**Q1.**

The table below shows screenshots of three different security measures.

Tick the box next to the CAPTCHA screenshot.

|  |  |
| --- | --- |
| **Security measure** | **Tick one box** |
|  |  |
|  |  |
|  |  |

**(Total 1 mark)**

**Q2.**

Give **three** examples of when it would be suitable to use a CAPTCHA system.

1.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 3 marks)**

**Q3.**

Define the term ‘cyber security’.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 2 marks)**

**Q4.**

Define the term ‘malware’.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 2 marks)**

**Q5.**

Shade the **two** lozenges that are examples of social engineering.

|  |  |  |
| --- | --- | --- |
| **A** | Blagging |  |
| **B** | Blogging |  |
| **C** | Faking |  |
| **D** | Phishing |  |
| **E** | Porting |  |
| **F** | Smashing |  |

**(Total 2 marks)**

**Q6.**

Explain how **each** of the following cyber security threats could be used by a student to gain unauthorised access to a school network:

•   weak and default passwords

•   misconfigured access rights

•   removable media

•   unpatched and/or outdated software.

In your answer you should also describe some possible consequences of these threats.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 8 marks)**

**Q7.**

Shade **one** lozenge to show which statement best describes the definition of the term ‘social engineering’.

|  |  |  |
| --- | --- | --- |
| **A** | The art of hacking a network to access confidential information. |  |
| **B** | The art of hacking a network to access public information. |  |
| **C** | The art of manipulating people so they give up confidential information. |  |
| **D** | The art of manipulating people so they give up public information. |  |

**(Total 1 mark)**

**Q8.**

Phishing is a form of social engineering.

Describe **two** methods a school could use to protect its staff and students from phishing.

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 4 marks)**

**Q9.**

A company has decided to move its business online but it is concerned about making sure that only authorised users can gain access to the system. The company has set up a CAPTCHA system to check that the user is not a robot.

Explain **three** different electronic methods that could then be used to confirm user identity.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 6 marks)**

**Q10.**

Penetration testing can be conducted as either black-box or white-box testing.

Explain the difference between these two types of penetration testing.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 4 marks)**

**Q11.**

A virus is a specific category of malware.

Describe **three** other different categories of malware.

Malware 1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Malware 2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Malware 3 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 6 marks)**

**Q12.**

Most schools have a computer network.

Some schools allow teachers to access the school network from their home computers.

Give **one** reason why some schools allow this and **one** reason why some schools do not allow this.

Reason for: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Reason against: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 2 marks)**

**Q13.**

Social engineering is where someone is tricked or manipulated into providing secure information or access to a secure system. Describe each of the following social engineering techniques.

**Blagging:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Phishing:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Shouldering:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 3 marks)**

**Q14.**

A games café is evaluating the security for their network.

(a)  State **two** reasons why using a biometric authentication measure is better than password authentication for staff accounts.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(2)**

(b)  Explain why it would not be appropriate for the café to use MAC address filtering on their wireless network.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(2)**

**(Total 4 marks)**

**Q15.**

Social engineering is where someone is tricked or manipulated into providing secure information or access to a secure system. Describe each of the following social engineering techniques.

**Blagging**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Phishing**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Shouldering (or shoulder surfing)**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(Total 3 marks)**

**Q16.**

AQATravel is a tour operator that sells holidays to places all around the world. They hold all of their customer and business data electronically. Following recent news articles about the effects of malware attacks on businesses, the management of AQATravel have been investigating how they could protect themselves against malware attacks.

Discuss four methods that AQATravel could use to prevent infections from malware and/or to minimise the damage that could be caused by malware.

**(Total 12 marks)**

**Q17.**

The algorithm below, expressed in pseudo-code, allows three users to log in to a computer program with individual usernames and passwords.

•        For this algorithm, array indexing starts at 0.

•        Line numbers are included, but are not part of the algorithm.

**01**   userlist ← [ 'Rachel', 'Sam', 'Tracey' ]

**02**   passlist ← [ '49Class', 'Smile', 'b1K3' ]

**03**    REPEAT

**04**      OUTPUT 'Enter Username'

**05**      username ← USERINPUT

**06**      OUTPUT 'Enter Password'

**07**      password ← USERINPUT

**08**      validlogin ← False

**09**      FOR usernum ← 0 TO 2

**10**         IF username = userlist[usernum]

**11**         AND password = passlist[usernum] THEN

**12**            validlogin ← True

**13**         ENDIF

**14**      ENDFOR

**15**   UNTIL validlogin = True

**16**   OUTPUT 'Login Successful'

The valid usernames and passwords are listed below.

|  |  |
| --- | --- |
| **Username** | **Password** |
| Rachel | 49Class |
| Sam | Smile |
| Tracey | b1K3 |

(a)     Shade in **one** lozenge in each row of the table below to indicate the most appropriate data type to use for each listed **Variable** from the algorithm, when the algorithm is implemented in a programming language.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Most appropriate data type (shade one lozenge per row)** | | | | |
| **Variable** | **Integer** | **Real** | **Boolean** | **Character** | **String** |
| password |  |  |  |  |  |
| validlogin |  |  |  |  |  |
| usernum |  |  |  |  |  |

**(3)**

(b)     It is suggested that line 09 of the algorithm is replaced with the following line:

FOR usernum ← 0 TO LEN(userlist)

The function LEN returns the number of items that are stored in the array that is passed to it as a parameter.

Explain why using the LEN function would make the algorithm more flexible and why the suggested replacement line would not work as it is.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(3)**

(c)     It is suggested that lines 08 to 14 of the algorithm are replaced with the following lines:

FOR usernum ← 0 TO 2

   IF username = userlist[usernum]

   AND password = passlist[usernum] THEN

      validlogin ← True

   ELSE

      validlogin ← False

   ENDIF

ENDFOR

Explain why making this replacement would mean that the algorithm no longer worked.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(3)**

(d)     State which of the three passwords listed in the table above is the least secure and explain why this is the case.

**Which password:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Why least secure:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**(2)**

**(Total 11 marks)**

**Q18.**

List **three** different measures that can be used to maintain the security of a computer system.

For each measure:

•        Outline what the measure is.

•        Explain what types of threat to cyber security it is effective against.

**(Total 9 marks)**

Mark schemes

**Q1.**

**Mark is for AO1 (understanding)**

****

**R.** If more than one box ticked.

**[1]**

**Q2.**

**3 marks for AO1 (understanding)**

1 mark for each of the following points (maximum of **three** marks):

•   account registration;

•   account access;

•   online voting systems;

•   ticket purchasing / transaction completion;

•   on pages where comments / reviews can be posted;

•   on parts of the website where fraudulent click-throughs may be possible;

**[3]**

**Q3.**

**2 marks for AO1 (recall)**

•   (the processes/practices/technologies/methods designed to) protect networks/computers/programs/data;

•   from attack/damage/threats/unauthorised access;

**[2]**

**Q4.**

**2 marks for AO1 (recall)**

•   (Malware is a blanket/umbrella term for) computer software/program/code;

•   with malicious/hostile/intrusive intent;

**[2]**

**Q5.**

**2 marks for AO1 (recall)**

**A** Blagging;

**D** Phishing;

**R.** If more than two lozenges are shaded.

**[2]**

**Q6.**

**8 marks for AO2 (apply)**

|  |  |  |
| --- | --- | --- |
| **Level** | **Description** | **Marks** |
| 4 | Responses at this level will contain a **thorough explanation** of how **all** of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent.  **More than one** consequence has been described. | 7-8 |
| 3 | Responses at this level will contain a **detailed explanation** of how **most** of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent.  **At least one** consequence has been described. | 5-6 |
| 2 | Responses at the upper end of the level will contain some **explanations** of how **most** of the threats could be exploited by a student. The response makes some reference to a school network. The response makes sense when read as a whole.  Responses at the lower end of the level will mostly contain **descriptions** of how **some** of the threats could be exploited by a student. The response might make some reference to a school network. The response makes some sense when read as a whole.  In this level students may not have referred to the consequences. | 3-4 |
| 1 | Responses at the upper end of the level will contain **descriptions** of **at least one** of the threats and/or consequences.  Responses at the lower end of the level will include a few **statements** related to one or more of the required threats/consequences. | 1-2 |
|  | **No creditworthy material** | 0 |

**Indicative Content**

The indicative content below is written in a generic manner for the benefit of examiners. Responses should be worded in the context of a school to gain the highest marks. For example reference to pupils using default passwords or them gaining access to staff-only areas through misconfigured access rights.

•   Weak and default passwords:

○   students could use brute force methods to crack passwords

○   weak admin passwords would allow students to gain admin level access

○   default passwords allow students to gain access without any effort

○   default passwords are published online so everyone knows them.

•   Misconfigured access rights:

○   allows students to access areas they are not supposed to

○   network admins might not know that secure areas had been breached as no-one has ‘broken in’

○   students could reconfigure network

○   students could create new user accounts to give themselves admin access.

•   Removable media:

○   could contain malware that allows students to gain access to network

○   could be used to steal data

○   could be used to allow students to take control of certain network processes (eg remote access systems).

•   Unpatched and/or outdated software:

○   could allow students to exploit known weakness/flaw

○   known weaknesses/flaws are published online

○   once in a student could install malware.

**[8]**

**Q7.**

**1 mark for AO1 (recall)**

**C** The art of manipulating people so they give up confidential information.

**R.** if more than one lozenge shaded.

**[1]**

**Q8.**

**4 marks for AO2 (apply)**

A **maximum of 4 marks** can be awarded.

**One mark** for each point and **one mark** for an expansion.

Answers that are too similar to each other must only be credited once.

Example responses include:

•   Train staff/students to be cautious of emails;

○   that come from unrecognised senders;

○   that ask you to confirm personal/financial information (over the Internet);

○   that make urgent requests for personal/financial information;

○   that are not personalised;

○   that try to upset you into acting quickly by threatening you with frightening information;

•   Train staff/students not to click on links/download files/open attachments (in emails); from unknown senders/sources;

•   Prevent students from being able to download; anything from the internet/email links;

•   Train staff/students to never enter personal information; in a pop-up screen;

•   Train staff/students not to copy web addresses (into a browser); from pop-ups;

•   Protect the school computers with a firewall/spam filters/anti-virus/anti-spyware software; and keep the software updated;

**[4]**

**Q9.**

**3 marks for AO1 (understanding) and 3 marks for AO2 (apply)**

2 marks per method, 1 mark for stating the method, 1 mark for an explanation.

•   Passwords; a set of characters that is only known by the person who is being authenticated//a set of characters that is entered and compared against a database / recorded version;

•   Biometric; measures such as fingerprint, facial, iris, voice-print that use the user’s physical features to prove who they are;

•   Email confirmation; sends an email which requires a valid email address and for the recipient to respond to prove the email and hence user is valid;

**A.** Other methods that are not in the specification that are appropriate should also be awarded marks. Examples such as 2 Factor Authentication (2FA), Authenticator Apps, security questions.

**[6]**

**Q10.**

**4 marks for AO1 (understanding)**

Maximum of 3 marks if only 1 type of testing.

**Black box testing:**

•   the tester does not know how the system operates;

•   the tester is acting as an external hacker;

•   requires a lot of investigation and guessing / brute-force to find issues;

•   may not test all of the system especially if you do not know it’s full functionality;

•   you are trying to discover and exploit the weak spots in the system;

**White box testing:**

•   the operation of the system is known;

•   the tester is simulating a malicious insider;

•   can be targeted to test specific vulnerabilities;

•   you know exactly what you are trying to test;

•   because you know what you are testing you should be able to test all possible scenarios;

**R.** Any direct opposites. Statements such as “Black box has no knowledge of how the system operates. White box has knowledge of how the system operates.” would be awarded only one mark.

**[4]**

**Q11.**

**3 marks for AO1 (recall), 3 marks for AO1 (understanding)**

1 mark each for stating, 1 mark each for describing.

•   Trojan (horse); a program which misleads the user into thinking it is another piece of software which, when run, executes another program;

•   Spyware; a program which records data such as usernames and passwords on a host system and forwards the information to a third party;

•   Adware; code embedded or attached to program files which will persistently show adverts (that attempt to generate revenue);

•   Worm; code which will run autonomously and replicates itself on a host system;

•   Ransomware; a program that encrypts user’s data to make it unreadable until they pay for the key;

•   Remote Access Tool (RAT); allows access to control and monitor a computer from a remote network location;

•   Rootkit; malware that has managed to gain ‘root’ admin privileges;

•   Bots / Zombies; a program installed on a computer that performs a job for the remote owner of the bot / zombie such as sending spam or sending web requests to perform a DOS or attacking a computer system;

•   Scareware; malware that tells you something is wrong with your system in an attempt to get you to make a purchase;

•   Keylogger; a program that monitors / records a user’s keystrokes in order to steal passwords / confidential details;

**R.** Specific named examples on their own, e.g. “Wannacry” would receive no marks, “Ransomware such as Wannacry” would receive 1 mark.

**R.** References to ‘virus’ as this is the example in the question.

**[6]**

**Q12.**

**All marks AO1 (understanding)**

**Reasons for allowing:**

Teachers can access resources on the school network to allow them to plan lessons at home;

Teachers can teach lessons from home (using videoconferencing) if they are not able to get into work (eg travel difficulties);

Teachers can access electronic copies of student work so that they do not have to carry marking home;

**Reasons for not allowing:**

Data protection issues – schools may not want potentially sensitive student information to be accessed outside of school;

To try to help teachers have a work-life balance;

Increased security risks as teachers may not have fully-protected computers at home (eg if a teacher does not have anti-virus software on their home computer this may cause problems when they connect their computer to the school network);

**Max 1 mark:** if only described reasons for allowing access

**Max 1 mark:** if only described reasons for not allowing access

**[2]**

**Q13.**

**3 marks for AO1 (understanding)**

1 mark each for describing the social engineering technique.

Blagging

This is where a victim is tricked/persuaded by a fraudster to give their details or payment information for a false reason/purpose;

Phishing

Is where the victim receives and responds to a communication that appears to be from a valid or known source but is in fact fraudulent. (It allows the fraudster to capture private information before the victim realises);

Shouldering

This is where someone watches and records\remembers a victim entering their pin or security information such as passwords. (They can then use this information to gain access to a system);

**[3]**

**Q14.**

(a)  **All marks AO2 (apply)**

Staff could forget their password // staff can’t forget biometric measure;

Shouldering risk when staff entering their password // no risk of shouldering when using biometric data;

Lower risk of hacking;

**Max 2**

**2**

(b)  **All marks AO2 (apply)**

Network is made available to members of the public;

Won’t know the MAC addresses for (most) of the devices connecting to the network;

**2**

**[4]**

**Q15.**

**3 marks for AO1 (understanding)**

1 mark each for describing the social engineering technique.

**Blagging (pretexting)**

This is where a victim is tricked / persuaded (by a fraudster) to give their details or payment information (for a fraudulent reason / purpose);

**Phishing**

Is where the victim receives and responds to a communication that appears to be from a valid or known source (but is in fact fraudulent. It allows the fraudster to capture private information before the victim realises);

**Shouldering (or shoulder surfing)**

This is where someone watches and records / remembers a victim entering their pin or security information such as passwords. (They can then use this information to gain access to a system);

**[3]**

**Q16.**

**4 marks for AO1 (understanding) and 8 marks for AO2 (apply)**

|  |  |  |
| --- | --- | --- |
| **Level** | **Description** | **Mark Range** |
| 4 | **Level 4 High mark range**  **Subject Criterion Context**  A **clear understanding** shown through the use of at least **four** relevant examples that **discuss** the methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection.  Examples are well supported by reasoned arguments and the detail given should explain how and why the methods\techniques would be in/effective. | 10-12 |
| 3 | **Level 3 Higher mid mark range**  **Subject Criterion Context**  A **more developed understanding** shown through the use of suitable examples that **discuss / explain** at **least three** methods a company or individual could use to protect their devices from malware and / or minimise the damage caused by infection.  Examples are supported by explanations of how the methods \ techniques would be in/effective. | 7-9 |
| 2 | **Level 2 Lower mid mark range**  **Subject Criterion Context**  **Some understanding** shown through the use of suitable examples that **describe** at **least two** methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection.  Examples are supported by limited descriptions and at least one explanation of how the method \ technique would be in/effective. | 4-6 |
| 1 | **Level 1 Lower mark range**  **Subject Criterion Context**  At the higher end of the mark range there is a simple **description** about at **least one** method \ technique that could be used by a company or individual to protect their devices from malware and / or minimise the damage caused by infection. The answer may not include an explanation of how the method(s) would work.  Simple **statements / example(s)** of methods / techniques (for example a bulleted list) supported by no comments is limited to the middle of this range. | 1-3 |
| **No creditworthy material** | | 0 |

|  |  |
| --- | --- |
| **Method**  **AO1 (Understanding)** | **Explanation**  **AO2 (apply)** |
| Regularly back up data and test backups. | Back up data so that you can restore data that has been accidentally deleted or destroyed. It is important to test that back-ups work on a regular basis. |
| Secure the backups. | Make sure that backups are off site so they are not lost under the same circumstances as the main data. Also if the backups are air-gapped then this will prevent a severe malware infection getting access to the backups as there is no physical connection. |
| Block or remove email attachments or links. | Check links contained in e-mails and do not open attachments included in unexpected e-mails. |
| Disable pop-ups. | Ensure the pop-up blocker is turned on and any website screening options are also on. |
| Control software downloads. | Only download software, especially free software, from sites you know and trust. Or prevent software downloads completely. |
| Ensure software is up to date. | Make sure all software is up to date and patched to prevent any exploitation of known vulnerabilities. |
| Anti-virus is up to date. | Ensure anti-virus automatically updates so that the latest vulnerabilities are detected and dealt with. |
| Disable macro scripts. | Prevent macros from running which could cause or run malicious code. |
| Only allow specified programs to run. | Preventing any unknown programs running should prevent any malicious code before it gets a chance to run. |
| Manage the use of privileged accounts and access levels to files. | Controlling the access to files should act as an internal firewall \ barrier to prevent unauthorised access or execution of programs. |
| Use virtualized environments \ sandboxes. | Operations are carried out in a controlled and temporary working space\environment which can be easily reset without effecting anything outside of the space\environment. |
| Use network filtering or a firewall. | Prevent \ block access into and out of the network using filtering and firewall to stop any malicious communications or transfer of viruses. |
| Remove the ability to use removable media. | Prevent unknown or unauthorised files to enter or leave the network. |
| MAC address filtering. | Can prevent access by unauthorised devices. |
| User training. | To educate staff in dangers of social engineering techniques and other unsafe practices. |
| Pen testing. | To allow organisation to understand where weaknesses may be, in order to strengthen their system security. |

**R.** Encryption, unless it is discussed in terms of minimising damage

**[12]**

**Q17.**

(a)     **3 marks for AO1 (knowledge and understanding)**

**1 mark** per correctly identified data type:

•        password : String

•        validlogin : Boolean

•        usernum : Integer

On any row, do not award a mark if more than one lozenge is shaded.

**3**

(b)     **3 marks for AO2 (apply)**

**Max 2 marks** for why using LEN makes the algorithm more flexible:

•        If the number of items in the array // number of users/passwords changes;

•        then line 09 // the FOR loop will not need to be changed;

**Max 2 marks** for why the stated line will not work:

•        The loop would count up to 3 // the loop will go past the end of the array;

•        because array indexing starts at 0 it should only count up to 2;

Award 2 marks for why the line will not work if the response includes the corrected line of pseudo-code:

FOR usernum ← 0 TO LEN(userlist)-1

**3**

(c)     **3 marks for AO2 (apply)**

validlogin get set after each comparison;

if the user details/username/password match the first or second user then validlogin will be reset to False later on;

validlogin will only reflect whether or not the user details/username/password matches the last value(s) in the arrays;

**3**

(d)     **1 mark for AO1 (knowledge and understanding)**

**1 mark for AO2 (apply)**

**Least Secure Password:** Smile;

**Reason:** It is a word (in the dictionary) // it only contains alphabetic characters // it does not contain any numbers/symbols;

**2**

**[11]**

**Q18.**

**9 marks for AO1 (knowledge and understanding)**

Award up to **three marks for each measure**. Of these:

•        Award up to two marks for an outline (one per point)

•        Award one mark for an example of a threat that it would be effective against.

The table below lists common examples but is not exhaustive; alternative valid responses should also be credited.

|  |  |
| --- | --- |
| Virus Checker | **Outline:** Scans files to look for malicious code Needs to be updated regularly with latest virus definitions Can quarantine / delete malware/suspicious files **Effective against:** Malware (accept examples) |
| Firewall | **Outline:** Analyses/scans network traffic Can block traffic from suspicious hosts/ computers/addresses/ports **Effective against:** Hackers Transmission of malware |
| Login system / Authentication / Password / Biometric | **Outline:** User has to enter username and password Can be authenticated by other methods such as biometric (accept examples) Login details matched to a database of users **Effective against:** Hackers Unauthorised access |
| MAC address filtering | **Outline:** Each hardware device has unique hardware address A database of allowed hardware/MAC addresses is kept/whitelist To connect to a network a device must have an address on the database/whitelist **Effective against:** Unauthorised devices |
| Encryption | **Outline:** Data is stored/transmitted as ciphertext (**A.** in coded form) Only people who know the encryption method/key can decrypt/read the data **Effective against:** Data theft |
| Prevention of use external storage devices / USB ports | **Outline:** Ports on a computer are disabled Storage devices connected to them cannot be accessed // flash drives cannot be used **Effective against:** Putting malware onto a computer Theft of data |
| Access rights | **Outline:** Users are associated with certain privileges These might control files that can be accessed/run // level of internet access // ability to create/delete files // ability to change settings **Effective against:** Hackers  Theft of data Authorised users doing unauthorised things |
| CAPTCHA | **Outline:** Users have to type in some distorted text // recognise images for a set of images Humans can do this but it is a difficult task for computer programs / bots  **Effective against:** Automated hacking programs Bots |
| Automatic software updates | **Outline:** Operating system / software configured to download updates from the internet Hackers look for security vulnerabilities in software Updates can patch security vulnerabilities **Effective against:** Hackers Malware |

**[9]**