A-LEVEL COMPUTER SCIENCE • EXERCISE SHEET

6.1 Data Security

Name: _____ Class: _____ Date: _____ **Total: 22 marks**

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.

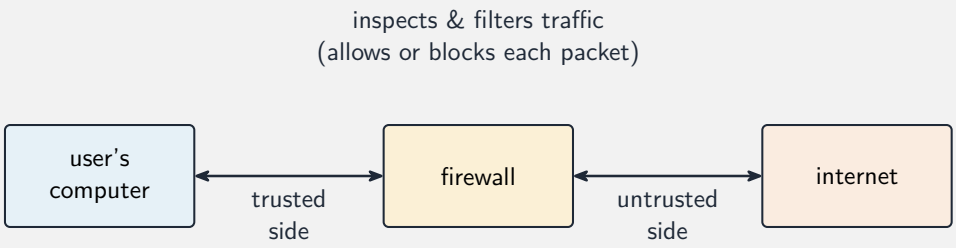
You must be able to:

- 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]

4 Go further

You are now ready for the real exam questions on this subtopic. Open the **6.1 Data Security** past-paper sheet in the Library, or try these in **Practice mode**:

- 9618/11 J24 —Q5 (security threats and protection methods)
- 9618/12 N25 —Q5 (malware and protecting a network)
- 9618/11 J25 —Q7 (keeping data secure)
- 9618/12 N24 —Q4 (security threats)

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.