MODULE G SECURITY · G2

# Social engineering and phishing: mark scheme

20 marks · OCR J277 spec 1.4.1 (forms of attack: social engineering, e.g. phishing, people as the 'weak point'; how the attack is used; the purpose of the attack)

**How to use.** One mark per bullet up to the maximum shown. **/** separates alternative words; **//** separates alternative answers for the same mark. Words in (brackets) are not needed for the mark. **NE** = not enough. Credit any other valid answer that shows the same understanding. Prevention methods are tested in G7 to G9 and are not needed here.

| QUESTION | ANSWER | MARKS | GUIDANCE |
|---|---|---|---|
| **1(a)** J277 1.4.1 | Manipulating / tricking / deceiving people into giving away confidential / personal information (e.g. passwords) // into giving access (to a system) // into doing something that breaks security | **1** | Must refer to people / users being tricked. Do not accept "hacking" or "stealing data" alone (NE). An example alone (e.g. "phishing") is NE. |
| **1(b)** J277 1.4.1 | People can be tricked / manipulated // people trust others / act on fear or urgency<br>People make mistakes // are careless, e.g. reuse or write down passwords // click links / open attachments without checking<br>People can give away passwords / details / access (willingly)<br>... so attackers can get past technical security (e.g. strong passwords, security software) without breaking it<br>It is often easier (for an attacker) to trick a person than to attack the technology / system | **2** | Max 2. Accept examples that make the point, e.g. "an employee might tell a caller their password". Do not accept "people are not secure" alone (NE). |
| **2(a)** J277 1.4.1 | Caller pretending to be IT support: Social engineering<br>Software trying thousands of passwords: Not social engineering<br>Watching someone type a password: Social engineering<br>Server flooded with requests: Not social engineering | **4** | One mark per correct row. A row with both boxes ticked scores 0. Row 2 is a brute-force attack; row 3 is shoulder surfing; row 4 is a denial of service attack. |
| **3(a)** J277 1.4.1 | It pretends to come from a trusted / familiar source // the payroll team<br>It creates urgency // gives a time limit (24 hours)<br>It uses fear / a threat // says the salary payment will be cancelled<br>It makes responding easy // gives a button / link to click<br>It looks official // uses an official-sounding subject line / "URGENT" | **2** | 1 mark each to max 2. Mark the first answer on each line. Do not accept two answers that make the same point (e.g. "24 hours" and "urgent" = 1 mark). A generic greeting ("Dear staff member") or the odd sender address is a sign of phishing, not a way of persuading: do not credit. |

| QUESTION | ANSWER | MARKS | GUIDANCE |
|---|---|---|---|
| **3(b)**<br>J277 1.4.1 | The employee clicks the button / link (in the email)<br>... which takes them to a fake website / log-in page<br>... that looks like the real (payroll) site<br>The employee enters their username / password / log-in details<br>The details are sent to / captured / recorded by the attacker<br>The attacker uses the details to log in to the (real) account | **3** | Max 3. Accept "replies with their log-in details" for MP4 + MP5 (1 mark each). Do not credit answers that describe a different attack, e.g. guessing every password. |
| **3(c)**<br>J277 1.4.1 | Steal / view personal data (e.g. address, bank details) // the firm's confidential data<br>Change the bank details so the salary is paid to the attacker // commit fraud / steal money<br>Use the details for identity theft<br>Sell the details (to other criminals)<br>Change / delete data<br>Install malware // get into the firm's network (for further attacks)<br>Send more phishing emails from the employee's account | **2** | 1 mark each to max 2. Mark the first two answers. Two answers that make the same point score 1. Do not accept "hack them" alone (NE). |
| **4(a)**<br>J277 1.4.1 | The attack targets the person / receptionist, not the computer / technology // people are the weak point<br>The receptionist may give the password willingly // is tricked into trusting the caller<br>The attacker would then log in with the correct username and password<br>... so the log-in looks genuine / the security software has nothing to detect // no malware / technical weakness is needed | **2** | Max 2. Do not accept "security software does not work" or "the software is not good enough" (NE / wrong). |
| **4(b)**<br>J277 1.4.1 | 1 mark for a method, 1 mark for how it gets the password, e.g.<br>Shoulder surfing // watching someone enter their password ...<br>... then remembering / recording it to log in later<br>Pretending in person to be a technician / visitor / new member of staff ...<br>... and asking a member of staff for their password / to log in for them<br>Leaving an infected USB drive where staff will find it ...<br>... when plugged in, malware (e.g. spyware) records the password // sends it to the attacker<br>A fake message on social media / a text message (e.g. from a fake colleague) ...<br>... asking for the password // linking to a fake log-in page | **2** | Mark in pairs: the second mark depends on a valid method. Mark the first method only. Any email (including a phishing email) or a phone call scores 0 (excluded by the question). Credit any other valid social engineering method. Brute force / guessing is not social engineering: 0. |

| QUESTION | ANSWER | MARKS | GUIDANCE |
|---|---|---|---|
| **5(a)**<br>J277 1.4.1 | The attachment contains / is malware (e.g. a virus, trojan, spyware, ransomware)<br>Opening it runs / installs the malware (on the computer)<br>... which could delete / corrupt / encrypt files // steal data / passwords // give the attacker control of the computer // spread to other computers | **2** | Max 2. Do not accept "it gives the computer a virus" alone for 2 marks (1 mark for MP1). Do not accept "it slows the computer" alone (NE). |

**Total: 20 marks**