

Solutions

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

2.1

- a web browser is used by a person to do a task
- it is **application software**

2.2

- any **two** of: managing files / memory / interrupts / user interface / peripherals / multitasking / security

2.3

- email asking for a password: **phishing**
- server flooded with requests: **DDoS**

2.4

- a **virus** attaches to a file and needs the user to open or run it
- a **worm** copies itself across a network on its own

2.5

- any **two** of: strong mixed password / limit log-in attempts / two-step verification / delay after failed attempts

3.1 B

- a **device driver** is system software
- A, C and D are application software

3.2

(a)

- the printer is hardware that needs attention
- **hardware interrupt**

(b)

- the processor **stops and saves its place**
- it runs the **interrupt service routine**
- then **restores its place and carries on**

3.3

(a)

- email asking for card details: **phishing**; prevent by not clicking unexpected links / checking the sender / anti-spam
- packet sniffer on Wi-Fi: **data interception**; prevent by **encryption** or a wireless network key

- site flooded with requests: **DDoS**; prevent by a **firewall**, proxy, or filtering

(b)

- **phishing**: a message; the user must click or reply
- **pharming**: no message; code on the computer or DNS redirects to a fake site
- so the user can type the **correct address** and still arrive at the fake site

(c)

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

(d)

- a second code is sent to a device the real user holds
- an attacker with the password still **cannot log in without that code**

(e)

- **social engineering**
- staff training: never give a password over the phone; **verify who is asking**