

# Exercise walk-through

## Understanding Social Engineering ■ 1.1

eXercise

## You must be able to

- name social-engineering tactics: **intimidation** 恐吓, **urgency** 紧迫感, authority, consensus
- explain how a tactic pressures a victim to act
- describe the impact when a victim reveals information or downloads **malware** 恶意软件

## Method — Spotting the tactic

Read the message and ask what feeling it creates. A threat of a bad result = **intimidation**. A tight deadline = **urgency**. A claim that everyone else already acted = **consensus**. Borrowed power from a boss = **authority**.

## Method — Explaining the impact

State what the victim gives up and what the adversary can then do. Example: giving a one-time password lets the adversary log in as the victim; giving personal details lets them answer challenge questions and impersonate the victim.

## Practice 2.1 ■ 2 marks

Define **social engineering** in one sentence.

## Solution 2.1

### Worked steps

manipulating people (not code) into breaking security **B1** by revealing information, clicking a link, or running malware **B1**.

## Practice 2.2 ■ 4 marks

Name two psychological tactics used in social engineering and describe each briefly.

## Solution 2.2

### Worked steps

any two of: intimidation = threatens a bad result **B1** **B1** +; urgency = invents a deadline **B1** **B1** +; authority = borrows a boss's power; consensus = claims everyone else acted.



## Practice 2.3 ■ 1 mark

An email says: “Confirm your details in the next hour or your account is deleted.”

- (a) Identify the main tactic used.
- (b) Explain how it pressures the reader.

## Solution 2.3

### Worked steps

(a) urgency **B1**. (b) the 1-hour deadline makes the reader act quickly **B1** without stopping to check whether the request is safe **B1**.

## Exam-style 3.1 ■ 1 mark

An adversary threatens to report an employee to the police unless they send a file.  
Which tactic is this?

**A** Consensus

**B** Intimidation

**C** Familiarity

**D** Scarcity

## Solution 3.1

A Consensus

B Intimidation



C Familiarity

D Scarcity

### Worked steps

B. a threat of a negative consequence is **intimidation**.

## Exam-style 3.2 ■ 1 mark

A victim gives an adversary their one-time password (OTP). The most likely impact is that the adversary can

- A** encrypt the network
- B** log in to a service as the victim
- C** jam the Wi-Fi
- D** clone an access card

## Solution 3.2

Method: Explaining the impact

- A encrypt the network
- B log in to a service as the victim
- C jam the Wi-Fi
- D clone an access card



### Worked steps

B. an OTP lets the adversary authenticate as the victim.

## Exam-style 3.3 ■ 1 mark

A message reads: “Over 90% of your team has already verified their account.”

- (a) Name the tactic being used.
- (b) Explain why this tactic is persuasive.

## Solution 3.3

Method: Spotting the tactic

### Worked steps

(a) consensus **B1**. (b) people tend to follow the crowd **B1**, so believing others acted pressures the victim to act too **B1**.