MODULE G SECURITY · G2

Social engineering, phishing and pharming: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (the processes involved in, and the aim of, social engineering, phishing and pharming)

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. Credit any other valid answer that shows the same understanding. Solutions such as checking the URL or the spelling and tone of a message (0478 5.3.2) are tested in G10.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	B	**1**	More than one box ticked scores 0.
2(a) 0478 5.3.1	Email that appears to come from the bank: Phishing Sent to a fake website after typing the correct address: Pharming Replies to a fake message with their password: Phishing Can work without the attacker sending any message: Pharming	**4**	One mark per correct row. A row with both boxes ticked scores 0.
3(a) 0478 5.3.1	Any three from: The customer clicks a link / opens an attachment that downloads the malicious code (onto their computer) Malicious code / malware is installed on the customer's computer // malicious code is stored on a DNS server / web server The (malicious) code changes / alters the IP address linked to the web address / URL // changes the DNS entry / record When the customer types the (correct) URL ... ... the request is redirected to the fake website (instead of the real one) The fake website looks like the real one // the customer does not know they have been redirected	**3**	max 3. Do not credit a link in an email taking the customer straight to the fake website (that is phishing): the customers typed the correct address. Credit clicking a link or attachment only when it installs the malicious code. Accept "the code redirects the browser / user to the fake website" for MP5.
3(b) 0478 5.3.1	Any two from: To obtain / collect / harvest the customers' card / bank / personal details ... that are entered into the fake website ... to use them for fraud // to steal money // to make purchases with the card ... for identity theft // to sell the details (to other criminals)	**2**	max 2. Do not accept "to hack the company" alone. Do not accept "to crash / slow down the website".

QUESTION	ANSWER	MARKS	GUIDANCE
4(a) 0478 5.3.1	Any two from: Pretends to be someone trusted / in authority // pretends to be from IT support Creates urgency // gives a short time limit (ten minutes / "straight away") Uses fear / a threat // says the account will be locked Does not give the receptionist time to check (who is calling)	**2**	max 2. Two answers that make the same point (e.g. "ten minutes" and "straight away") score 1.
4(b) 0478 5.3.1	Any one from: To obtain the receptionist's password // log-in details To gain (unauthorised) access to the receptionist's account / the firm's computer system / the firm's data	**1**	Do not accept "to hack" alone.
4(c) 0478 5.3.1	One mark for a method, one mark for how it gains access, e.g. Shoulder surfing // watching someone type their password ... ... and then using the password to log in Leaving a USB drive (containing malware) where an employee will find it ... ... when it is plugged in, the malware is installed / gives the attacker access // records / sends passwords to the attacker Pretending in person to be a technician / visitor / new employee ... ... to be let into the building / to be given a password / to be logged in to a computer Sending a fake text / social media message pretending to be a trusted person ... ... asking for log-in details // linking to a fake log-in page	**2**	max 2. Second mark must follow from a valid method. Mark the first method only. A phone call or an email scores 0 (excluded by the question). Do not credit brute-force or other non-social-engineering attacks.
5(a) 0478 5.3.1	Any three from: The message appears to come from a trusted source / the bank It creates urgency / fear (an unusual payment) so the user acts quickly The user taps / clicks the link ... ... which takes them to a fake website (that looks like the bank's) The user enters their bank / log-in / card details The details are sent to / collected by the attacker // the attacker uses the details for fraud / to access the account	**3**	max 3. Accept "the link downloads malware that steals the details" as an alternative for MP4 + MP5 (max 2 for this route). Do not credit a description of pharming (redirection after typing a correct URL).

QUESTION	ANSWER	MARKS	GUIDANCE
5(b) 0478 5.3.1	Any two from: Phishing needs the user to click / tap a link / respond to a message ... ... whereas pharming redirects the user even when they type the correct URL Phishing sends a fake message / email to the user ... ... whereas pharming uses malicious code on the user's computer / a DNS server With pharming the user may not have received any message from the attacker	**2**	max 2. A difference must be clear. 1 mark for a correct statement about one attack only; 2 marks need the comparison with the other. Do not accept "pharming is more dangerous" alone.

Total: 20 marks