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