

1.1 Understanding Social Engineering

Name: _____ Class: _____ Date: _____

Total: 14 marks

Objective

Build the skills to answer exam questions on **social engineering** 社会工程学 and its psychological tactics.

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

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ 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**.

■ 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.

2 Practice

2.1 Define **social engineering** in one sentence.

[2]

2.2 Name two psychological tactics used in social engineering and describe each briefly.[4]

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

(a) Identify the main tactic used. [1]

(b) Explain how it pressures the reader. [2]

3 Exam-style questions

3.1 An adversary threatens to report an employee to the police unless they send a file. Which tactic is this? [1]

- **A** Consensus
 - **B** Intimidation
 - **C** Familiarity
 - **D** Scarcity
-

3.2 A victim gives an adversary their one-time password (OTP). The most likely impact is that the adversary can [1]

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

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

(a) Name the tactic being used. [1]

(b) Explain why this tactic is persuasive. [2]

4 Go further

- work through the **1.1 Understanding Social Engineering** lesson on the **Learn** page;
- read the **Introduction to Security** section of the AP Cybersecurity handout on the **Know** page.

Solutions

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

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

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

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

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

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