MODULE G · OCR J277 1.4.1, 1.4.2 · CAMBRIDGE 0478 5.3.1, 5.3.2

Network and cyber security

Malware, **social engineering**, **brute force**, **denial of service**, **interception**, **SQL injection** and the methods that limit them. Learn how each attack works, its purpose, and how each method limits it. **OCR J277: skip card 10. Cambridge 0478: skip 06 and 09**, and rows tagged for the other board. Specs as checked in November 2026.

01 Malware (G1) · both boards

Malware Software made to damage, disrupt or gain unauthorised access to a system.

Spread Email attachments, infected downloads and links, USB sticks, unpatched software.

Purpose Delete or corrupt data; steal data; extort money; take control of the device.

IGCSE only Virus (needs a host file), worm (spreads by itself), Trojan horse (disguised as genuine), spyware (records keys), adware (adverts), ransomware (encrypts files, demands payment).

02 Social engineering (G2) · both boards

Social eng. Manipulating people (trust, fear, urgency) into giving away information or access: fake calls, shoulder surfing.

Phishing Fake message from a "trusted" sender: click a link, open an attachment or reply. Aim: steal details, install malware.

GCSE only People are the "weak point".

IGCSE only Pharming: code on the device or a DNS server redirects to a fake site, even when the correct address is typed.

03 Brute-force attacks (G3) · both boards

How Software tries password after password (common ones first) until one works. Automated, very fast.

Purpose Unauthorised access: steal, change or delete data, plant malware.

Numbers 4-digit PIN: 10^4 = 10,000. 8 characters from 62: 62^8 = 218,340,105,584,896 (about 253 days at 10 million a second).

Limit Long, complex passwords; lock after a set number of fails (5 tries at a PIN = 1 in 2,000).

04 Denial of service (G4) · both boards

DoS Floods a server with more requests than it can handle; it slows or crashes; genuine users cannot get in.

DDoS Malware makes many devices into a botnet; they flood the server at once. Many IP addresses: hard to block.

Purpose Disrupt: lost sales, reputation, extortion, protest. Usually no data stolen.

Terms OCR says DoS; Cambridge says DDoS.

05 Interception (G5) · both boards

Interception Data captured while it is transmitted (packet sniffing). Wi-Fi is easier: anyone in range. Often unnoticed.

Purpose Steal passwords and bank details for fraud.

Limit Encryption: taken, but not understood without the key.

GCSE only Data theft: stolen laptops or USB drives; insiders copying files.

IGCSE only Hacking: unauthorised access to a system, to steal, change or delete data.

06 SQL injection (G6) GCSE only

How Attacker types SQL code into an input box (log-in, search). Not validated, so it becomes part of the site's query and the database runs it.

Purpose Bypass a log-in; view, steal, change or delete data.

Cause Poor input validation in the program.

Limit Input validation and sanitisation; restricted database access levels; penetration testing.

07 Firewalls and anti-malware (G7) · both boards

Firewall Checks traffic in and out of a network against rules; blocks what breaks them (IP addresses, ports, websites).

Limits Unauthorised access, malware connecting in or out, some DoS traffic. Not a USB stick.

Anti-malware Scans files against a database of known malware; quarantines or deletes it. Must be updated, or new malware is missed.

IGCSE only Anti-virus and anti-spyware. Automating software updates: patches fix weaknesses as soon as released.

08 Access levels and passwords (G8) · both boards

Access levels Read-only, read/write, administrator. A stolen log-in only gets that user's access.

Strong Long; upper and lowercase, digits, symbols; no words or personal details; not reused; never shared.

Lockout Locks after a set number of failed attempts: limits brute force.

IGCSE only Authentication: username and password, biometrics (fingerprint, face, iris, voice compared with stored data), two-step verification (one-time code to a registered phone or email).

09 Pen testing, physical, encryption (G9) GCSE only

Pen testing Authorised, simulated attacks to find weaknesses before real attackers; reported and fixed. Does not stop attacks itself.

Physical Locks, keycards, biometric doors, CCTV, alarms, guards. Limits theft and direct access to servers.

Encryption Scrambled with a key: stolen or intercepted data cannot be understood. Does not stop it being taken (D6).

10 Staying safe online (G10) IGCSE only

SSL Encrypts browser-server data; https:// and a padlock. Browser asks server to identify itself; server sends its SSL certificate; browser checks it; encrypted session begins.

Proxy server Between device and internet: hides the IP address, filters traffic, blocks sites, takes the force of a DDoS.

Privacy Settings limit who sees personal data: less to guess passwords or phish with.

Checks Hover to see a link's real URL (misspelt domain, http://). Spelling errors, generic greeting, urgency, threats = phishing.

01
Encryption does **not stop** interception or theft. The data **cannot be understood** without the key.

02
A firewall checks **network traffic**. Malware on a **USB stick** needs **anti-malware**.

03
Never write "more secure" alone. Name the **threat** and say **how** the method limits it.

04
Brute force: software guesses. **Social engineering**: a person is tricked. **DoS**: no data stolen.