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