A-LEVEL COMPUTER SCIENCE • EXERCISE SHEET

6.1 Data Security

Name: _____ Class: _____ Date: _____ **Total: 36 marks**

KEY WORDS security 安全 • integrity 完整性 • phishing 网络钓鱼 • data security 数据安全 • privacy 隐私

Objective

Build the skills to answer exam questions on **data security** 数据安全 — the difference between security, privacy and integrity; the threats from networks; and the measures that protect a system.

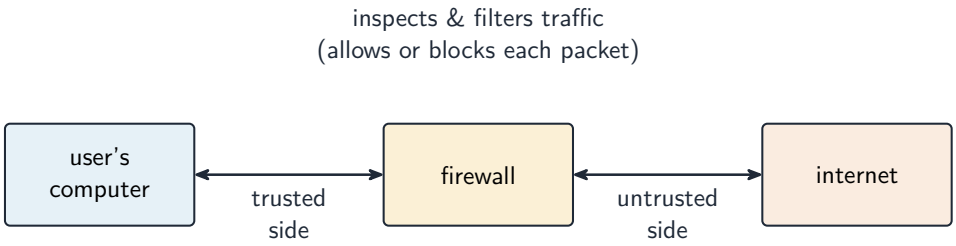
You must be able to:

- explain the difference between **security**, **privacy** 隐私 and **integrity** 完整性
- describe the **threats** to data and systems posed by networks and the internet
- describe **security measures** for a standalone PC and for a networked system

1 Worked examples

Study these first. Each one shows the method for a question type used later — follow the steps and you can do the Practice and Exam-style questions yourself.

■ Three different ideas



A firewall is a core data-security control at the network edge

Term	Means	Example failure
security	protect data from **unauthorised** access/change	a hacker reads the file
privacy	a person controls **who sees** their personal data	data shared without consent
integrity	data stays **accurate and complete**	a typo corrupts a record

All three are needed — a file can be secure but still have a typo (no integrity), or

accurate but readable by anyone (no privacy).

■ **Threats from the internet**

Threat	What it does
virus / worm	self-copying malware (a worm spreads over the network alone)
Trojan horse	looks useful but hides malicious code
ransomware	encrypts your files and demands payment
spyware	secretly records keystrokes / passwords
phishing	fake emails/sites trick users into giving credentials
pharming 域名欺骗	redirects a user to a fake site **even when they type the correct address**
denial of service	floods a server so real users can't connect
brute-force attack	tries many passwords until one works

■ **Security measures**

- **standalone PC:** strong password; up-to-date antivirus; software updates; **backup**; **encryption**; locked screen.
- **networked system:** all of the above **plus** a **firewall** 防火墙, per-user **permissions**, central account management and **audit logs**.

2 Practice

Now apply the methods above.

2.1 State the difference between data **security** and data **privacy**. [2]

2.2 Name the type of malware that **encrypts a user's files and demands payment**. [1]

2.3 State **two** security measures suitable for a standalone PC. [2]

2.4 State what a **firewall** does. [1]

3 Exam-style questions

3.1 Explain the difference between **security**, **privacy** and **integrity**, giving an example of each. [3]

3.2 Describe **two** threats posed by connecting a computer to the internet, and give a measure that reduces each. [4]

3.3 (a) State what **phishing** is. [1]

(b) State one way a user can reduce the risk of falling for a phishing attack. [1]

3.4 Explain how a **firewall** and **user permissions** together help protect a networked system. [3]

3.5 State **one** difference between **phishing** and **pharming**. [2]

3.6 A bank sends confidential statements to its customers over the internet.

(a) **Describe** how the bank uses **asymmetric encryption** so that only the intended customer can read a statement. [3]

(b) The statement also carries a **digital signature**. **Describe** how the signature is created by the bank and checked by the customer, and **state** what it proves. [5]

(c) A **checksum** is sent with the file as well. **Explain** what a checksum detects that a digital signature does not need to, and **state** why a checksum alone would not be enough for security. [3]

(d) A customer's computer is infected by **malware** that records keystrokes. **Name** this type of malware and **describe** two measures that would reduce the risk. [3]

(e) The bank also protects its own network with a **firewall**. **Describe** two things a firewall does. [2]

Solutions

2.1 Security = protecting data from unauthorised access/change; privacy = the individual's right to control **who sees** their personal data.

2.2 Ransomware.

2.3 Any two of: strong password; up-to-date antivirus; software updates; backups; encryption; locked screen.

2.4 It monitors and controls traffic between a trusted network and an untrusted one (the internet), blocking unauthorised connections.

3.1 Security = protection from unauthorised access (e.g. a hacker); privacy = controlling who sees personal data (e.g. consent); integrity = data being accurate/complete (e.g. not corrupted by a typo).

3.2 Any two threats, each with a measure, e.g.: malware → antivirus + updates; phishing → user training / don't click unknown links. *(Other valid pairs accepted.)*

3.3 (a) Fake emails or websites that trick the user into giving away credentials/personal data.
(b) e.g. check the sender / don't click links in unexpected emails / type the address yourself.

3.4 The firewall blocks unauthorised connections from outside; user permissions limit what each account can access inside, so even a logged-in user (or attacker) can only reach what they are allowed to.

3.5 Phishing tricks the user into clicking a fake link / giving details themselves; pharming **redirects** the user to a fake site automatically even when they type the correct web address.

3.6 (a) The customer has a key pair and publishes the **public** key. The bank encrypts the statement with that public key. Only the customer's **private** key can decrypt it, and the customer never shares it, so nobody else can read the statement.
(b) The bank puts the statement through a **hashing algorithm** to produce a digest, then encrypts that digest with the **bank's private key** — that is the signature. The customer decrypts the signature with the **bank's public key** to recover the digest and hashes the received statement themselves. If the two digests match, the statement came from the bank and has not been altered.
(c) A checksum detects **accidental corruption** in transmission — dropped or flipped bits. It is not enough for security because an attacker who alters the file can simply recompute the checksum; a signature cannot be forged that way, because the attacker does not have the bank's private key.
(d) A **keylogger**, a form of spyware. Any two: keep antivirus software installed and up to date; do not open attachments or install software from unknown sources; use two-factor authentication so a stolen password alone is useless; use an on-screen keyboard or a password manager for sensitive entry.
(e) Any two: it **inspects** incoming and outgoing traffic against a set of rules and blocks whatever fails them; it maintains a blacklist or whitelist of addresses and ports; it can block traffic to unauthorised applications and log attempted intrusions.