_\_\_\_, by \_\_\_\_\_ message, or through \_\_\_\_\_ messages.

### Section 2 — Two psychological tactics

\_\_\_\_\_ : the adversary \_\_\_\_\_ 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 \_\_\_\_\_ to negative consequences — in other words, it uses \_\_\_\_\_ to incite action.

\_\_\_\_\_ : the adversary creates a reason the target must act \_\_\_\_\_. 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 \_\_\_\_\_ or \_\_\_\_\_.

### Section 3 — Three impacts of a successful attack

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

**2. Account takeover.** A disclosed \_\_\_\_\_ (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 \_\_\_\_\_ on the device, steal browser-stored credentials, or redirect to a fake \_\_\_\_\_ page that captures the password.

## Quick check

The first thing to do when you suspect social engineering is to \_\_\_\_\_. The second thing is to verify the message via a separate \_\_\_\_\_.