MODULE G SECURITY · G1

Malware: mark scheme

21 marks · OCR J277 spec 1.4.1 (forms of attack: malware; how the attack is used; the purpose of the attack)

How to use. One mark per bullet up to the maximum shown. **/** separates alternatives; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. J277 does not name types of malware, so students do not need to name them; where a correct type (e.g. virus, worm, Trojan, spyware, ransomware) is used accurately, accept it. Ways to prevent malware are tested in G7.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) J277 1.4.1	(Malicious) software / a program designed to harm / damage / disrupt a computer (system) // to gain unauthorised access to a computer (system) / data	**1**	Must be software / a program with a harmful purpose. Do not accept "a virus" alone (an example, not a meaning). Do not accept "bad software" alone (NE).
1(b) J277 1.4.1	(Opening) an email attachment Clicking a link (in an email / message / on a website) Downloading / installing software / files (from the internet / an untrusted source) Removable media // USB memory stick / external drive Spreading across a network (from another infected computer) Through a weakness / vulnerability in software that has not been updated / patched Hidden inside / disguised as software that seems legitimate Installed by a hacker who has gained access (e.g. after a brute-force or social engineering attack)	**2**	1 mark each to max 2. Credit any other valid way. Do not award two marks for the same way written twice (e.g. "from the internet" and "from a website" with no further detail = 1 mark). "The internet" alone is NE.
2(a) J277 1.4.1	Records key presses and sends them: Steal data Locks files and demands payment: Extort money Overwrites documents: Delete or corrupt data Runs commands from another location: Take control of the device	**4**	1 mark per correct row. A row with two or more ticks scores 0.
3(a) J277 1.4.1	Spread on a USB memory stick: True Only by downloading from a website: False Some malware copies itself across a network without user action: True Always shows a warning: False	**4**	1 mark per correct row. A row with both boxes ticked scores 0.

QUESTION	ANSWER	MARKS	GUIDANCE
4(a) J277 1.4.1	The program appears to be legitimate / genuine / useful // the malware is disguised (as a useful program) ... the program does what it claims / converts files as expected (so nothing seems wrong) The malware runs secretly / hidden / in the background ... with no message / warning // nothing visible on screen The employee chose to install the program (so did not suspect it)	**2**	1 mark per bullet to max 2. Accept a correct reference to a Trojan (horse). Do not accept "the malware is invisible" alone (NE) unless linked to running in the background / with no sign.

4(b)
J277 1.4.1
	The data includes usernames / passwords / log-in details (typed by the employee)
	... the attacker can log in to the firm's systems / email / accounts (as the employee) // gain unauthorised access
	Access / steal / copy confidential client data / clients' financial records
	Bank / card details could be captured // money could be stolen / transferred (from the firm or clients)
	Data could be sold (to other criminals) // used for identity theft / fraud
	The attacker could change / delete the firm's data
	The attacker could install further malware (once logged in)
	The attacker could blackmail the firm / clients (by threatening to release data)
	Messages typed (e.g. emails) could be read // confidential business information revealed
		3	1 mark per bullet to max 3. Credit any other valid harm that follows from the recorded data. Do not accept "hack them" / "steal things" alone (NE).

5(a) J277 1.4.1	To extort money // to make the practice pay (a ransom / fee) (to unlock the files)	**1**	Accept "to get money (from the practice)". Do not accept "to lock the files" alone (that is how, not why). Accept ransomware named with the purpose.

QUESTION	ANSWER	MARKS	GUIDANCE
5(b) J277 1.4.1	Staff cannot access appointment / animal / client records / bookings ... ... so the practice cannot treat animals / take bookings / work normally // the practice may have to close (for a time) The practice may lose income / money (while it cannot work) ... ... and it costs time / money to restore the files / systems (e.g. from a backup) The practice may pay the ransom ... ... but there is no guarantee the files will be unlocked // it could lose the money and the data Data may be permanently lost (if the files are never unlocked) ... ... so medical histories / treatment records are no longer available Client data may have been copied / stolen / leaked ... ... so the practice's reputation is damaged // clients lose trust / go to another practice	**4**	Mark in pairs: 1 mark for an effect, 1 mark for the linked expansion (...), max 2 per way, max 4. The second way must be different from the first. Do not accept "it is bad for the business" alone (NE). Credit any other valid effect with an expansion.

Total: 21 marks