OCR GCSE (J277)

Module G: Security

Workbooklet mark scheme · 9 parts · 184 marks

G10 is IGCSE only and not on J277.

Contents

Part	Topic	Marks
G1	Malware: mark scheme	21
G2	Social engineering and phishing: mark scheme	20
G3	Brute-force attacks: mark scheme	20
G4	Denial of service attacks: mark scheme	20
G5	Data interception and theft: mark scheme	21
G6	SQL injection: mark scheme	20
G7	Firewalls and anti-malware: mark scheme	21
G8	User access levels and passwords: mark scheme	20
G9	Preventing attacks 3: mark scheme	21
	Total	**184**

MODULE G SECURITY · G1

Malware: mark scheme

21 marks · OCR J277 spec 1.4.1 (forms of attack: malware; how the attack is used; the purpose of the attack)

How to use. One mark per bullet up to the maximum shown. **/** separates alternatives; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. J277 does not name types of malware, so students do not need to name them; where a correct type (e.g. virus, worm, Trojan, spyware, ransomware) is used accurately, accept it. Ways to prevent malware are tested in G7.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	(Malicious) software / a program designed to harm / damage / disrupt a computer (system) // to gain unauthorised access to a computer (system) / data	**1**	Must be software / a program with a harmful purpose. Do not accept "a virus" alone (an example, not a meaning). Do not accept "bad software" alone (NE).
1(b) J277 1.4.1	(Opening) an email attachment Clicking a link (in an email / message / on a website) Downloading / installing software / files (from the internet / an untrusted source) Removable media // USB memory stick / external drive Spreading across a network (from another infected computer) Through a weakness / vulnerability in software that has not been updated / patched Hidden inside / disguised as software that seems legitimate Installed by a hacker who has gained access (e.g. after a brute-force or social engineering attack)	**2**	1 mark each to max 2. Credit any other valid way. Do not award two marks for the same way written twice (e.g. "from the internet" and "from a website" with no further detail = 1 mark). "The internet" alone is NE.
2(a) J277 1.4.1	Records key presses and sends them: Steal data Locks files and demands payment: Extort money Overwrites documents: Delete or corrupt data Runs commands from another location: Take control of the device	**4**	1 mark per correct row. A row with two or more ticks scores 0.
3(a) J277 1.4.1	Spread on a USB memory stick: True Only by downloading from a website: False Some malware copies itself across a network without user action: True Always shows a warning: False	**4**	1 mark per correct row. A row with both boxes ticked scores 0.

QUESTION	ANSWER	MARKS	GUIDANCE
4(a) J277 1.4.1	The program appears to be legitimate / genuine / useful // the malware is disguised (as a useful program) ... the program does what it claims / converts files as expected (so nothing seems wrong) The malware runs secretly / hidden / in the background ... with no message / warning // nothing visible on screen The employee chose to install the program (so did not suspect it)	**2**	1 mark per bullet to max 2. Accept a correct reference to a Trojan (horse). Do not accept "the malware is invisible" alone (NE) unless linked to running in the background / with no sign.

4(b)
J277 1.4.1
	The data includes usernames / passwords / log-in details (typed by the employee)
	... the attacker can log in to the firm's systems / email / accounts (as the employee) // gain unauthorised access
	Access / steal / copy confidential client data / clients' financial records
	Bank / card details could be captured // money could be stolen / transferred (from the firm or clients)
	Data could be sold (to other criminals) // used for identity theft / fraud
	The attacker could change / delete the firm's data
	The attacker could install further malware (once logged in)
	The attacker could blackmail the firm / clients (by threatening to release data)
	Messages typed (e.g. emails) could be read // confidential business information revealed
		3	1 mark per bullet to max 3. Credit any other valid harm that follows from the recorded data. Do not accept "hack them" / "steal things" alone (NE).

5(a) J277 1.4.1	To extort money // to make the practice pay (a ransom / fee) (to unlock the files)	**1**	Accept "to get money (from the practice)". Do not accept "to lock the files" alone (that is how, not why). Accept ransomware named with the purpose.
5(b) J277 1.4.1	Staff cannot access appointment / animal / client records / bookings ... ... so the practice cannot treat animals / take bookings / work normally // the practice may have to close (for a time) The practice may lose income / money (while it cannot work) ... ... and it costs time / money to restore the files / systems (e.g. from a backup) The practice may pay the ransom ... ... but there is no guarantee the files will be unlocked // it could lose the money and the data Data may be permanently lost (if the files are never unlocked) ... ... so medical histories / treatment records are no longer available Client data may have been copied / stolen / leaked ... ... so the practice's reputation is damaged // clients lose trust / go to another practice	**4**	Mark in pairs: 1 mark for an effect, 1 mark for the linked expansion (...), max 2 per way, max 4. The second way must be different from the first. Do not accept "it is bad for the business" alone (NE). Credit any other valid effect with an expansion.

Total: 21 marks

MODULE G SECURITY · G2

Social engineering and phishing: mark scheme

20 marks · OCR J277 spec 1.4.1 (forms of attack: social engineering, e.g. phishing, people as the 'weak point'; how the attack is used; the purpose of the attack)

How to use. One mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. **NE** = not enough. Credit any other valid answer that shows the same understanding. Prevention methods are tested in G7 to G9 and are not needed here.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	Manipulating / tricking / deceiving people into giving away confidential / personal information (e.g. passwords) // into giving access (to a system) // into doing something that breaks security	**1**	Must refer to people / users being tricked. Do not accept "hacking" or "stealing data" alone (NE). An example alone (e.g. "phishing") is NE.
1(b) J277 1.4.1	People can be tricked / manipulated // people trust others / act on fear or urgency People make mistakes // are careless, e.g. reuse or write down passwords // click links / open attachments without checking People can give away passwords / details / access (willingly) ... so attackers can get past technical security (e.g. strong passwords, security software) without breaking it It is often easier (for an attacker) to trick a person than to attack the technology / system	**2**	Max 2. Accept examples that make the point, e.g. "an employee might tell a caller their password". Do not accept "people are not secure" alone (NE).
2(a) J277 1.4.1	Caller pretending to be IT support: Social engineering Software trying thousands of passwords: Not social engineering Watching someone type a password: Social engineering Server flooded with requests: Not social engineering	**4**	One mark per correct row. A row with both boxes ticked scores 0. Row 2 is a brute-force attack; row 3 is shoulder surfing; row 4 is a denial of service attack.
3(a) J277 1.4.1	It pretends to come from a trusted / familiar source // the payroll team It creates urgency // gives a time limit (24 hours) It uses fear / a threat // says the salary payment will be cancelled It makes responding easy // gives a button / link to click It looks official // uses an official-sounding subject line / "URGENT"	**2**	1 mark each to max 2. Mark the first answer on each line. Do not accept two answers that make the same point (e.g. "24 hours" and "urgent" = 1 mark). A generic greeting ("Dear staff member") or the odd sender address is a sign of phishing, not a way of persuading: do not credit.

QUESTION	ANSWER	MARKS	GUIDANCE
3(b) J277 1.4.1	The employee clicks the button / link (in the email) ... which takes them to a fake website / log-in page ... that looks like the real (payroll) site The employee enters their username / password / log-in details The details are sent to / captured / recorded by the attacker The attacker uses the details to log in to the (real) account	**3**	Max 3. Accept "replies with their log-in details" for MP4 + MP5 (1 mark each). Do not credit answers that describe a different attack, e.g. guessing every password.
3(c) J277 1.4.1	Steal / view personal data (e.g. address, bank details) // the firm's confidential data Change the bank details so the salary is paid to the attacker // commit fraud / steal money Use the details for identity theft Sell the details (to other criminals) Change / delete data Install malware // get into the firm's network (for further attacks) Send more phishing emails from the employee's account	**2**	1 mark each to max 2. Mark the first two answers. Two answers that make the same point score 1. Do not accept "hack them" alone (NE).
4(a) J277 1.4.1	The attack targets the person / receptionist, not the computer / technology // people are the weak point The receptionist may give the password willingly // is tricked into trusting the caller The attacker would then log in with the correct username and password ... so the log-in looks genuine / the security software has nothing to detect // no malware / technical weakness is needed	**2**	Max 2. Do not accept "security software does not work" or "the software is not good enough" (NE / wrong).
4(b) J277 1.4.1	1 mark for a method, 1 mark for how it gets the password, e.g. Shoulder surfing // watching someone enter their password ... ... then remembering / recording it to log in later Pretending in person to be a technician / visitor / new member of staff ... ... and asking a member of staff for their password / to log in for them Leaving an infected USB drive where staff will find it ... ... when plugged in, malware (e.g. spyware) records the password // sends it to the attacker A fake message on social media / a text message (e.g. from a fake colleague) ... ... asking for the password // linking to a fake log-in page	**2**	Mark in pairs: the second mark depends on a valid method. Mark the first method only. Any email (including a phishing email) or a phone call scores 0 (excluded by the question). Credit any other valid social engineering method. Brute force / guessing is not social engineering: 0.
5(a) J277 1.4.1	The attachment contains / is malware (e.g. a virus, trojan, spyware, ransomware) Opening it runs / installs the malware (on the computer) ... which could delete / corrupt / encrypt files // steal data / passwords // give the attacker control of the computer // spread to other computers	**2**	Max 2. Do not accept "it gives the computer a virus" alone for 2 marks (1 mark for MP1). Do not accept "it slows the computer" alone (NE).

Total: 20 marks

MODULE G SECURITY · G3

Brute-force attacks: mark scheme

20 marks · OCR J277 spec 1.4.1 (brute-force attacks: how the attack is used, its purpose) and 1.4.2 (passwords: how they limit the attack)

How to use. One mark per bullet up to the maximum shown. **/** separates alternatives; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. NE = not enough. For "give / state two" items, mark the first two answers only. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	Trial and error: True Tricking a person: False Automated, many passwords quickly: True Purpose is unauthorised access: True One more character reduces combinations: False	**5**	One mark per correct row. A row with both boxes ticked scores 0. Row 2 describes social engineering, not brute force.
2(a) J277 1.4.1	(The attacker uses) software / an automated program (to make the guesses) It tries (a member's username with) password after password // trial and error ... (systematically) trying every possible combination (of characters) Common / weak passwords / dictionary words may be tried first Huge numbers of attempts are made very quickly / per second Until the correct password is found / one works, (then the attacker logs in)	**3**	Max 3. Do not accept "hacks the account" or "guesses the password" alone (NE): the answer must show repeated / systematic attempts. Do not credit tricking the member or phishing (social engineering).
2(b) J277 1.4.1	Steal / view the member's personal data (name / address) Steal / use the payment card details // make payments / hire bikes with the member's card Change / delete the member's data // change the password to lock the member out Sell the data (to others) Use the details for identity theft / fraud Install / spread malware // use the account to attack the company's system	**2**	1 mark each, max 2. Do not accept "get into the account" / "gain access" (repeats the question). Two answers that are the same idea (e.g. "steal data" and "take data") = 1 mark.
3(a) J277 1.4.1, 1.4.2	Each extra character multiplies / greatly increases the number of possible passwords / combinations // e.g. 4 letters = 456,976 but 8 letters = about 209 billion So it takes (much) longer to try them all // e.g. under 0.1 seconds for 4 letters but about 6 hours for 8 letters ... so the attacker may give up / be detected (before the password is found)	**2**	Max 2. Credit figures quoted from the table as the evidence. Do not accept "more secure" / "harder to guess" alone (NE).

QUESTION	ANSWER	MARKS	GUIDANCE
3(b) J277 1.4.1, 1.4.2	More possible characters for each position (62 instead of 26) So there are (many) more possible combinations (for the same length) // e.g. about 218 million million (218,340,105,584,896) instead of about 209 billion So it takes much longer to try every combination // e.g. about 253 days instead of about 6 hours	**2**	Max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone (NE).
4(a) J277 1.4.2	C	**1**	Correct answer only. Accept the password written out instead of the letter.
4(b) J277 1.4.2	It is long / has 12 characters // it is the longest option It mixes uppercase and lowercase letters It contains digits / numbers It contains symbols / special characters It is random / is not a (dictionary) word / name // has no pattern or repeated characters	**2**	1 mark each, max 2. If 4(a) is not C, award marks only for features that are true of the password the student chose and that do make it harder to find (e.g. B: uppercase letter, digits). Do not accept "it is complicated / strong" alone (NE).
5(a) J277 1.4.1, 1.4.2	A brute-force attack needs to make a (very) large number of attempts / guesses Only five guesses can be made before the account is locked ... so the attack is slowed down (to a few guesses every 30 minutes) // the number of guesses that can be made is greatly reduced So it would take far too long to try every / enough combinations // the password is very unlikely to be found Repeated lock-outs can alert the user / the firm (that an attack is happening)	**3**	Max 3. Do not accept "stops hackers" or "makes it more secure" alone (NE). Allow "the attack is stopped / blocked" for the second or third point only if linked to the limited number of attempts.

Total: 20 marks

MODULE G SECURITY · G4

Denial of service attacks: mark scheme

20 marks · OCR J277 spec 1.4.1: forms of attack, denial of service attacks (threats posed to devices/systems, how the attack is used, the purpose of the attack)

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. Credit any other valid answer that shows the same understanding. A distributed denial of service (DDoS) attack is a form of denial of service attack: accept DDoS descriptions anywhere, but never require the term DDoS or botnet.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	Stops genuine users accessing a website / network: True Floods a server with more requests than it can handle: True Attacker must know a user's password: False Main aim is usually to copy the data on the server: False	**4**	1 mark per correct row. 2+ ticks in a row = 0 for that row.
2(a) J277 1.4.1	(The attacker) sends / floods the (web) server with a very large number of requests / traffic ... more requests than the server can handle / process // uses up the server's resources / the bandwidth available The server slows down / cannot respond / crashes Genuine customers' requests are not answered // customers cannot access / load the booking website The requests may be sent from many devices at the same time	**3**	1 mark per bullet, max 3. Must be an attack on the **server / website / network**. Do not credit answers that describe an attack on a customer's own computer. Do not accept "hacks the website" / "puts a virus on the server" / "steals the data". A description of how to prevent the attack scores 0.
2(b) J277 1.4.1	Cannot load / access the booking website // the website times out The website is very slow (to respond) Cannot book / buy tickets (online) at that time Cannot check / change / cancel an existing booking May have to book another way (e.g. by phone) // may book with a different company May miss out on a sailing / ticket offer	**2**	1 mark per bullet, max 2. Mark the first two answers. Two answers that say the same thing (e.g. "cannot access the site" and "cannot load the page") = 1 mark. Do not accept "their data is stolen" / "their computer gets a virus".
2(c) J277 1.4.1	Customers cannot book (1) ... so tickets are not sold / income is lost while the website is down (1) Customers may book with a competitor instead // may not come back (1) Damage to the company's reputation // customers lose trust in the company (1) ... so fewer bookings in future (1) Cost of staff time / experts to get the website working again (1) Cost of paying for extra protection / a bigger server / more bandwidth (1) Cost of refunds / compensation to customers who missed out (1)	**2**	1 mark per point, max 2. Two separate points, or one point and its expansion. Do not accept "they lose money" alone (repeats the question). Do not credit a ransom being paid unless linked to the attackers demanding payment.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.1	To disrupt the organisation // stop it providing its service To make the organisation lose money / income To damage the organisation's reputation To demand money to stop the attack // extortion / blackmail As a protest // to make a political point Revenge // a grudge (e.g. a former employee) As a distraction while another attack takes place To help a competitor // to stop customers using a rival For fun // to show they can do it	**2**	1 mark per bullet, max 2. Credit any other valid reason. Do not accept "to steal data" alone (a denial of service attack does not usually steal data); accept "to distract the organisation while data is stolen". Do not accept "ransom" alone without reference to payment to stop the attack.
4(a) J277 1.4.1	The devices have been infected with malware (e.g. from an email attachment / download) The malware lets the attacker control the devices (remotely) // the devices become bots / zombies / part of a botnet The attacker instructs the devices to send requests to the (ferry company's) server (at the same time) The malware runs hidden / in the background, so the owners do not notice	**2**	1 mark per bullet, max 2. Do not require the words bot / botnet. Accept "virus / Trojan" for malware. Do not accept "they have been hacked" alone.
4(b) J277 1.4.1	The requests come from many different devices // many different IP addresses / locations ... so blocking one device / IP address does not stop the others It is hard to tell the attack traffic from genuine customers' traffic // blocking the traffic could also block real customers Many devices together send far more requests than one computer could	**2**	1 mark per bullet, max 2. Do not accept "it is more powerful / bigger" alone. Do not accept "the devices are in other countries" alone (repeats the stem) unless linked to blocking.
5(a) J277 1.4.1	A denial of service attack aims to make the website / service unavailable, not to steal data It works by flooding the server with requests // it does not need to break into / log in to the server ... so customers' data is not usually accessed / stolen by this attack The slow website was caused by too much traffic / the server being overloaded, not by a break-in However, the attack could have been a distraction for a different attack, so the company should still check // data could only be stolen by a separate attack	**3**	1 mark per bullet, max 3. Full marks are possible without the final ("however") point. Do not credit answers that agree with the manager. Do not accept "the data is encrypted" / "they have a firewall" (not what the attack does).

Total: 20 marks

MODULE G SECURITY · G5

Data interception and theft: mark scheme

21 marks · OCR J277 spec 1.4.1, 1.4.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative answers; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. **NE** = not enough. Spec points covered: J277 1.4.1 forms of attack: data interception and theft (how the attack is used; the purpose of the attack); J277 1.4.2 how to limit the threats posed in 1.4.1 (encryption, physical security, user access levels, passwords and the other named methods). The term "packet sniffing" is credited but never required.

QUESTION	ANSWER	MARKS	GUIDANCE
1 J277 1.4.1	Data is captured while it is being transmitted across a network	**1**	Correct answer only. 2+ ticks = 0 marks.
2(a) J277 1.4.1	Data is sent across the network in packets Wireless signals can be picked up by any device within range The attacker uses software/hardware that captures/copies the packets // packet sniffing/packet sniffer The packets are captured/copied while they are being transmitted // in transit The attacker examines/analyses the contents of the captured packets ... looking for useful data, e.g. usernames, passwords, payment/card details If the data is not encrypted, the attacker can understand it	**3**	1 mark per bullet, max 3. "Hacks the Wi-Fi" / "steals the data" alone = NE: must describe the data being captured while it is transmitted. Do not credit descriptions of other attacks (e.g. flooding the network, guessing passwords). Credit any other valid answer.
2(b) J277 1.4.1	The data still reaches its destination / the online shop (as normal) ... because the attacker copies the data rather than stopping/blocking it The attacker does not change the data, so nothing looks different to the customer // there is no visible sign / no warning on the phone The attacker only listens/receives, so does not need to interact with the customer's phone	**2**	1 mark per bullet, max 2. "It is hidden" / "the attacker is sneaky" alone = NE. Credit any other valid answer.
2(c) J277 1.4.1	Wireless data is sent through the air / as radio signals ... so anyone within range can pick up the signals No physical access to a cable / the network hardware is needed // with a wired network the attacker would need to connect to the cable The signal may reach beyond the café, e.g. outside / next door, so the attacker need not be inside	**2**	1 mark per bullet, max 2. "Wireless is less secure" alone = NE: must say why. Do not accept "wired networks cannot be intercepted" alone. Credit any other valid answer.

QUESTION	ANSWER	MARKS	GUIDANCE
2(d) J277 1.4.1	To steal the login details / username and password (1) ... to log in to the customer's shop account and place orders / change the account details (1) To steal the payment / card / bank details (1) ... to make purchases / take money (fraud) // to sell the details to other criminals (1) To steal personal details, e.g. name, address, email (1) ... to commit identity theft // open accounts in the customer's name (1) To collect personal/private information (1) ... to blackmail the customer // to send them targeted phishing messages (1) To sell the stolen data (1) ... for money / profit (1)	**4**	Mark in pairs: 1 for the purpose, 1 for the explanation. The second mark depends on the first. Do not award the same purpose twice. "To steal data" alone = NE: must say what data or what it is used for. Credit any other valid answer.
3(a) J277 1.4.1	A laptop is stolen / lost and taken (e.g. from a meeting or a car) A storage device / USB drive / backup holding the records is stolen A member of staff / insider copies the records (e.g. to a USB drive / personal email) without permission Someone uses a laptop left logged in / unattended to copy the data Someone reads / photographs the data on the screen // shoulder surfing Printed copies of the records are taken Someone gains unauthorised access to the agency's files / system and copies the data	**2**	1 mark per bullet, max 2. Mark the first two answers. Do not accept answers that describe interception of data during transmission (the question excludes it). Credit any other valid answer.
3(b) J277 1.4.1, 1.4.2	Encrypting storage prevents the laptop being stolen: False Thief cannot understand encrypted data without the key: True Data theft can be carried out by a person who works for the organisation: True	**3**	1 mark per correct row. 2+ ticks in a row = 0 for that row.

QUESTION	ANSWER	MARKS	GUIDANCE
4 J277 1.4.2	Encryption (1) … if a laptop / data is stolen, the data cannot be understood without the key (1) Physical security, e.g. locks / locked cupboards / cable locks / keycard doors / CCTV / alarms (1) … stops unauthorised people physically getting to / taking the laptops or storage devices // deters theft (1) User access levels (1) … each member of staff can only open/copy the records they need, so an insider (or someone using their account) cannot take all the data (1) (Strong) passwords (1) … a thief / unauthorised person cannot log in to the laptop / open the records without knowing the password (1) Firewall (1) … blocks unauthorised connections to the agency's network // can block data being sent out to unauthorised places (1) Anti-malware (software) (1) … detects and removes malware such as spyware that could send the data to an attacker (1) Penetration testing (1) … finds weaknesses in the agency's systems so they can be fixed before data is stolen (1)	**4**	Mark in pairs: 1 for the method, 1 for how it limits data theft. The second mark depends on the first. Two different methods needed. Encryption: do not accept "stops the data being stolen"; "cannot be read" alone = NE (it cannot be *understood*). "Makes it more secure" alone = NE. Credit any other valid J277 1.4.2 method with a matching explanation.

Total: 21 marks

MODULE G SECURITY · G6

SQL injection: mark scheme

20 marks · OCR J277 spec 1.4.1: the concept of SQL injection (how the attack is used, the purpose of the attack); 1.4.2: how to limit the threat (user access levels, penetration testing) and remove the vulnerability (input validation, also J277 2.3.1)

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. **...** at the start of a bullet means it builds on the bullet before. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1, 1.4.2	Enters SQL code into an input box: True Malware that copies itself: False Could change or delete records: True Encrypting browser–server data prevents it: False	**4**	1 mark per correct row. 2 ticks in a row = 0 for that row. Row 4: the code is typed into the site's own form, so it reaches the server whether or not the connection is encrypted.
2(a) J277 1.4.1	(Attacker) types / enters SQL code / commands into an input box / field / form (on a website) The code becomes part of the website's (SQL) query // the code is run / executed by the database To access / view / steal / change / delete data without permission // to bypass a login / authentication It takes advantage of input that is not validated / checked	**2**	1 mark per bullet, max 2. Do not accept "hacking a database" or "attacking a website" alone (NE). Do not accept answers that describe it as a virus / malware.
2(b) J277 1.4.1	The typed text is put directly into the query // the input is not validated / checked before it is used (1) ... so the database treats the typed code as part of the SQL command / runs it, instead of treating it as a plant name to search for (1) The code can change the condition / the WHERE part // can make the query return / affect other data (e.g. customer details) (1)	**2**	1 mark per bullet, max 2. Do not accept "the query will not work" or "it causes an error" alone. Answers do not need to quote any SQL.
2(c) J277 1.4.1	View / read / steal customers' names / addresses / order details Change / alter data, e.g. plant prices / orders / customer addresses Delete records / tables / data (e.g. the plant list or orders) Add (false) records, e.g. fake orders / accounts Get past a login / bypass authentication // gain access to an account (e.g. an administrator or customer account)	**2**	1 mark each, max 2. Mark the first two answers. Each must be a different action (view, change, delete, add, bypass login). Do not accept "hack the database", "get data" alone (NE), or "install a virus / malware".

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.1	The attacker types SQL code / commands (into the username or password box) instead of a normal username / password The input is not validated / checked / sanitised ... ... so the code becomes part of the login query / is joined into the query The code changes the query's condition so it is always true // so it no longer checks the password (correctly) The database finds / returns a matching record ... ... so the website logs the attacker in // authentication is bypassed	**3**	1 mark per bullet, max 3. Candidates do not need to give any actual SQL. Do not accept "guesses the password" or "tries every password" (that is a brute-force attack). Do not accept "hacks in" alone (NE).
3(b) J277 1.4.1, 2.3.1	The input is not validated / checked / sanitised (before it is used) // the typed values are put directly into the SQL query	**1**	Accept "it does not use parameterised queries / prepared statements". Do not accept "weak passwords", "no firewall" or "no encryption".
4(a) J277 1.4.2, 2.3.1	The program checks the input before it is used in the query / sent to the database (1) Input that contains SQL code / commands / unexpected characters (e.g. quote marks) // that is too long / not in the expected format is rejected / removed (1) ... so the attacker's code is never run by the database / never becomes part of the query (1)	**2**	1 mark per bullet, max 2. Accept "sanitisation" for validation. Do not accept "it checks the password is correct" (that is authentication, not validation). Do not accept "stops hackers" alone (NE).
4(b) J277 1.4.2	The account is given only the access it needs, e.g. read-only / only the tables needed for logging in (1) Injected code could then not change / delete data (1) Injected code could then not reach other tables, e.g. members' payment details (1)	**2**	1 mark per bullet, max 2. Do not accept "it stops SQL injection" (it limits the damage, not the attack). Do not accept "members get less access" (the question is about the program's account).
5(a) J277 1.4.2	Authorised testers / the security firm simulate / carry out an attack on the website (with permission) (1) e.g. they try entering SQL code into the login / input boxes (1) To find weaknesses / vulnerabilities (before a real attacker does) (1) ... so the weaknesses can be reported and fixed / the program can be changed before the form goes live (1)	**2**	1 mark per bullet, max 2. Do not accept "tests the website" or "tests the passwords" alone (NE). Do not accept answers that say penetration testing stops attacks by itself.

Total: 20 marks

MODULE G SECURITY · G7

Firewalls and anti-malware: mark scheme

21 marks · OCR J277 spec 1.4.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative answers; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. **...** at the start of a bullet means it builds on the bullet before. **NE** = not enough. Spec points covered (J277 1.4.2): anti-malware software and firewalls as prevention methods, including what each may limit/prevent and how it limits the attack (threats from 1.4.1). Penetration testing, user access levels, passwords, encryption and physical security (also 1.4.2) are tested in other Module G worksheets, not here.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.2	Checks data in and out of a network against rules: Firewall Compares files with a database of known malware: Anti-malware software Moves an infected file into quarantine: Anti-malware software Can block traffic from a particular IP address: Firewall	**4**	1 mark per correct row. 2+ ticks in a row = 0 for that row.
2(a) J277 1.4.2	Monitors / examines (all) traffic / data (packets) coming into (and going out of) the network Checks the traffic against a set of rules / criteria (set by the company) Blocks / rejects traffic that breaks the rules // that comes from an unknown / untrusted / blocked source Only allows traffic that meets the rules / that is from a trusted source // that the network asked for Sits between the network and the internet // acts as a barrier, so a hacker's connection from the internet does not reach the computers / server Can log / alert staff to blocked attempts to get in	**3**	Max 3. "Stops hackers" alone = NE (must say how). "Blocks viruses" alone = NE here. Do not accept answers that describe scanning files on the computer (that is anti-malware). Credit any other valid answer.
2(b) J277 1.4.2	Block traffic from (a list of) particular / suspicious IP addresses Only allow traffic from (a list of) trusted IP addresses / devices // whitelist Block access to particular websites / web addresses Block particular ports // only allow traffic on certain ports Block particular programs / types of traffic from using the network // e.g. block file-sharing traffic Block incoming connections that the network did not request Block traffic at certain times // e.g. outside office hours	**2**	1 mark each to max 2. Mark first two answers only. Two answers that are the same rule reworded = 1 mark. "Block hackers" / "block bad traffic" = NE. Credit any other valid rule.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.2 (threats from 1.4.1)	**Form of attack (1 mark):** Malware // named type of malware e.g. virus, worm, spyware, ransomware Denial of service (DoS / DDoS) **How (max 2), e.g.:** *Malware:* blocks downloads / traffic from known malicious / blocked websites or IP addresses ... stops malware already on a computer connecting to / sending data out to the attacker ... blocks unrequested incoming connections that malware (e.g. a worm) uses to spread *DoS:* identifies traffic from the attacking IP address(es) ... and blocks / drops it before it reaches the server ... can limit / block an unusually large number of requests (from one source) // so the server is not overwhelmed / stays available	**3**	1 mark for a valid attack, then up to 2 for how the firewall limits that attack. No marks for "how" if the attack is invalid. Do **not** accept data interception (a firewall does not stop data being intercepted while it travels across the internet). Do not accept "unauthorised access / hacking" (excluded by the question). Credit any other valid attack with a valid "how", e.g. brute-force: blocks repeated login attempts from the same IP address.
4(a) J277 1.4.2	Scans files / programs / downloads / email attachments / memory (for malware) Compares them with a database / list / signatures of known malware Checks files as they are opened / downloaded // real-time scanning // runs scheduled scans Removes / deletes the malware // quarantines the infected file (so it cannot run / spread) Alerts / warns the user that malware has been found Can detect suspicious behaviour of a program (that may be new malware) Can stop malware being installed / downloaded // blocks it before it runs	**3**	Max 3. "Gets rid of viruses" alone = 1 mark (removes malware) only. "Stops hackers" = NE. Do not accept answers that describe checking network traffic against rules (that is a firewall). Credit any other valid answer.
4(b) J277 1.4.2	New malware is being created all the time ... the update adds the new malware to the database / definitions / signatures ... otherwise (new) malware not in the database would not be detected / could infect the computer Updates can also fix weaknesses / bugs in the anti-malware software itself	**2**	Max 2. "To keep it up to date" / "to make it work better" = NE. Credit any other valid answer.

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) J277 1.4.2	**Why the firewall will not stop it (max 2):** A firewall (only) monitors / filters network traffic // data passing between the network and the internet The memory stick is connected directly to the computer // the malware does not travel across the network / through the firewall A firewall does not scan / check files stored on a device **How anti-malware limits it (max 2):** Scans the files on the memory stick (when it is plugged in / when a file is opened) Compares the files with its database of known malware Quarantines / deletes the infected file // stops it running ... before it can infect / damage the computer // spread to other computers on the network Warns the worker that the file contains malware	**4**	Max 4. Max 2 for each half: an answer that covers only one half scores max 2. "The firewall doesn't work offline" = NE. Do not credit the claim that anti-malware stops the memory stick being plugged in. Credit any other valid answer.

Total: 21 marks

MODULE G SECURITY · G8

User access levels and passwords: mark scheme

20 marks · OCR J277 spec 1.4.2 (user access levels, passwords; how each limits the threats in 1.4.1)

How to use. 1 mark per bullet up to the Max shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. "..." means the point builds on the one before it. Credit any other valid answer that shows the same understanding. Biometrics and two-step verification are not J277 prevention methods: do not penalise them, but they earn no marks where the question asks about user access levels or passwords.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.2	Different permissions (read-only, read/write): User access levels Secret string entered with a username: Passwords Stops people getting to data they are not authorised to access: Both Harder to crack in a brute-force attack when long and mixed: Passwords	**4**	1 mark per correct row. 2+ ticks in a row = 0 for that row.
2(a) J277 1.4.2	1 mark each to Max 2: Contains a (dictionary) word / name // Rover could be found in a dictionary / common-word list (tried early in an attack) Uses personal details // the dog's name / year of birth could be found out / guessed (e.g. from social media) Has no symbols / special characters It is (quite) short // only 9 characters Follows a predictable pattern // word followed by a year	**2**	Mark the first answer on each line. Do not accept "has no capital letters" or "has no numbers" (it has both). "Easy to guess" alone = NE; needs a reason (word / personal detail / pattern).
2(b) J277 1.4.2	1 mark each to Max 2: A strong password is long / uses a mix of upper case, lower case, numbers and symbols // is not a word or personal detail ... so there are many more possible combinations (to try) ... so it would take (far) too long for the software to try every combination // the attacker is less likely to find it Not a common / dictionary word, so it is not found by trying common passwords / words first	**2**	"Harder to guess" / "more secure" alone = NE. A brute-force attack does not "decrypt" a password: no credit for that.
2(c) J277 1.4.2	1 mark each to Max 2: A brute-force attack needs to make a very large number of attempts / guesses After five wrong attempts no more guesses can be made (on that account) ... so the attacker cannot keep trying combinations until one works // the attack is stopped The locked account alerts the user / technician that someone may be trying to get in	**2**	"Stops hackers" alone = NE. Must link the lock to stopping repeated / many guesses.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.2	1 mark each to Max 2: Never tell anyone your password // do not give it over the phone / by email, even to IT staff Check a caller is genuine (e.g. call the IT department back on a known number) before giving any details Do not write the password down / leave it where others can see it Do not let anyone watch you type it // cover the keyboard (shoulder surfing) Do not enter your password through a link in an email / message (phishing) Do not share / reuse your password (on other accounts / sites) Change the password straight away if you think someone knows it	**2**	Mark the first answer on each line. Rules about password strength (length, symbols) answer a different question: no credit here. Credit any other valid rule that keeps the password secret.
4(a) J277 1.4.2	Read-only (access)	**1**	Accept "read" / "view only". Do not accept read/write, full access, or no access.
4(b) J277 1.4.2	1 mark each to Max 3: The attacker only gets the permissions / access rights of the administrator's account The attacker cannot open / see / steal the staff pay records The attacker can only read / view the design files // cannot change / edit / delete the designs The attacker cannot change settings / other users' permissions // cannot install software (e.g. malware), as this is not an administrator-level account So less data can be stolen / damaged // the damage is limited to what that user can reach	**3**	Award marks applied to the scenario. "Stops the attacker logging in" = 0 (the attacker has already logged in). Do not accept "the attacker cannot see anything".
5(a) J277 1.4.2 (limiting 1.4.1 threats)	1 mark each to Max 4: A strong password can still be found out / stolen // e.g. through phishing / social engineering / shoulder surfing / spyware / a data breach Once an attacker is logged in, a password does not limit what they can do Access levels limit what each account can see / change / delete ... so a stolen account can only reach part of the data // damage / data theft is limited Employees already know their own passwords, so a password does not stop an employee (insider) looking at / copying / deleting data they should not Sensitive data, e.g. pay records, can be restricted to only the staff who need it Read-only access reduces accidental (or deliberate) changes / deletion of designs Fewer accounts can install software / change settings, so malware is less likely to be installed	**4**	At least one mark must explain a limit of passwords and at least one must explain what access levels add; otherwise Max 3. Generic "more secure" / "extra layer of security" alone = NE.

Total: 20 marks

MODULE G SECURITY · G9

Preventing attacks 3: mark scheme

21 marks · OCR J277 spec 1.4.2

How to use. 1 mark per bullet up to the maximum shown. **/** separates alternative answers; **//** separates alternative statements for the same mark. Words in (brackets) are not needed for the mark. **NE** = not enough. **BOD** = benefit of the doubt. Spec points covered (J277 1.4.2): common prevention methods (penetration testing, encryption, physical security; firewalls only as a contrast in Q1 and Q5); what each prevention method may limit/prevent and how it limits the attack; methods to remove vulnerabilities; how to limit the threats posed in 1.4.1. Anti-malware, user access levels and passwords (also 1.4.2) are tested in G7/G8. This part is OCR only: Cambridge 0478 5.3.2 does not list penetration testing or physical security.

QUESTION	ANSWER	MARKS	GUIDANCE
1 J277 1.4.2	Keycard to open the server room door: physical security Security team tries to break in, with permission: penetration testing Data scrambled using a key: encryption Incoming traffic checked against rules: firewall	**4**	1 mark per correct row. Anti-malware is not used. Accept "pen testing" / "penetration test". Ignore spelling if the method is clear.
2(a) J277 1.4.2, 1.4.1	Lock the server room door // fit a keycard / keypad / biometric lock (1) ... so only authorised staff can get in // the visitor cannot reach the servers (1) Security guard / reception desk that signs visitors in // visitors must be escorted (1) ... so visitors cannot walk into the server room on their own (1) Keep the servers in a locked cabinet / rack // physically lock / block the USB ports (1) ... so nothing can be plugged in even if someone enters the room (1) CCTV / alarm on the server room (1) ... deters the visitor // the person can be identified // staff are alerted quickly (1)	**2**	Mark in pairs: 1 for a physical security method, 1 for how it limits this threat. The second mark depends on the first. Do not award software methods (e.g. anti-malware, firewall, encryption, passwords): they are not physical security. "Security" / "protect the room" alone = NE. Credit any other valid physical security method with a matching explanation.
2(b) J277 1.4.2, 1.4.1	Lock the laptop in a drawer / cabinet / safe overnight (1) ... so it cannot be picked up from the desk (1) Cable lock fixing the laptop to the desk (1) ... so it cannot easily be carried away (1) Lock the office // keycard / biometric entry to the office (1) ... so only authorised people can get to the desk after hours (1) Alarm / security guard / night patrol (1) ... stops or interrupts a break-in // staff / guards are alerted (1) CCTV (1) ... deters theft // the thief can be identified (and the laptop recovered) (1)	**2**	Mark in pairs as 2(a). Do not award encryption or a password here: they protect the data, not the laptop, and are not physical security. The same method as 2(a) can score again if the explanation is applied to the laptop. Credit any other valid physical security method with a matching explanation.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) J277 1.4.2	Penetration testing simulates a real attack (on the new page) // an authorised person tries to break in It finds vulnerabilities / weaknesses (e.g. in the login, search box, payment form or database) ... before real attackers / criminals can find and exploit them The weaknesses are reported so they can be fixed / removed before the page goes live Reduces the risk of customer (login / payment) details being stolen // of attackers getting in through the new page	**3**	1 mark per bullet, max 3. "To check it is secure" / "to test it" alone = NE. Do not award answers saying penetration testing *stops* attacks by itself: it finds weaknesses, and fixing them limits attacks. Credit any other valid point.
3(b) J277 1.4.2, 1.4.1	Brute-force attack (e.g. on customer logins) SQL injection (e.g. through the login or search box) Denial of service (DoS / DDoS) Social engineering / phishing (e.g. of staff) Malware Data interception	**2**	1 mark each, max 2. Mark the first answer on each line. Two answers that are the same attack (e.g. "DoS" and "DDoS") = 1 mark. "Hacking" alone = NE. Credit any other valid form of attack from J277 1.4.1.
3(c) J277 1.4.2	A penetration tester has permission (from the owner) // is authorised / employed / paid by the company; a criminal attacker does not have permission A penetration tester reports the weaknesses so they can be fixed; a criminal attacker exploits them // steals / changes / deletes data A penetration tester does not damage the system or keep the data	**1**	Any one. Mark the first answer only. Only one side of the difference needs to be stated if the other is clearly implied. "One is legal" alone = BOD. "Uses different tools" = 0.
4(a) J277 1.4.2, 1.4.1	The data on the drive is scrambled / encoded (using a key / an encryption algorithm) The thief cannot understand the customer data // the data is meaningless ... without the (correct) key Only the company (with the key) can decrypt it / turn it back into the original data	**2**	1 mark per bullet, max 2. "Cannot be read / accessed" alone = NE (it can be read, it just cannot be understood). Do not award "the drive cannot be stolen" or "stops the data being taken": encryption does not stop theft.
4(b) J277 1.4.2, 1.4.1	Data interception (e.g. when customer data is sent over the internet / a network) // packet sniffing Theft of data by someone who gets unauthorised access to the server / database (e.g. a hacker or SQL injection), because the stolen data is meaningless A member of staff copying the files without permission Theft of another device / storage medium holding the data (e.g. the laptop in Q2(b))	**1**	Any one. Mark the first answer only. Do not accept denial of service, brute-force or phishing alone: encryption does not limit these. "Hacking" alone = NE unless linked to stealing the data. Credit any other valid answer.

QUESTION	ANSWER	MARKS	GUIDANCE
5 J277 1.4.2	**Physical security** A firewall only checks / filters network traffic (between the network and the internet) // it does nothing to stop someone physically reaching the servers Someone in the building could steal / damage a server or copy data from it (e.g. with a USB drive) without going through the firewall Physical security (e.g. locks / keycards / CCTV / guards) stops or limits unauthorised people getting to the servers **Penetration testing** The firewall may be set up wrongly / have weak rules // the system may have other vulnerabilities that a firewall does not stop Some attacks (e.g. SQL injection or brute-force on the login page) arrive in traffic the firewall allows through to the website Penetration testing finds these weaknesses (including in the firewall set-up) so they can be fixed before attackers exploit them	**4**	1 mark per bullet, max 4. Max 2 if only physical security **or** only penetration testing is addressed. "A firewall is not enough" / "hackers can get past it" alone = NE: must say why. Credit any other valid point (e.g. a firewall does not limit threats from staff already inside the building).

Total: 21 marks