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