Solutions

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

2.1

- the attacker tries password after password
- a **brute-force attack** tries many passwords very quickly until one works

2.2

- ransomware **locks your files and demands payment** to unlock them

2.3

- before encryption: **plaintext**
- after encryption: **ciphertext**

2.4

- any **two** of: filters traffic / caches web pages / hides the user's IP / acts as a firewall

2.5

- encryption only **scrambles** the data
- an interceptor can still take a copy, but without the key the ciphertext is **meaningless**

3.1 B

- a firewall **checks data in/out and blocks what is not allowed**
- A is anti-malware; C is encryption; D is a proxy

3.2

(a)

- **fake emails or messages**
- they trick you into **giving away private details**

(b)

- any **two** of: authentication / anti-malware / access levels / automatic updates / proxy server

3.3

- a **virus** attaches to a file and copies itself when the file is opened
- a **worm** copies itself across a network on its own

3.4

(a)

- readable **plaintext** is scrambled with a key into **ciphertext**
- it cannot be understood without the matching key to decrypt it

(b)

- **SSL** or **TLS**
- the address begins with `https`, or a **padlock** is shown

(c)

- any **two** of: examines traffic in and out / compares with criteria and blocks failures / keeps a log / blocks named sites or IP addresses

(d)

- each user is given only the permissions **their job needs**
- a clerk who logs in **cannot open customer files** reserved for managers

(e)

- after the password is accepted, a **one-time code** is sent to a device the user holds
- the user must enter that code to complete the log-in
- a thief with only the password **cannot get in without the device**

(f)

- the bank publishes a **public key** that anyone may use to encrypt
- **no secret key** has to be sent over the internet, unlike symmetric encryption