1.3 EXCHANGING DATA · 1.3.3

Network security & threats

Malware, phishing, DoS and SQL injection — and how to defend against them. Spec 1.3.3(c).

01 Threats

Virus	Attaches to a host file; spreads when the file is run.
Worm	Self-spreading across a network; no host file needed.
Trojan	Disguised program; opens a back door.
Ransomware	Encrypts files, demands payment.
Phishing	Fake email/site tricks the **user** into giving data.
DoS	Floods a server so it can't serve users.
SQL injection	Malicious SQL via unvalidated input field.

02 Protection

Firewall	Filters traffic against a rule set (first line).
Anti-malware	Scans for & removes malware.
Encryption	Stolen/intercepted data stays unreadable.
Auth	Strong passwords, 2FA, access rights.
Education	Spot phishing — defends the human weak point.
Validation	Sanitise input → stops SQL injection.
Backups/ patch	Recover from ransomware; close vulnerabilities.

03 Match the defence to the threat

Virus/ worm	Anti-malware + patching.
Phishing	User education + 2FA.
DoS	Firewall / traffic filtering.
SQL injection	Input validation / parameterised queries.
Data theft	Encryption + access rights.

FINAL PASS BEFORE THE EXAM

Rapid exam tips

Six slips on security questions.

01

Worm = self-spreading; **virus** = needs a host file that is run.

02

A **firewall filters traffic**; **anti-malware removes malware** — different jobs.

03

Phishing targets the **user**; main defence is **education**.

04

SQL injection = **SQL typed into an input box**; fix = **input validation**.

05

In scenario questions, give **layered** defence and match each measure to a threat.

06

Encryption doesn't *stop* theft — it makes stolen data **unreadable**.