

Topic 1.1: Understanding Social Engineering

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

MCQ Practice Set — Topic 1.1

5 set-based questions in AP style. Questions 3 and 4 share the email stimulus. Pace yourself: target ~12 minutes total.

1. A small business owner receives the following email:

"Hi — this is Anna from the IRS. We've flagged unusual activity on your business's tax filing from last year. Please call this number within 24 hours or we will issue a warrant for your arrest. — Anna"

Which psychological tactic is PRIMARILY at work in this email?

- (A) Elicitation through casual conversation.
- (B) Intimidation through threat of a negative consequence. **(correct)**
- (C) Reciprocity through offering a favor.
- (D) Social proof through claims about other people's actions.

Why: The email threatens arrest (a negative consequence) to compel action — the textbook definition of intimidation per EK 1.1.A.2.

Tagged: Skill 1.A | LO/EK 1.1.A.2

2. Which of the following scenarios BEST illustrates social engineering?

- (A) An adversary brute-forces a login form by trying thousands of common passwords.
- (B) An adversary scans an open port on a public web server and finds an outdated service to exploit.
- (C) An adversary calls a help desk impersonating a locked-out executive to get a password reset. **(correct)**
- (D) An adversary intercepts unencrypted Wi-Fi traffic at a coffee shop to read login credentials in transit.

Why: Social engineering manipulates a PERSON (the help-desk agent) through psychological tactics (impersonating authority). The other options are technical exploits, not social engineering.

Tagged: Skill 1.A | LO/EK 1.1.A.1

Email reported as suspicious by a student

From: support@app1e-id-recovery.example.com
To: students@school.edu
Subject: Final notice: your Apple ID will be deleted today

Dear Student,

We have detected unusual activity on your Apple ID. To prevent permanent deletion of your account and loss of all photos, contacts, and purchases, you must verify your account within 4 hours.

Click here to verify: <http://app1e-id-recovery.example.com/verify>

97% of users have already verified. Don't be the last one to act.

Apple ID Support

3. Use the email above to answer.

Which TWO red flags in this email are the strongest evidence that it is a social engineering attempt?

- (A) The email mentions photos and contacts, which are real Apple ID services.
- (B) The email is signed "Apple ID Support" and uses HTML formatting.
- (C) The greeting says "Dear Student" instead of using the recipient's full legal name.
- (D) A lookalike sender domain (numeric 1 for l) plus a non-Apple verification link. **(correct)**

Why: The lookalike domain (numeric 1 substitute) and the mismatched verification URL are the strongest spoofing indicators. Generic greeting (D) is also a red flag but weaker on its own than the domain spoof. (A) and (B) are not red flags.

Tagged: Skill 1.A | LO/EK 1.1.A.1

4. Use the same email above. If a student clicks the verification link and enters their full Apple ID and password, what is the MOST LIKELY immediate impact?

- (A) The adversary captures the student's credentials and takes over the Apple ID account. **(correct)**
- (B) The student's photos are immediately deleted from iCloud.
- (C) The student's personal information is used to answer challenge questions on a different website.
- (D) Malware is installed on the student's phone.

Why: The link captures credentials via a fake login page (EK 1.1.C.3) leading directly to account takeover (EK 1.1.C.2). Malware (A) is possible but not the most likely IMMEDIATE impact of credential entry on a fake form. (C) is a downstream impact requiring more info. (D) is fiction; the adversary controls the account but doesn't auto-delete data.

Tagged: Skill 1.A | LO/EK 1.1.C.2

5. A new employee at a hospital receives a text from an unknown number that reads:

"Hi! This is Carl from the IT department. I'm setting up your accounts and I just need to confirm

your username and the temporary password from your welcome email. Thanks!"

Which response BEST reduces the risk that this is social engineering?

- (A) Forward the text to a coworker and ask them to handle it.
- (B) Verify Carl's identity through a separate channel first. **(correct)**
- (C) Reply with the username only, and ask Carl to call back for the password.
- (D) Reply with both pieces of information since the request came from "IT".

Why: Verification through a separate trusted channel (out-of-band verification) is the universal defensive response to a suspected social engineering attempt. (A) still discloses partial info. (B) trusts an unverified sender. (D) just shifts the risk.

Tagged: Skill 1.A | LO/EK 1.1.A.1