AP COMPUTER SCIENCE PRINCIPLES • EXERCISE SHEET

5.6 Safe Computing

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

Objective

Build the skills to answer exam questions on **safe computing**.

You must be able to:

- explain how **personally identifiable information (PII)** 个人身份信息 can be misused
- describe threats such as **phishing** 钓鱼, malware, and social engineering
- explain how **encryption** 加密 protects data
- distinguish **symmetric** 对称 from **asymmetric** 非对称 encryption

1 Worked examples

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

■ PII and threats

Personally identifiable information (PII) —such as a name, address, or ID number —can be misused if exposed. Common threats include **phishing** (fake messages that trick you), **malware**, and **social engineering**.

■ Encryption

Encryption encodes data so that only authorized users can read it.

- **Symmetric** encryption uses **one shared key** for both encoding and decoding.
- **Asymmetric** encryption uses a **public + private key pair**.

Safe practices include strong **authentication** and cautious sharing.

2 Practice

2.1 State what PII is. [1]

2.2 Name two common security threats. [2]

2.3 State what encryption does. [1]

3 Exam-style questions

3.1 PII stands for personally identifiable [1]

- **A** internet
- **B** information
- **C** interface
- **D** index

3.2 Encryption protects data by [1]

- **A** deleting it
- **B** encoding it so only authorized users can read it
- **C** compressing it
- **D** sorting it

3.3 A fake email tricks a user into revealing a password.

(a) Name this type of threat. [1]

(b) Name one safe practice that reduces the harm. [1]

(c) State the difference between symmetric and asymmetric encryption. [1]

4 Go further

- work through the **5.6 Safe Computing** lesson on the **Learn** page;
- read the **Impact of Computing** section of the AP Computer Science Principles handout on the **Know** page.

Solutions

2.1 personally identifiable information —data that can identify a person, which can be misused if exposed.

2.2 any two of: phishing, malware, social engineering.

2.3 it encodes data so that only authorized users can read it.

3.1 B.

3.2 B.

3.3 (a) phishing. (b) strong authentication, or being cautious about sharing information (any one). (c) symmetric uses one shared key; asymmetric uses a public and private key pair.