OCR GCSE (J277)

Module G: Security

Workbooklet · 9 parts · 184 marks

G10 is IGCSE only and not on J277.

Contents

Part	Topic	Marks
G1	Malware: how it is used and its purpose	21
G2	Social engineering and phishing	20
G3	Brute-force attacks	20
G4	Denial of service attacks	20
G5	Data interception and theft	21
G6	SQL injection	20
G7	Preventing attacks 1: firewalls and anti-malware	21
G8	Preventing attacks 2: user access levels and passwords	20
G9	Preventing attacks 3: penetration testing, physical security and encryption	21
	Total	**184**

MODULE G SECURITY · G1

Malware: how it is used and its purpose

Original practice questions · 21 marks · ~25 minutes · OCR J277 spec 1.4.1

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: 3 marks

(a) State what is meant by **malware**. **[1]**

(b) Give **two** ways that malware can get onto a computer system. **[2]**

1

2

2

Total: 4 marks

Once malware is on a computer, it can be written to carry out different actions.

(a) Tick (✓) **one** box in each row to show the main purpose of each malware action. **[4]**

Malware action	Steal data	Extort money	Delete or corrupt data	Take control of the device
Records every key pressed and sends a copy to the attacker				
Locks the user's files and shows a demand for payment to unlock them				
Overwrites documents with meaningless characters so they can no longer be opened				
Lets the attacker run commands on the computer from another location				

3 Total: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement about malware is true or false. **[4]**

Statement	True	False
Malware can be spread on a USB memory stick		
Malware can only get onto a computer if the user downloads it from a website		
Some malware can copy itself to other computers on a network without the user doing anything		
Malware always shows a warning message when it is installed		

4 Total: 5 marks

An employee at an accountancy firm downloads a free file-converter program from an unfamiliar website. The program converts files as expected, but it also secretly installs malware that records everything the employee types.

(a) Explain why the employee is unlikely to notice that malware has been installed. **[2]**

(b) Describe how the attacker could use the recorded data to harm the firm or its clients. **[3]**

5 **Total: 5 marks**

One morning, staff at a veterinary practice cannot open any of the files on the practice's server. Every computer shows a message demanding a payment before the files will be unlocked.

(a) State the purpose of this attack. **[1]**

(b) Explain **two** ways this attack could affect the veterinary practice. **[4]**

1

2

Total for this worksheet: 21 marks

MODULE G SECURITY · G2

Social engineering and phishing

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.1

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: 3 marks

(a) State what is meant by **social engineering**. **[1]**

(b) Explain why people are often called the 'weak point' in the security of a computer system. **[2]**

2

Total: 4 marks

(a) Tick (✓) **one** box in each row to show whether each attack is an example of social engineering. **[4]**

Attack	Social engineering	Not social engineering
A caller pretends to work for an organisation's IT support team and asks an employee to read out their password		
Software automatically tries thousands of possible passwords on a log-in page		
A person on a train watches an office worker type their password on a laptop		
A web server is flooded with so many requests that genuine users cannot reach it		

3 **Total: 7 marks**

An employee at an architecture firm receives this email. It is a phishing email.

From: Staff Payroll Team <payroll-team@staff-pay-update.example>
Subject: URGENT: your salary payment is on hold

Dear staff member,
We could not process this month's salary payment. You must confirm your log-in details within 24 hours or your payment will be cancelled.
[Confirm my details]

(a) Identify **two** ways the email tries to persuade the employee to respond. **[2]**

1

2

(b) Describe how the attacker could use this email to gain access to the employee's account. **[3]**

(c) Give **two** things the attacker could do once they have the employee's log-in details. **[2]**

1

2

4 **Total: 4 marks**

A hotel receptionist receives a phone call. The caller says they work for the company that supplies the hotel's booking system. They say there is an urgent fault and ask for the administrator username and password so they can fix it.

(a) The hotel's computers are fully updated and protected by security software. Explain why this attack could still succeed. **[2]**

(b) Describe **one** other method of social engineering, apart from an email or a phone call, that an attacker could use to get a member of staff's password. **[2]**

5 **Total: 2 marks**

Some phishing emails include an attachment instead of a link.

(a) Explain how opening the attachment could harm the employee's computer. **[2]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G3

Brute-force attacks

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.1, 1.4.2

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: 5 marks

(a) Tick (✓) **one** box in each row to show whether each statement about brute-force attacks is true or false. **[5]**

Statement	True	False
A brute-force attack uses trial and error to find a password		
A brute-force attack works by tricking a person into telling the attacker their password		
Brute-force attacks are usually automated, so a very large number of passwords can be tried quickly		
The purpose of a brute-force attack is usually to gain unauthorised access to an account or system		
Adding one more character to a password reduces the number of possible combinations		

2 **Total: 5 marks**

A city bike-hire company lets members hire bikes through an online account. Each account is protected by a username and password, and stores the member's name, address and payment card details.

(a) Describe how a brute-force attack could be used to get into a member's account. **[3]**

(b) State **two** things an attacker might aim to do once they have got into a member's account. **[2]**

1

2

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 attacker'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) Using the table, explain why a longer password makes a brute-force attack less likely to succeed. **[2]**

(b) Using the table, explain why using a mix of character types helps protect against a brute-force attack. **[2]**

4 **Total: 3 marks**

An office manager is choosing a new password for the office's file server. These are the four options.

Option	Password
A	`garden`
B	`Garden26`
C	`gT8!wq#Lm2vZ`
D	`zzzz`

(a) Identify the option that would take a brute-force attack the **longest** to find. **[1]**

(b) Give **two** features of the password you identified in part (a) that make it harder to find with a brute-force attack. **[2]**

1

2

5 **Total: 3 marks**

A small accountancy firm's cloud file system locks a user's account for 30 minutes after five failed log-in attempts in a row.

(a) Explain how this rule limits the threat of a brute-force attack. **[3]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G4

Denial of service attacks

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.1

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: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement about denial of service attacks is true or false. **[4]**

Statement	True	False
A denial of service attack tries to stop genuine users from accessing a website or network.		
A denial of service attack floods a server with more requests than it can handle.		
An attacker must know a user's password to carry out a denial of service attack.		
The main aim of a denial of service attack is usually to copy the data stored on the server.		

2 **Total: 7 marks**

A ferry company sells tickets on its booking website, which runs on the company's web server. One evening the website becomes so slow that most customers cannot load the booking page. The company finds that its web server is the target of a denial of service attack.

(a) Describe how the denial of service attack is being used against the booking website. **[3]**

(b) State **two** effects the attack could have on customers who want to book tickets. **[2]**

1

2

(c) No data was stolen during the attack. Explain how the attack could still cost the ferry company money. **[2]**

3 **Total: 2 marks**

(a) Give **two** reasons why a person might carry out a denial of service attack on an organisation. **[2]**

1

2

4 **Total: 4 marks**

A week later, a second denial of service attack on the ferry company's web server comes from thousands of devices in different countries at the same time. Most of the owners of these devices do not know that their devices are taking part.

(a) Explain how the devices could be taking part in the attack without their owners knowing. **[2]**

(b) Explain why this attack is harder for the company to stop than an attack that comes from one computer. **[2]**

5 **Total: 3 marks**

After the attacks, a manager at the ferry company says: "The attackers must have broken into our web server, so we have to assume that every customer's data has been stolen."

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

Total for this worksheet: 20 marks

MODULE G SECURITY · G5

Data interception and theft

Original practice questions · 21 marks · ~25 minutes · OCR J277 spec 1.4.1, 1.4.2

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: 1 mark

Tick (✓) **one** box to show which statement describes data interception. **[1]**

Statement	Tick (✓)
A server is sent more requests than it can handle, so genuine users cannot reach it	
Data is captured while it is being transmitted across a network	
Software tries every possible password until one of them works	
A program that looks useful is installed, but it secretly carries out a harmful task	

2 **Total: 11 marks**

A café offers free Wi-Fi to its customers. One evening, a customer uses the Wi-Fi on their phone to log in to an online shop account and pay for an order. Someone sitting at another table is using a laptop with software that captures packets sent over the café's wireless network.

(a) Describe how data interception could take place on the café's wireless network. **[3]**

(b) Explain why the customer may not know that their data has been intercepted. **[2]**

(c) Explain why the café's wireless network is an easier target for data interception than a wired network would be. **[2]**

(d) Explain **two** purposes an attacker might have for intercepting the customer's data. **[4]**

1

2

3

Total: 5 marks

A recruitment agency keeps the personal details of thousands of job seekers. Staff store these records on laptops, which they take to meetings with employers.

(a) Give **two** ways the agency's data could be stolen, other than by intercepting it while it is transmitted. **[2]**

1

2

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

Statement	True	False
Encrypting a laptop's storage prevents the laptop from being stolen		
If an encrypted laptop is stolen, the thief cannot understand the data without the key		
Data theft can be carried out by a person who works for the organisation		

4

Total: 4 marks

The recruitment agency wants to limit the threat of its data being stolen. **[4]**
Identify **two** prevention methods the agency could use. For each method, explain how it limits data theft.

Method 1

How it limits data theft

Method 2

How it limits data theft

Total for this worksheet: 21 marks

MODULE G SECURITY · G6

SQL injection

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.1, 1.4.2

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: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement about SQL injection is true or false. **[4]**

Statement	True	False
The attacker enters SQL code into an input box, such as a search box or a login form		
SQL injection is a type of malware that copies itself from one computer to another		
A successful SQL injection attack could let the attacker change or delete records in a database		
Encrypting the data sent between the browser and the web server prevents SQL injection		

2

Total: 6 marks

A mail-order plant nursery has a website with a search box. When a visitor types the name of a plant and clicks Search, the website's program puts the typed text straight into this SQL query and sends it to the nursery's database:

```
SELECT PlantName, Price FROM Plants WHERE PlantName = '[text typed in the search box]'
```

The same database also stores customers' names, addresses and order details.

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

(b) Explain why typing SQL code into the search box could change what this query does. **[2]**

(c) Give **two** things an attacker could try to do to the nursery's database using SQL injection. **[2]**

1

2

3

Total: 4 marks

A community energy cooperative has a members' website. Members log in by typing a username and a password. The website's program builds an SQL query from the two values typed in. If the database finds a matching record, the member is logged in.

(a) Explain how SQL injection could let an attacker log in to the website without knowing a member's password. **[3]**

(b) State the weakness in the website's program that makes SQL injection possible. **[1]**

4 **Total: 4 marks**

The energy cooperative from Question 3 wants to protect its members' website against SQL injection.

(a) Explain how **input validation** could help to prevent an SQL injection attack on the login form. **[2]**

(b) The website's program connects to the database using an account that can read, change and delete the data in every table, including members' payment details.
Explain how restricting the **access level** of this account would limit the damage an SQL injection attack could cause. **[2]**

5 **Total: 2 marks**

Before the new login form goes live, the cooperative pays a security firm to carry out penetration testing on the website.

(a) Describe how **penetration testing** could help the cooperative protect its website from SQL injection. **[2]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G7

Preventing attacks 1: firewalls and anti-malware

Original practice questions · 21 marks · ~25 minutes · OCR J277 spec 1.4.2

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 whether each statement describes a firewall or anti-malware software. **[4]**

Statement	Firewall	Anti-malware software
Checks data coming into and going out of a network against a set of rules		
Compares files with a database of known malware		
Moves an infected file into quarantine so that it cannot run		
Can block all traffic that comes from a particular IP address		

2 **Total: 5 marks**

A regional bus company has an office network of 30 computers and a server that stores its timetables and staff records. The network is connected to the internet. The company installs a firewall between its network and the internet.

(a) Describe how the firewall limits unauthorised access to the company's network. **[3]**

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

1

2

3 **Total: 3 marks**

(a) Apart from unauthorised access, identify **one** other form of attack that the bus company's firewall may limit. Explain how the firewall limits this attack. **[3]**

Form of attack

How the firewall limits it

4 **Total: 5 marks**

The bus company also installs anti-malware software on every computer in the office.

(a) Describe how the anti-malware software protects a computer from malware. **[3]**

(b) The anti-malware software downloads new updates every day. **[2]**
Explain why the anti-malware software needs to be updated regularly.

5 **Total: 4 marks**

An office worker at the bus company plugs a USB memory stick into their computer. One of the files on the memory stick contains malware.

(a) Explain why the firewall will **not** stop this malware reaching the computer, **and** how the anti-malware software could limit this attack. **[4]**

Total for this worksheet: 21 marks

MODULE G SECURITY · G8

Preventing attacks 2: user access levels and passwords

Original practice questions · 20 marks · ~25 minutes · OCR J277 spec 1.4.2

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**. The company, staff and passwords on this sheet are made up.

An engineering company keeps its product designs, customer orders and staff pay records on a file server. Every employee logs in to the network with a username and a password.

1

Total: 4 marks

(a) Tick (✓) **one** box in each row to show whether each statement describes user access levels, passwords, or both. **[4]**

Statement	User access levels	Passwords	Both
Different users are given different permissions, for example read-only or read/write			
A secret string of characters is entered with a username to log in			
Helps to stop people getting to data they are not authorised to access			
Is harder to crack in a brute-force attack when it is long and uses a mix of character types			

2 **Total: 6 marks**

A sales manager at the company uses the password **Rover1987**. Rover is the name of her dog and 1987 is the year she was born.

(a) State **two** reasons why this is a weak password. **[2]**

1

2

(b) Explain how using strong passwords limits a brute-force attack. **[2]**

(c) The network locks a user's account after five incorrect password attempts. Explain how this limits a brute-force attack. **[2]**

3 **Total: 2 marks**

Some employees have received phone calls from a caller pretending to work in the company's IT department.

(a) Give **two** rules employees should follow so that their passwords are not given away to an attacker. **[2]**

1

2

4 **Total: 4 marks**

The company uses user access levels. An office administrator needs to look up dates in the product design files, but must not change them. The administrator does not need the staff pay records.

(a) State the access level the office administrator should be given to the product design files. **[1]**

(b) An attacker logs in to the network using the office administrator's username and password. Explain how user access levels limit what the attacker can do. **[3]**

5 **Total: 4 marks**

A director says: "Everyone has a strong password, so we do not need user access levels."

(a) Explain why the company should still use user access levels as well as strong passwords. **[4]**

Total for this worksheet: 20 marks

MODULE G SECURITY · G9

Preventing attacks 3: penetration testing, physical security and encryption

Original practice questions · 21 marks · ~25 minutes · OCR J277 spec 1.4.2

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

Complete the table by writing the prevention method that each description matches. Choose from the list. Not all methods are used. **[4]**

anti-malware · encryption · firewall · penetration testing · physical security

Description	Prevention method
Staff must swipe a keycard to open the door of the room where the servers are kept.	
A company pays a security team to try to break into its systems, with permission, and report the weaknesses it finds.	
Data is scrambled using a key, so that anyone who intercepts it cannot understand it.	
Traffic coming in from the internet is checked against a set of rules, and traffic that breaks the rules is blocked.	

2 **Total: 4 marks**

A company sells concert tickets through its website. Its servers are kept in a room on the ground floor of a shared office building. People from other businesses use the same main entrance.

Describe how physical security could limit each of these threats.

(a) A visitor walks into the unlocked server room and plugs a USB drive into one of the servers. **[2]**

(b) A laptop that holds customer records is left on a desk in the office and is taken overnight. **[2]**

3 **Total: 6 marks**

The ticket company is about to launch a new web page where customers log in, search for concerts and pay for tickets.

(a) Explain why the company should have penetration testing carried out before the new page goes live. **[3]**

(b) Give **two** types of attack that a penetration tester could simulate on the new page. **[2]**

1

2

(c) State **one** difference between a penetration tester and a criminal attacker. **[1]**

4 **Total: 3 marks**

Every Friday, a backup copy of the customer database is saved onto an external hard drive. A manager carries the drive to the company's second office. The backup is encrypted.

(a) Explain how encrypting the backup limits the threat if the drive is stolen on the way. **[2]**

(b) State **one** other threat to the customer data that encryption could help to limit. **[1]**

5 **Total: 4 marks**

The company's IT manager says: "Our firewall keeps attackers out, so we don't need physical security for the servers and we don't need penetration testing."

Explain why the IT manager is wrong. Refer to **both** physical security **and** penetration testing in your answer. **[4]**

Total for this worksheet: 21 marks