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.

QUESTION	ANSWER	MARKS	GUIDANCE
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.
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".

QUESTION	ANSWER	MARKS	GUIDANCE
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