

0	1
---	---

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.

[3 marks]

Blagging: _____

Phishing: _____

Shouldering (or shoulder surfing): _____

0 2 . 3 Penetration testing can be conducted as either black-box or white-box testing.

Explain the difference between these two types of penetration testing.

[4 marks]

0	3
---	---

A virus is a specific category of malware.

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

[6 marks]

Malware 1 _____

Malware 2 _____

Malware 3 _____

0 4 . 1 Define the term 'cyber security'.

[2 marks]

0 4 . 2 Define the term 'malware'.

[2 marks]

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- unpatched and/or outdated software.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.

[8 marks]

[illegible]

[illegible]

0	4	.	4
---	---	---	---

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

[1 mark]

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.

☐

0	4	.	5
---	---	---	---

Phishing is a form of social engineering.

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

[4 marks]

1 _____

2 _____

Turn over for the next question

0	5	.	1
---	---	---	---

State **two** issues with only using usernames and passwords in an authentication system.

[2 marks]

1 _____

2 _____

0	6	.	1
---	---	---	---

Explain what penetration testing is.

[2 marks]

0	6	.	2
---	---	---	---

Describe the aim of a white-box penetration test.

[2 marks]

Turn over for the next question

0	7	.	1
---	---	---	---

Define the term **cyber security**.**[2 marks]**

0	7	.	2
---	---	---	---

State **one** type of malware.**[1 mark]**

0	7	.	3
---	---	---	---

The network manager of a new computer games company, AQAware, is configuring the network. They are concerned about potential cyber security threats that could affect the company's systems.

Discuss the potential impact of the following threats on AQAware:

- weak and default passwords
- misconfigured access rights
- unpatched and/or outdated software.

In your response you should include:

- how these threats could be exploited by an attacker
- how AQAware could protect themselves against these threats.

[9 marks]

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

0	8
---	---

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.

[3 marks]

Blagging: _____

Phishing: _____

Shouldering: _____

0	9
---	---

Blagging and phishing are social engineering techniques.

Describe blagging and phishing.

[4 marks]

1	0
---	---

Viruses, trojans and spyware are forms of malware.

Describe how **two** of these forms of malware work.

[4 marks]

Name of malware 1 _____

Description _____

Name of malware 2 _____

Description _____
