CAMBRIDGE IGCSE (0478)

Module G: Security

Workbooklet mark scheme · 8 parts · 166 marks

G6 and G9 are GCSE (OCR) only and not on 0478.

Contents

Part	Topic	Marks
G1	Malware: mark scheme	21
G2	Social engineering, phishing and pharming: mark scheme	20
G3	Brute-force attacks: mark scheme	20
G4	DDoS attacks: mark scheme	20
G5	Hacking and data interception: mark scheme	21
G7	Firewalls, anti-malware and updates: mark scheme	21
G8	Access levels and authentication: mark scheme	21
G10	Staying safe online: SSL, proxy servers, privacy settings and checking messages: mark scheme	22
	Total	**166**

MODULE G SECURITY · G1

Malware: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.1 (processes and aim of cyber security threats: malware: virus, worm, Trojan horse, spyware, adware, ransomware)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. A bullet starting "..." builds on the one before it. Credit any other valid answer that shows the same understanding. Anti-malware and other solutions are tested in G7.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	One mark for each correct type: Unwanted adverts, redirects searches: adware Standalone, copies itself across a network: worm Encrypts files, demands payment: ransomware Looks genuine, hidden harmful code: Trojan horse Attaches to a file / program: virus Monitors user, sends data to a third party: spyware	**6**	Accept "Trojan" for Trojan horse. Ignore capitals and minor spelling errors if the type is clear. Do not accept "malware" or "hacking" for any row. Accept "keylogger" for the spyware row.
2(a) 0478 5.3.1	Any two from: The worm replicates / copies itself ... and sends / moves the copies across the network to other (connected) computers It does not need to attach to a host file / program // it is standalone It does not need any user action / input (to spread) It uses weaknesses / security holes / vulnerabilities in software / the operating system (to get onto other computers)	**2**	max 2. Do not accept "it is sent by email by the user" (that needs user action).
2(b) 0478 5.3.1	Any two from: Uses up / takes up bandwidth // slows the network down Takes up storage / memory space Slows down / crashes the computers Deletes / damages / corrupts data / files Opens back doors (to the computers) // lets a hacker gain access Installs / delivers other malware (onto networked computers) The network / systems may have to be shut down / taken offline (to remove it)	**2**	max 2. Do not accept "it spreads" alone (that is how, not an effect).

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.1	Any three from: The ransomware gets onto the system (e.g. through an email attachment / a link / a download / removable media) It encrypts the data / files (on the firm's computers / system) ... so the firm cannot access / use its data / files / computers A message / demand for payment / a ransom (fee) is displayed ... the decryption key is only given if the fee is paid // the files are only "released" if the fee is paid The attacker may threaten to delete / publish the data (if the fee is not paid) Paying does not guarantee the files will be decrypted	**3**	max 3. Accept "locks" for encrypts. Do not accept "it steals the files" alone.
3(b) 0478 5.3.1	Any one from: To extort money // to get the victim to pay a fee / ransom (to unlock / decrypt the data)	**1**	Accept "to make money from the victim". Do not accept "to encrypt files" (that is the process, not the aim).
4(a) 0478 5.3.1	Any two from: The spyware monitors / records key presses // acts as a keylogger ... it captures the username / password (as it is typed) The data is sent to a third party / the attacker ... who uses the log-in details to log in to the accounts	**2**	max 2. Accept "records screen activity / what the user types" for MP1. Do not accept "it hacks the account" alone.
4(b) 0478 5.3.1	Any two from: Displays / generates unwanted adverts / pop-ups Redirects the browser / searches / user to other / fake / unsafe websites Slows down the computer // reduces internet speed / performance Adverts, when clicked, may link to / download other malware / viruses May contain spyware // may collect data about the user / browsing May change browser settings / the home page // can be hard to remove	**2**	max 2. Two different effects needed.
5(a) 0478 5.3.1	A virus needs a host file / program: True A Trojan horse copies itself on its own: False Some adware contains spyware: True	**3**	One mark per correct row. A row with both boxes ticked scores 0.

Total: 21 marks

MODULE G SECURITY · G2

Social engineering, phishing and pharming: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (the processes involved in, and the aim of, social engineering, phishing and pharming)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. Credit any other valid answer that shows the same understanding. Solutions such as checking the URL or the spelling and tone of a message (0478 5.3.2) are tested in G10.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	B	**1**	More than one box ticked scores 0.
2(a) 0478 5.3.1	Email that appears to come from the bank: Phishing Sent to a fake website after typing the correct address: Pharming Replies to a fake message with their password: Phishing Can work without the attacker sending any message: Pharming	**4**	One mark per correct row. A row with both boxes ticked scores 0.
3(a) 0478 5.3.1	Any three from: The customer clicks a link / opens an attachment that downloads the malicious code (onto their computer) Malicious code / malware is installed on the customer's computer // malicious code is stored on a DNS server / web server The (malicious) code changes / alters the IP address linked to the web address / URL // changes the DNS entry / record When the customer types the (correct) URL ... ... the request is redirected to the fake website (instead of the real one) The fake website looks like the real one // the customer does not know they have been redirected	**3**	max 3. Do not credit a link in an email taking the customer straight to the fake website (that is phishing): the customers typed the correct address. Credit clicking a link or attachment only when it installs the malicious code. Accept "the code redirects the browser / user to the fake website" for MP5.
3(b) 0478 5.3.1	Any two from: To obtain / collect / harvest the customers' card / bank / personal details ... that are entered into the fake website ... to use them for fraud // to steal money // to make purchases with the card ... for identity theft // to sell the details (to other criminals)	**2**	max 2. Do not accept "to hack the company" alone. Do not accept "to crash / slow down the website".
4(a) 0478 5.3.1	Any two from: Pretends to be someone trusted / in authority // pretends to be from IT support Creates urgency // gives a short time limit (ten minutes / "straight away") Uses fear / a threat // says the account will be locked Does not give the receptionist time to check (who is calling)	**2**	max 2. Two answers that make the same point (e.g. "ten minutes" and "straight away") score 1.

QUESTION	ANSWER	MARKS	GUIDANCE
4(b) 0478 5.3.1	Any one from: To obtain the receptionist's password // log-in details To gain (unauthorised) access to the receptionist's account / the firm's computer system / the firm's data	**1**	Do not accept "to hack" alone.
4(c) 0478 5.3.1	One mark for a method, one mark for how it gains access, e.g. Shoulder surfing // watching someone type their password ... ... and then using the password to log in Leaving a USB drive (containing malware) where an employee will find it ... ... when it is plugged in, the malware is installed / gives the attacker access // records / sends passwords to the attacker Pretending in person to be a technician / visitor / new employee ... ... to be let into the building / to be given a password / to be logged in to a computer Sending a fake text / social media message pretending to be a trusted person ... ... asking for log-in details // linking to a fake log-in page	**2**	max 2. Second mark must follow from a valid method. Mark the first method only. A phone call or an email scores 0 (excluded by the question). Do not credit brute-force or other non-social-engineering attacks.
5(a) 0478 5.3.1	Any three from: The message appears to come from a trusted source / the bank It creates urgency / fear (an unusual payment) so the user acts quickly The user taps / clicks the link ... ... which takes them to a fake website (that looks like the bank's) The user enters their bank / log-in / card details The details are sent to / collected by the attacker // the attacker uses the details for fraud / to access the account	**3**	max 3. Accept "the link downloads malware that steals the details" as an alternative for MP4 + MP5 (max 2 for this route). Do not credit a description of pharming (redirection after typing a correct URL).
5(b) 0478 5.3.1	Any two from: Phishing needs the user to click / tap a link / respond to a message ... ... whereas pharming redirects the user even when they type the correct URL Phishing sends a fake message / email to the user ... ... whereas pharming uses malicious code on the user's computer / a DNS server With pharming the user may not have received any message from the attacker	**2**	max 2. A difference must be clear. 1 mark for a correct statement about one attack only; 2 marks need the comparison with the other. Do not accept "pharming is more dangerous" alone.

Total: 20 marks

MODULE G SECURITY · G3

Brute-force attacks: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (process and aim of a brute-force attack) and 5.3.2 (solutions: authentication by username and password, biometrics, two-step verification)

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

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	Row 2 ticked only (using a program to try one password after another)	**1**	More than one tick = 0. (Row 1 is DDoS, row 3 pharming, row 4 phishing.)
2(a) 0478 5.3.1	Any three from: Trial and error (is used) to guess / find the password // password after password is tried (with the guest's username) Every possible combination of characters is tried (in turn) ... until the correct password is found / one works // then the hacker logs in to the account It can be carried out automatically by software / a program Common / weak passwords / dictionary words may be tried first A huge number of attempts are made very quickly / every second	**3**	max 3. The "... until" point builds on the trial-and-error or the combination point. Accept "tries to guess the password" for the trial-and-error point. Do not accept "hacks into the account" alone. Do not credit tricking the guest (that is phishing / social engineering).
2(b) 0478 5.3.1	One mark for each correct row: Obtain payment card details: Yes Make the website unavailable by flooding it: No Change or cancel bookings: Yes	**3**	A row with both boxes ticked scores 0. Row 2 is the aim of a DDoS attack.
3(a) 0478 5.3.1, 5.3.2	Any two from: A longer password has (many) more possible combinations // each extra character multiplies the number of combinations // e.g. 456,976 for 4 letters but about 209 billion for 8 letters ... so it takes (much) longer to try them all // e.g. less than 0.1 seconds for 4 letters but about 6 hours for 8 letters ... so a longer password is less likely to be found // the attack is less likely to succeed (in a reasonable time)	**2**	max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone.

QUESTION	ANSWER	MARKS	GUIDANCE
3(b) 0478 5.3.1, 5.3.2	Any two from: More characters can be used in each position // 62 possible characters 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 them all // e.g. about 253 days instead of about 6 hours So the guests' accounts / card details are less likely to be accessed	**2**	max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone.
4(a) 0478 5.3.2	Any two from: A brute-force attack needs to make a very large number of attempts Only a few attempts are allowed before the account is locked // the hacker cannot keep repeatedly trying passwords ... so it would take far too long to try enough combinations // the password is very unlikely to be found The guest / hotel can be alerted that someone is trying to get in	**2**	max 2. Do not accept "stops hackers" / "makes it more secure" alone.
4(b) 0478 5.3.2	Any two from: After the password is entered, an extra code / data is sent to the guest's registered device / phone / email (account) ... the code must also be entered (to complete the log-in) The hacker would also need access to the guest's device / email to get the code So finding the password by brute force is not enough to get into the account	**2**	max 2. Do not accept "the guest has to log in twice" alone. Accept "two-factor authentication".
4(c) 0478 5.3.2	Any two from: A fingerprint is unique to the guest / to each person It cannot be found by trying combinations of characters // there is no password to try It is very difficult to copy / fake // the hacker would need the guest's actual finger / biometric data So a brute-force attack (on the app log-in) cannot succeed / is not possible	**2**	max 2. Do not accept "biometrics are more secure" alone.
5(a) 0478 5.3.1	One mark for each correct word, in order: trial and error combination software	**3**	Words must be in the correct gaps. Accept "combinations" for gap 2.

Total: 20 marks

MODULE G SECURITY · G4

DDoS attacks: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (describe the processes involved in, and the aim of carrying out, a range of cyber security threats, including a distributed denial of service (DDoS) attack)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	To stop genuine users from accessing a website or server	**1**	More than one tick = 0.
1(b) 0478 5.3.1	The attack / requests come from many computers / devices (at the same time) // from many different places / sources // from a botnet	**1**	Do not accept "it is spread out" / "it is shared" alone. Do not accept "it attacks many servers".
1(c) 0478 5.3.1	Very large number of requests at the same time: True Owners usually know their computers are used: False Usual aim is to copy the data on the server: False	**3**	One mark per correct row. A row with both boxes ticked scores 0.
2(a) 0478 5.3.1	Correct order: A 1, **E 2**, **C 3**, **F 4**, **B 5**, **D 6** One mark for each of E, C, F, B, D with the correct number (max 4)	**4**	max 4: all five correct = 4. A number used twice: mark neither statement with that number.
3(a) 0478 5.3.1	Any three from: Many computers / bots (in a botnet) send requests to the web server A (very) large number of requests is sent at the same time The web server cannot handle / respond to all the requests // is overloaded / flooded The web server slows down / fails / crashes / times out The customers' (genuine) requests cannot reach the web server // are not answered	**3**	max 3. Do not credit "the customers' computers are infected" / "the data is stolen" / "the website is hacked" alone.
3(b) 0478 5.3.1	To get money from the company // to demand a ransom // extortion / blackmail	**1**	Do not accept "to steal money" / "to steal data".
3(c) 0478 5.3.1	Any two from: To disrupt the company // stop its service being used To make the company lose money / sales To damage the company's reputation Revenge // a grudge against the company As a protest // to make a political point For entertainment // for fun // to show they can As a distraction while another attack takes place To help a competitor To test how well a system copes with heavy traffic // to test its resilience	**2**	max 2. Credit any other valid aim. Do not credit demanding money / ransom again (it is the aim in (b)). Do not accept "to steal data" alone.

QUESTION	ANSWER	MARKS	GUIDANCE
4(a) 0478 5.3.1	Any two from: The requests come from many (different) computers / bots Each computer / bot has a different IP address // there are many IP addresses The other bots keep sending requests // blocking one removes only a very small part of the traffic The web server is still overloaded (by the requests from the other bots) The attack traffic is hard to tell apart from genuine users' requests	**2**	max 2. Do not accept "the attacker is too clever" / "the attack is too strong" alone.
5(a) 0478 5.3.1	Any three from: The bots are (usually) other people's computers, not the company's own computers The bots / botnet can be anywhere (in the world) // outside the company The attack works by sending (large numbers of) requests to the web server (over the internet) The web server does not need to be infected with malware for the attack to work Anti-malware on the office computers cannot stop the requests being sent // reaching the web server Any web server that is connected to the internet can be a target	**3**	max 3. Do not credit "anti-malware does not work" / "anti-malware can be out of date" (the stem says it is up to date) without a point about how the attack works.

Total: 20 marks

MODULE G SECURITY · G5

Hacking and data interception: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.1 (processes involved in, and aim of, data interception and hacking), 5.3.2 (solutions that keep data safe) and 2.3.1 (purpose of encryption when transmitting data)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. The term "packet sniffer" is credited but never required. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1 0478 5.3.1	One mark for each correct row: Captured while being transmitted: Data interception Gains access without the owner's permission: Hacking Aim can be to steal personal data such as passwords: Both Can delete or change stored files: Hacking	**4**	A row with more than one box ticked scores 0.
2(a) 0478 5.3.1	Any four from: Data is sent across the network in packets Wireless signals can be picked up by any device within range (of the hotel network) The attacker uses a packet sniffer // software/hardware that captures/copies packets The packets are intercepted/captured/copied while they are being transmitted // in transit The captured packets are sent to / stored on the attacker's device The attacker examines/analyses the contents of the packets ... to find useful data, e.g. login details / payment details The data still reaches the booking website // the interception can go unnoticed If the data is not encrypted, the attacker can understand it	**4**	max 4. Do not credit "hacks the network" / "steals the data" alone. Do not credit descriptions of other threats (e.g. flooding the network, redirecting to a fake website).
2(b) 0478 5.3.1	Any two from: To steal login details / username and password // to use them to access the guest's account To steal payment / bank / card details // to commit fraud / take money To steal personal data // to commit identity theft To sell the data (to other criminals) To blackmail the guest To monitor / spy on the guest's communications	**2**	max 2. Do not credit "to steal data" alone. Do not award two aims that are the same point (e.g. bank details and card details).
2(c) 0478 2.3.1	Any two from: Encryption does not stop/prevent the data being intercepted // the data can still be captured (But) the intercepted data cannot be understood // is meaningless without the (decryption) key The data is sent as ciphertext // it has been scrambled, so the person who intercepts it only gets ciphertext	**2**	max 2. Do not credit "the data cannot be read" alone (it can be captured and read as ciphertext; it cannot be understood). Do not credit answers saying encryption stops the data being intercepted or stolen.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.1	Any two from: Gaining access to a computer system / network / data ... ... that is unauthorised // without the owner's permission (Often) by finding / exploiting weaknesses in security // by getting round security measures // using stolen or guessed login details	**2**	max 2. The second point builds on the first. "Gaining unauthorised access to a computer system" scores both of the first two points. "Breaking into a computer" alone scores 1.
3(b) 0478 5.3.1	Any three from: Steal data, e.g. building designs / client records Delete data Change / corrupt data Install malware (e.g. ransomware / spyware) on the server Sell / leak the data // blackmail the firm Use the server to carry out further attacks // to access other computers on the network Spy on / monitor the firm's activity Damage the firm's reputation // disrupt its work	**3**	max 3. Accept "steal designs to give to a rival firm". "Delete or change data" written as one point scores 1. Do not credit "to hack the server" or "to cause damage" alone.
3(c) 0478 5.3.2	One mark for each solution and one mark for its matching explanation (max 2 solutions): Firewall (1) ... monitors traffic between the server / network and the internet and blocks unauthorised traffic / connections that break its rules (1) Access levels (1) ... each user can only access the files they need, so a hacker using one account cannot reach / change all the data (1) Authentication using a (strong) username and password (1) ... only users who enter the correct details can access the server // a strong password is hard to guess (1) Biometrics (1) ... access needs a unique physical feature, e.g. a fingerprint, which a hacker cannot easily copy / guess (1) Two-step verification (1) ... a one-time code is sent to the member of staff's phone / email, so a stolen password alone is not enough to access the server (1) Automating software updates (1) ... security weaknesses that hackers could exploit are fixed as soon as patches are released (1) Proxy server (1) ... sits between the network and the internet and filters / blocks unwanted traffic // hides the IP addresses of devices on the network (1) Anti-malware (1) ... detects and removes malware, e.g. spyware / a Trojan horse, that could give a hacker access (1)	**4**	max 4. The explanation mark must match the solution given. Two different solutions are needed: username and password, biometrics and two-step verification may each count as a separate solution. Do not credit "makes it more secure" alone.

Total: 21 marks

MODULE G SECURITY · G7

Firewalls, anti-malware and updates: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.2 (explain how a range of solutions are used to help keep data safe from security threats: anti-malware, including anti-virus and anti-spyware; automating software updates; firewalls)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. **...** at the start of a point means it builds on the point before. Credit any other valid answer that shows the same understanding. Access levels, authentication, proxy-servers, privacy settings, SSL and checking URLs / communications (also 5.3.2) are tested in other Module G worksheets, not here.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.2	Installs patches as soon as they are released: Automating software updates Checks traffic between a network and the internet against rules: Firewall Finds and removes software that records key presses: Anti-spyware Scans files and compares them with known viruses: Anti-virus	**4**	One mark per correct row. A row with more than one tick scores 0.
2(a) 0478 5.3.2	Any three from: Monitors / examines (all) the traffic coming into (and going out of) the network Checks whether the traffic meets the rules / criteria (set by the network manager) Blocks / rejects traffic that does not meet the rules // traffic from a blacklisted / unknown source Allows traffic that meets the rules // traffic from a whitelisted / trusted source Can block traffic from hackers // unauthorised access to the server // traffic that may carry malware Can keep a log of (blocked) traffic // alert the network manager	**3**	max 3. "Stops hackers" alone is too vague: it must be linked to blocking traffic. Do not credit scanning files for viruses (that is anti-virus).
2(b) 0478 5.3.2	Any two from: Block traffic from a particular / suspicious IP address // set a blacklist of IP addresses Only allow traffic from trusted / known IP addresses // set a whitelist Block access to particular websites / URLs Block particular ports // types of traffic // applications from using the network Block incoming traffic that was not requested by a computer on the network Block traffic at certain times // outside office hours	**2**	max 2. The same rule given twice in different words scores 1. "Block bad / dangerous traffic" alone is too vague.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.2	Any three from: Scans the computer system / files (for viruses) Has a record / database of known viruses // compares files with known viruses Checks files / data before they are downloaded / opened // scans in real time ... and stops the download // warns the user the file may contain a virus Quarantines / removes / deletes any virus found ... so the virus cannot replicate / spread // delete or corrupt the firm's data Can run scheduled / regular scans	**3**	max 3. "Gets rid of viruses" alone scores 1 (removes any virus found) only.
3(b) 0478 5.3.2	Any one from: Scans the computer for spyware Removes / quarantines any spyware that is found Stops spyware being downloaded / installed Stops spyware recording key presses // sending the financial details to a third party	**1**	Do not credit answers about viruses only, or "stops hacking".
3(c) 0478 5.3.2	Any two from: New malware / viruses / spyware are created all the time ... the update adds them to the record / database of known malware ... otherwise new malware would not be detected / removed // could infect the computers Updates can fix weaknesses / bugs in the anti-malware software itself	**2**	max 2. "To keep it up to date" alone is too vague.
4(a) 0478 5.3.2	Any three from: Updates contain patches // fix bugs / security weaknesses / vulnerabilities in the software ... that hackers / malware could use to gain access to the computers / data Automatic updates are installed as soon as they are released ... so the computers are open to attack for less time Does not rely on staff remembering / choosing to install updates // staff cannot delay or ignore them All computers are kept up to date (with the latest version) Anti-malware updates are also installed automatically // new malware can be detected straight away	**3**	max 3. "Keeps the software up to date" alone scores 0 unless linked to fixing weaknesses or speed of installation. Do not credit "updates stop all attacks".

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) 0478 5.3.2	Any three from: A firewall only checks / filters the traffic between the network and the internet A firewall does not scan the files stored on the computers A firewall does not remove / quarantine malware (already on a computer) Malware can arrive in traffic that the firewall allows // in an email attachment / download from an allowed source Malware can arrive without going through the firewall // e.g. on a USB memory stick / external storage Anti-malware scans files and compares them with known malware // detects and removes malware the firewall misses The two solutions work together // give more than one layer of protection	**3**	max 3. "A firewall cannot stop viruses" alone is too vague.

Total: 21 marks

MODULE G SECURITY · G8

Access levels and authentication: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.2 (access levels; authentication: username and password, biometrics, two-step verification)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. 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. Accept "two-factor authentication" for two-step verification.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.2	One-time code sent to registered phone / email: Two-step verification Physical feature scanned: Biometrics Secret string of characters typed: Username and password Data unique to the user's body compared with stored data: Biometrics	**4**	One mark per correct row. More than one tick in a row: 0 for that row.
2(a) 0478 5.3.2	One mark for allow, one mark for not allow: Allow: view / book / change appointments // view / edit owners' contact details // view a list of animals booked in Not allow: view / edit animals' treatment / medical records // delete records // change other users' access levels / system settings // view staff / financial / pay data // install software	**2**	Allow must fit the receptionist's job in the stem. "Not allow" must be something a receptionist would not need. Credit any other reasonable answer.
2(b) 0478 5.3.2	Any two from: The hacker can only access what the receptionist's access level allows ... so the hacker cannot see / change / delete data the receptionist cannot // e.g. medical / treatment records ... so the hacker cannot change access levels / settings // cannot give themselves more access Less data can be stolen / changed / deleted // limits the damage	**2**	max 2. "Stops the hacker logging in" = 0 (the hacker has already logged in).
3(a) 0478 5.3.2	Any two from: Make it longer // use more characters Add upper-case / capital letters Add symbols / special characters // e.g. ! # @ Do not use a (dictionary) word / name / the pet's name Do not use personal information // e.g. a pet's name or a year that others may know Use a random mix of characters // a random string / unrelated words	**2**	max 2. Do not accept "add numbers" (it already has numbers). Do not accept "change it regularly" (it does not make this password stronger). A correct example of a stronger password with no stated change: max 1.

QUESTION	ANSWER	MARKS	GUIDANCE
3(b) 0478 5.3.2 (threat 5.3.1)	Any two from: A brute-force attack tries every / many possible combinations (of characters) // tries common words / passwords first A strong password has many more possible combinations ... so it would take (far) too long to find // is very difficult to guess ... so the hacker is less likely to access the account / data Not a (dictionary) word, so it is not found by trying common words / passwords Limiting the number of login attempts stops the hacker trying many combinations	**2**	max 2. "More secure" / "harder to hack" alone is too vague.
4(a) 0478 5.3.2	Any two from: The vet places their finger on the scanner // the fingerprint is scanned The scan is compared with the vet's fingerprint data stored (earlier) on the system If they match, the vet is given access // is logged in If they do not match, access is refused	**2**	max 2.
4(b) 0478 5.3.2	Any two from: A fingerprint is unique to each person ... so it is very difficult to copy / fake // a hacker would need the vet's biometric data It cannot be guessed // cannot be found by a brute-force attack It cannot be forgotten / written down / shared (like a password) The vet must be physically present to log in // it cannot be used from a remote location It cannot be seen by someone watching (as a typed password can) // cannot be given away in a phishing attack	**2**	max 2. Do not accept "it cannot be hacked" or "it is impossible to fake".
5(a) 0478 5.3.2	Any three from: The manager first enters their username and password The system then sends a (one-time) code to the manager's registered / pre-set phone / email // an app on the registered device shows a code The manager enters the code into the system / login page Access is only given if the password and the code are both correct The code can only be used once // expires after a short time	**3**	max 3. Accept a request on the registered device that the manager approves in place of typing a code.

QUESTION	ANSWER	MARKS	GUIDANCE
5(b) 0478 5.3.2 (threat 5.3.1)	Any two from: The hacker also needs the code // the password alone is not enough to log in The code is sent to the manager's registered device / email, which the hacker does not have The code is one-time / expires, so a code seen earlier cannot be reused The manager receives a code they did not ask for // is alerted that someone is trying to log in (and can change the password)	**2**	max 2. Do not accept "the hacker cannot get the password" (the password has been stolen).

Total: 21 marks

MODULE G SECURITY · G10

Staying safe online: SSL, proxy servers, privacy settings and checking messages: mark scheme

22 marks · Cambridge 0478 syllabus 5.3.2 (how a range of solutions are used to help keep data safe from security threats)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. A point starting with **...** builds on the point before it. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.2	One mark for each correct row: Requests and responses pass through it: Proxy server Security protocol that encrypts data between browser and server: SSL Lets a user choose who can see their profile and posts: Privacy settings Can stop websites seeing the device's IP address: Proxy server	**4**	A row with more than one tick scores 0.
2(a) 0478 5.3.2	One mark for each step in the correct position: 2: The web server sends a copy of its SSL certificate to the web browser 3: The web browser checks that the SSL certificate is authentic 4: The web browser sends a message to the web server to say that communication can begin 5: The web server acknowledges the message and the SSL-encrypted session begins	**4**	Order in the table, top to bottom: 2, 5, 1, 3, 4.
2(b) 0478 5.3.2	Any two from: SSL encrypts the data // the password is sent as ciphertext ... so the intercepted data / password is meaningless // cannot be understood (by the criminal) ... without the (decryption) key // only the web server can decrypt it	**2**	max 2. Do not accept "the data cannot be intercepted" or "SSL stops the data being stolen". "Cannot be read" alone is not enough; "cannot be read / understood without the key" is creditworthy. Accept TLS for SSL.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.2	Any four from, max two per way: Web requests are sent by the proxy server on behalf of the office computers ... ... so websites / the internet only see the proxy server's IP address // the IP addresses of the office computers are hidden ... so attackers / hackers cannot easily find / target the office computers directly // the internal network is hidden The proxy server filters / checks requests and responses (against rules) ... ... and blocks access to (known) harmful / fake / unsuitable websites ... so staff are less likely to download malware // reach a phishing / fake website and give away data The proxy server can block suspicious / unauthorised incoming traffic // helps stop hacking (attempts) Attacks (such as a DDoS attack) are aimed at / reach the proxy server instead of the museum's network / computers	**4**	max 4. Credit two separate ways, each with its explanation. Do not accept "makes the network faster" or "stores web pages in a cache" as a way of keeping data safe. Do not accept "more secure" / "safer" alone, or "stops all attacks".
4(a) 0478 5.3.2	Any three from: Spelling / grammar mistakes, e.g. "acount", "Costumer", "you're", "Securty" Generic / impersonal greeting // does not use the customer's name, e.g. "Dear Valued Costumer" Urgent tone // pressure to act quickly, e.g. "URGENT", "NOW", "24 hours", "today" Threatening tone, e.g. account "closed permanently" // "legal action" Asks for personal / sensitive details, e.g. the full password / card number Uses capital letters to alarm / shout, e.g. "URGENT", "NOW"	**3**	max 3. Max 1 for spelling / grammar mistakes, however many are listed. Max 1 for urgency, however many examples are given. Credit any other valid sign of a phishing message.
4(b) 0478 5.3.2	Any two from: The link uses http not https // the link is not secure / does not use SSL The domain name is misspelt // "fernbr0ok" uses a zero instead of the letter o The link has extra words / "-verify" in the domain name // the domain name is different from the genuine domain name	**2**	max 2. A difference must be in the URL. Do not accept "it is a fake link" alone. Ignore the "/login" page name (a genuine site can have a login page).

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) 0478 5.3.2	Any three from: Privacy settings control who can see the profile / posts / personal data ... e.g. set the account to private // friends / followers only ... so strangers / criminals / hackers cannot see the date of birth / home town / pet's name ... so there is less personal data that could be used to guess passwords / security answers // for identity theft ... so there is less data for social engineering // to write convincing phishing messages Location (sharing) can be turned off // posts no longer show where they were posted ... so criminals cannot tell where the dog groomer is / lives / works Can limit who can contact / message / tag the dog groomer	**3**	max 3. Do not accept "stops hacking" / "makes the account secure" / "safer" alone. Accept "hides" for "stops people seeing".

Total: 22 marks