CAMBRIDGE IGCSE (0478)

Module G: Security

Workbooklet · 8 parts · 166 marks

G6 and G9 are GCSE (OCR) only and not on 0478.

Contents

Part	Topic	Marks
G1	Malware: viruses, worms, Trojan horses, spyware, adware and ransomware	21
G2	Social engineering, phishing and pharming	20
G3	Brute-force attacks	20
G4	Distributed denial of service (DDoS) attacks	20
G5	Hacking and data interception	21
G7	Preventing attacks 1: firewalls, anti-malware and updates	21
G8	Preventing attacks 2: access levels, passwords, biometrics and two-step verification	21
G10	Staying safe online: SSL, proxy servers, privacy settings and checking messages	22
	Total	**166**

MODULE G SECURITY · G1

Malware: viruses, worms, Trojan horses, spyware, adware and ransomware

Original practice questions · 21 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **21 marks**.

1

Total: 6 marks

Each description in the table matches a different type of malware.

(a) Complete the table by writing the type of malware that matches each description. **[6]**

Description	Type of malware
Displays unwanted adverts on the screen and may redirect web searches to other websites	
A standalone program that copies itself to other computers across a network, without needing a host file or any action by the user	
Encrypts the user's files and demands a payment before they can be decrypted	
Looks like genuine, useful software, but contains hidden harmful code that runs once it is installed	
Attaches itself to a file or program, and copies itself when that file or program is run	
Secretly monitors what the user does, such as the keys pressed, and sends this data to a third party	

2 **Total: 4 marks**

A logistics company has a network of 200 computers. A worm gets onto one of the computers.

(a) Describe how the worm spreads to other computers on the company's network. **[2]**

(b) Give **two** effects the worm could have on the company's network. **[2]**

1

2

3 **Total: 4 marks**

An engineering firm's computer system is attacked with ransomware.

(a) Describe the processes involved in a ransomware attack on the firm's computer system. **[3]**

(b) State the aim of carrying out a ransomware attack. **[1]**

4 Total: 4 marks

Spyware has been installed, without the user knowing, on a computer used by a travel agent.

(a) Explain how the spyware could be used to gain access to the travel agent's online accounts. **[2]**

(b) The same computer is also infected with adware. Describe **two** effects the adware could have on the computer. **[2]**

1

2

5 Total: 3 marks

(a) Tick (✓) **one** box in each row to show whether each statement is true or false. **[3]**

Statement	True	False
A virus needs a host file or program to attach itself to		
A Trojan horse copies itself to other computers on its own		
Some adware also contains spyware		

Total for this worksheet: 21 marks

MODULE G SECURITY · G2

Social engineering, phishing and pharming

Original practice questions · 20 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **20 marks**.

1

Total: 1 mark

(a) Tick (✓) **one** box to show the aim of phishing. **[1]**

Aim	✓
A To make a website unavailable to genuine users	
B To obtain a user's personal data, such as passwords or bank details	
C To try every possible combination of characters until a password is found	
D To show unwanted adverts on a user's screen	

2

Total: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement describes **phishing** or **pharming**. **[4]**

Statement	Phishing	Pharming
The user receives an email that appears to come from their bank		
The user is sent to a fake website even though they typed the correct web address		
The user replies to a fake message with their password		
The attack can work without the attacker sending the user any message		

3 **Total: 5 marks**

A company sells garden tools online. Several customers typed the company's correct web address into their browser. A website that looked exactly like the company's website then asked them to enter their card details. The company finds out this was caused by **pharming**.

(a) Describe how pharming sent these customers to the fake website. **[3]**

(b) Explain the aim of the attacker in carrying out this pharming attack. **[2]**

4 **Total: 5 marks**

The receptionist at an engineering firm receives a phone call. The caller says they are from the firm's IT support team. They say the receptionist's account will be locked in ten minutes unless the receptionist tells them their password straight away.

(a) Identify **two** ways the caller tries to manipulate the receptionist. **[2]**

1

2

(b) State the aim of the caller. **[1]**

(c) Describe **one** other way, apart from a phone call or an email, that social engineering could be used to gain access to the firm's computer system. **[2]**

5 **Total: 5 marks**

A user receives a text message. It says it is from their bank, that an unusual payment has been made from their account, and that they should tap a link to stop the payment. The message is a phishing attack.

(a) Describe how this phishing attack could lead to the user's bank details being stolen. **[3]**

(b) Phishing and pharming can both use a fake website to collect personal data. Explain **one** difference between the processes of phishing and pharming. **[2]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G3

Brute-force attacks

Original practice questions · 20 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1, 5.3.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **20 marks**.

1

Total: 1 mark

(a) Tick (✓) **one** box to show which description is a brute-force attack. **[1]**

Description	✓
Sending a very large number of requests to a web server so it cannot respond to real users	
Using a program to try one password after another until the correct one is found	
Redirecting a user from a genuine website to a fake one without their knowledge	
Sending an email that pretends to be from a trusted organisation to get personal details	

2

Total: 6 marks

A hotel chain lets guests book rooms through an online account. Each account is protected by a username and password, and stores the guest's bookings and payment card details.

(a) Describe the process involved in a brute-force attack on a guest's account. **[3]**

(b) Tick (✓) **one** box in each row to show whether each one is a possible aim of a brute-force attack on a guest's account. **[3]**

Possible aim	Yes	No
To obtain the guest's payment card details		
To make the hotel's website unavailable by flooding it with requests		
To change or cancel the guest's bookings		

3 **Total: 4 marks**

The table shows how many different passwords are possible for some password rules. It also shows how long it would take to try every one of them, assuming the hacker's software tries 10 million passwords per second.

Characters allowed	Length	Possible passwords	Time to try them all
Lowercase letters only (26)	4	456,976	less than 0.1 seconds
Lowercase letters only (26)	6	308,915,776	about 31 seconds
Lowercase letters only (26)	8	208,827,064,576	about 6 hours
Upper and lowercase letters and digits (62)	8	218,340,105,584,896	about 253 days

(a) Explain, using the table, how the length of a password affects the chance of a brute-force attack being successful. **[2]**

(b) Explain, using the table, why the hotel should require passwords that contain a mixture of character types. **[2]**

4 **Total: 6 marks**

The hotel chain wants to reduce the risk of a brute-force attack on a guest's account being successful. Explain how each security solution helps.

(a) Locking the account after a set number of failed log-in attempts. **[2]**

(b) Two-step verification. **[2]**

(c) Letting guests log in to the hotel's app with a fingerprint (biometrics) instead of a password. **[2]**

5 **Total: 3 marks**

(a) Complete the sentences using words from the list. Not all of the words are used. **[3]**

combination · encryption · hardware · packet · phishing · software · trial and error

A brute-force attack finds a password by ....., trying every possible ..... of characters until one works. It is carried out using ....., so a huge number of attempts can be made every second.

Total for this worksheet: 20 marks

MODULE G SECURITY · G4

Distributed denial of service (DDoS) attacks

Original practice questions · 20 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **20 marks**.

1

Total: 5 marks

(a) Tick (✓) **one** box to show the aim of a distributed denial of service (DDoS) attack. **[1]**

Aim	Tick (✓)
To find a password by trying every possible combination	
To intercept data while it is being sent across a network	
To stop genuine users from accessing a website or server	
To send a user to a fake website when they type in a real web address	

(b) The word *distributed* in distributed denial of service tells you where the attack comes from. State what it tells you. **[1]**

(c) Tick (✓) **one** box in each row to show whether each statement about DDoS attacks is true or false. **[3]**

Statement	True	False
A DDoS attack sends a very large number of requests to a server at the same time.		
The owners of the computers used in a DDoS attack usually know that their computers are being used.		
The usual aim of a DDoS attack is to copy the data stored on the server.		

2 **Total: 4 marks**

(a) The statements **A** to **F** describe the process of a DDoS attack on a web server. Statement **A** is the first step. Write the numbers **2** to **6** in the table to show the order of the other steps. **[4]**

	Statement	Order
A	The attacker spreads malware to many computers, for example in infected email attachments.	**1**
B	The web server cannot respond to all of the requests.	
C	The attacker sends an instruction to the bots to start the attack on a chosen web server.	
D	Genuine users cannot access the website because the web server is very slow or has crashed.	
E	Each infected computer becomes a bot, and together the bots form a botnet that the attacker controls.	
F	The bots all send large numbers of requests to the web server at the same time.	

3 **Total: 6 marks**

A bus company has a journey-planner website that customers use to find bus times and buy tickets. The website is stored on the company's web server. One morning the web server suffers a DDoS attack.

(a) Explain why customers cannot use the journey planner during the attack. **[3]**

(b) During the attack, the company receives a message from the attackers. The message demands money to stop the attack. Identify the aim of this attack. **[1]**

(c) Give **two other** aims a person might have for carrying out a DDoS attack on a company. **[2]**

1

2

4 **Total: 2 marks**

A technician at the bus company finds the IP address of one of the computers sending requests to the web server. The technician blocks this IP address, but the attack continues.

(a) Explain why blocking this IP address does not stop the attack. **[2]**

5 **Total: 3 marks**

A manager at a different company says: "Every computer in our office has up-to-date anti-malware software, so our web server cannot suffer a DDoS attack."

(a) Explain why the manager is **not** correct. **[3]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G5

Hacking and data interception

Original practice questions · 21 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.1, 5.3.2, 2.3.1

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **21 marks**.

1

Total: 4 marks

Tick (✓) **one** box in each row to show whether each statement applies to data interception, hacking or both. **[4]**

Statement	Data interception	Hacking	Both
Data is captured while it is being transmitted across a network			
A person gains access to a computer system without the owner's permission			
One aim can be to steal personal data such as passwords			
The attacker can delete or change files stored on the computer system			

2 **Total: 8 marks**

A hotel provides a free wireless network for its guests. A guest uses a laptop on this network to log in to a travel booking website and enter their payment details.

(a) Describe the process of data interception on the hotel's wireless network. **[4]**

(b) Give **two** aims a person might have for intercepting the guest's data. **[2]**

1

2

(c) The booking website encrypts the data sent between the guest's laptop and the website. **[2]**
The guest says: "Because my data is encrypted, it cannot be intercepted."
Explain why the guest is wrong.

3 **Total: 9 marks**

An architecture firm stores its building designs and client records on a file server. Staff can connect to the server from home over the internet.

(a) Describe what is meant by hacking. **[2]**

(b) Give **three** aims a hacker might have once they have access to the firm's file server. **[3]**

1

2

3

(c) Explain how **two** different solutions could help keep the data on the firm's file server safe from hacking. **[4]**

Solution 1

Solution 2

Total for this worksheet: 21 marks

MODULE G SECURITY · G7

Preventing attacks 1: firewalls, anti-malware and updates

Original practice questions · 21 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **21 marks**.

1

Total: 4 marks

(a) Tick (✓) **one** box in each row to show which security solution each description matches. **[4]**

Description	Firewall	Anti-virus	Anti-spyware	Automating software updates
Installs patches that fix weaknesses in the operating system as soon as they are released				
Checks the traffic between a network and the internet against a set of rules				
Finds and removes software that secretly records the keys a user presses				
Scans files and compares them with a record of known viruses				

2 **Total: 5 marks**

A small accountancy firm keeps its clients' financial records on a server in its office. The office network is connected to the internet. The network manager sets up a firewall between the network and the internet.

(a) Describe what the firewall does with the traffic that arrives from the internet. **[3]**

(b) Give **two** examples of rules that the network manager could set on the firewall. **[2]**

1

2

3 **Total: 6 marks**

The firm installs anti-malware software, including anti-virus and anti-spyware, on every computer.

(a) Describe how the anti-virus software helps keep the firm's data safe from viruses. **[3]**

(b) State **one** way the anti-spyware software helps keep the clients' financial details safe. **[1]**

(c) Explain why the anti-malware software must be updated regularly. **[2]**

4 **Total: 3 marks**

The network manager sets every computer in the firm to install software updates automatically, instead of leaving staff to install them.

(a) Explain how automating software updates helps keep the firm's data safe. **[3]**

5 **Total: 3 marks**

One of the accountants says: "Now that we have a firewall, we do not need the anti-malware software."

(a) Explain why the accountant is **not** correct. **[3]**

Total for this worksheet: 21 marks

MODULE G SECURITY · G8

Preventing attacks 2: access levels, passwords, biometrics and two-step verification

Original practice questions · 21 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **21 marks**. The practice, staff and passwords on this sheet are made up.

A veterinary practice keeps records about animals, their owners and appointments on a computer system. The vets, receptionists and the practice manager all log in to the system.

1

Total: 4 marks

(a) Tick (✓) **one** box in each row to show which authentication method each statement describes. **[4]**

Statement	Username and password	Biometrics	Two-step verification
A one-time code is sent to the user's registered phone or email address, and the user must enter it			
A physical feature of the user, such as a fingerprint or face, is scanned			
The user types a secret string of characters that they chose			
Data that is unique to the user's body is compared with data stored earlier			

2 **Total: 4 marks**

The practice gives each type of user a different access level. Receptionists book appointments and update owners' contact details.

(a) Give **one** thing a receptionist's access level should allow, and **one** thing it should **not** allow. **[2]**

Allow .....

Not allow .....

(b) A hacker finds out a receptionist's username and password and logs in. Explain how access levels help to keep the practice's data safe. **[2]**

3 **Total: 4 marks**

A receptionist uses the password **bella2019**. Bella is the name of her cat.

(a) Suggest **two** changes that would make this password stronger. **[2]**

1

2

(b) Explain how a strong password helps to keep data safe from a brute-force attack. **[2]**

4 **Total: 4 marks**

The vets log in to tablet computers in the treatment rooms using a fingerprint scanner.

(a) Describe how the fingerprint scanner is used to authenticate a vet. **[2]**

(b) Explain why biometrics can keep the tablets more secure than a password. **[2]**

5 **Total: 5 marks**

The practice manager logs in to the practice's online booking system from home. The system uses two-step verification.

(a) Describe how two-step verification is used when the practice manager logs in. **[3]**

(b) The practice manager's password is stolen in a phishing attack. Explain why two-step verification still helps to stop the hacker logging in. **[2]**

Total for this worksheet: 21 marks

MODULE G SECURITY · G10

Staying safe online: SSL, proxy servers, privacy settings and checking messages

Original practice questions · 22 marks · ~25 minutes · Cambridge 0478 syllabus 5.3.2

Name _____ Date _____

Instructions. Answer all questions in the spaces provided. The marks for each part are shown in brackets [ ]. The total for this worksheet is **22 marks**. All organisations, names and web addresses in this worksheet are invented.

1

Total: 4 marks

(a) Tick (✓) **one** box in each row to show which solution each statement describes. **[4]**

Statement	SSL	Proxy server	Privacy settings
Requests and responses pass through it on their way between a user's device and the internet			
A security protocol that encrypts data sent between a web browser and a web server			
Lets a user choose who can see their profile and posts			
Can stop websites seeing the IP address of the user's device			

2

Total: 6 marks

A housing association lets its tenants log in to its website to report repairs and pay their rent. The website uses the secure socket layer (SSL) protocol.

(a) The statements describe how SSL sets up a secure connection when a tenant's web browser connects to the website's web server. Step 1 has been done for you. **[4]**
Write the numbers **2**, **3**, **4** and **5** in the table to show the order of the other steps.

Step	Order
The web server sends a copy of its SSL certificate to the web browser.	
The web server acknowledges the message and the SSL-encrypted session begins.	
The web browser asks the web server to identify itself.	**1**
The web browser checks that the SSL certificate is authentic.	
The web browser sends a message to the web server to say that communication can begin.	

(b) During a session, a criminal intercepts the data that contains a tenant's password. **[2]**
Explain why the tenant's password is still protected.

3

Total: 4 marks

A museum sends all web traffic between the computers in its offices and the internet through a proxy server.

(a) Explain **two** ways the proxy server helps to keep the museum's network and data safe. **[4]**

1

2

4 **Total: 5 marks**

A customer of Fernbrook Savings receives this message.

> **From:** Fernbrook Savings · **Subject:** URGENT – your acount is suspended
>
> Dear Valued Costumer,
> We have detected unusual activity on you're account. Your acount will be closed permanently in 24 hours unless you confirm your details NOW.
> Click below and enter your full password and card number to keep your account open.
>
> **Confirm my account**
>
> If you do not act today we will take legal action against you.
> Fernbrook Savings Securty Team

(a) The customer checks the spelling and tone of the message. **[3]**

Identify **three** signs in the message that suggest it is **not** genuine.

1

2

3

(b) The customer hovers the pointer over the button, without clicking it, to check the URL attached to the link. The browser shows the first address below. The second address is the genuine Fernbrook Savings website.

URL attached to the link	`http://fernbr0ok-savings-verify.example/login`
Genuine website	`https://www.fernbrook-savings.example`

Give **two** differences between the two URLs that show the link is not genuine. **[2]**

1

2

5 **Total: 3 marks**

A self-employed dog groomer has a public social media account. Their profile shows their date of birth, their home town and their own pet's name. Each post shows the place where it was posted.

(a) Explain how changing the privacy settings on the account could help keep the dog groomer's personal data safe. **[3]**

Total for this worksheet: 22 marks