Solutions

Each answer shows the steps, then the **result**.

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

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

- it 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
- the customer 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