UNITED ARAB EMIRATES
MINISTRY OF EDUCATION

Security Measures

Cycle 2 – Grade 7

Computing, Creative Design and Innovation

Student book

Grade 7
Volume 3

1445- 1446 A.H./2024- 2025 A.D

Security measures

Security measures (also called **cybersecurity**) are **physical and digital methods** used to **protect electronic devices and information** from **harm, theft, and unauthorised use**. Security measures are important as networked computers can render information vulnerable to threats. Some threats you should already know about are:

- phishing
- hacking
- spyware
- data interception

Physical security measures

Physical measures are used to **stop someone accessing devices or information** in **person**. Some physical security measures include:

- locks
- safe boxes
- alarm systems
- surveillance systems

Locks

Locks can be used to stop a person from accessing a device or server room where devices are stored. They are often used in combination with **doors, fences, gates and walls**. Some modern locks **use ID cards** or **biometrics** such as **facial recognition** or **fingerprint** scans which are more secure than traditional locks that use keys or codes.

Safe boxes

Safe boxes can be used to stop someone accessing a backup drive or portable device. They can be used to store **digital backup drives** away from the network and hard copies of information. Similarly, to door locks they can be used to stop someone accessing a device or information in person.

Alarm systems

Alarm systems can stop someone accessing a device or information in person. Modern alarm systems will **alert the property owner** in the event of **unauthorised access**. These systems often also work as a **deterrent** for those who may want to attempt to gain unauthorised access.

Surveillance systems

Surveillance systems often work alongside alarm systems. They can **monitor** an area for intruders who wish to access information without permission. The surveillance system can include cameras or security personnel who patrol an area. If an intruder is found, the alarm system is switched on.

A logbook can also be used to monitor who enters and leaves the area.

Theory

Activity 24

Digital security measures

Digital measures are used to stop someone accessing devices or information electronically. Some digital security measures include:

- passwords
- antivirus software
- firewall software

Passwords

Passwords can help to stop unauthorised authorised access to devices, networks and accounts. They are a digital way of **proving who you are**. A good password will meet the following requirements:

- an English uppercase character (A-Z).
- an English lowercase character (a-z).
- a number (0-9) and/or symbol (such as !, #, or %).
- eight or more characters in total.

For passwords to work effectively you **must not share them** with others and remember to **lock devices and log out of accounts** when you are not using them.

Anti-virus software

Anti-virus software can help to stop viruses and malware getting onto your device. This software works by **inspecting device files and files downloaded from a network**. The software will compare each file to known viruses and remove or quarantine any suspicious files that are identified. Though anti-virus software is very effective it can only identify known viruses, so it is important to update the software regularly.

Firewall software

Firewalls can help to stop someone hacking your computer or network. Firewalls monitor network traffic and decides whether to allow or block specific traffic based on a set of security rules. Firewalls are often used to create a barrier between trusted local area networks and untrusted outside networks, such as the Internet.

Activity 25 (Theory)

Activity 26 (Interactive)

Encryption

What is encryption?

Ahmed has come up with a new entrepreneurial idea. He wants to send it to his friends using the internet to get feedback. He is worried about hackers stealing his idea, so Ahmed uses an **encrypted software** to send the information.

This means that the information is **converted into a format that is not readable for anybody** who tries to steal it. Only the people who have a **key** can convert the code back to its original format.

Remember

Encryption is a process of converting normal data into an unreadable form. It is normally done by the **sender** of information.

Decryption is a method of converting the unreadable/coded data into its original form. It is normally done by the **receiver** of information.

- **Plaintext** is the original message format
- **Ciphertext** is the converted message format
- **Cryptographic key** is the method used to lock (encrypt) data so that only the person with the correct key can unlock (decrypt) it

Did You Know?

Encryption does not stop people from intercepting a message, it only helps to stop them from understanding it

Why is data encryption necessary?

Privacy – it stops unintended recipients from reading sensitive data

Security – it can prevent data breaches of important information

Data integrity – it helps to stop people from tampering or changing information

Authentication – the cryptographic key can be proof that somebody is the owner of certain information

Regulations – companies that handle data are requested to use data encryption for all the reasons above

Activity 27 Interactive

Types of encryption

There are two main types of encryption:

- **Symmetric encryption**
- **Asymmetric encryption**

Symmetric encryption

In symmetric encryption, there is only one key used for both encryption and decryption.

Asymmetric encryption

In asymmetric, there are two keys. One key is used for encryption, and a different key is used for decryption.

Theory

Activity 28

The Caesar cipher

An early method of encryption was the **Caesar cipher**. Julius Caesar used this to send messages to his military. He used **encryption** in case his enemies would intercept the messages. It meant that his enemies would **not be able to read his strategies**.

How the Caesar cipher works

The method was simple. The message was **encrypted** by replacing the real letters with replacements. The **key** looked something like **below**, where A is represented by D.

A simple message like "move forward" would be **encrypted** to look like "pryh iruzdug".

Remember

The process of changing the original message into code words is called encryption.

Encryption

In below table, first word "move" is changed to "pryh"

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

m	o	v	e
↓	↓	↓	↓
p	r	y	h

And the second word "forward" is changed to "iruzdug" in the below table.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

f	o	r	w	a	r	d
↓	↓	↓	↓	↓	↓	↓
i	r	u	z	d	u	g

The simple message "move forward" is now **encrypted** to look like "pryh iruzdug". If the message gets lost or stolen, the person will have difficulty reading the message. For this reason, it is important that the **key** is kept separate to the message.

Decryption

Once the message has been received by the intended person, the **key** can be provided to **unlock it**. This process is called **decryption** and is the **opposite of encryption**.

Decrypting the **encrypted** message "pryh".

Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

p	r	y	h
↓	↓	↓	↓
m	o	v	e

Decrypting the **encrypted** message "iruzdug".

Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

i	r	u	z	d	u	g
↓	↓	↓	↓	↓	↓	↓
f	o	r	w	a	r	d

Activity 29

Theory

Activity 30

Theory

Online platforms for research

Many resources are available on the internet that can be used for research. Some examples of resources that can be used for research are:

- **social media**
- **websites**

When using online resources for research it is important to remember:

- **not to access content that is inappropriate or illegal**. For example, music or videos protected by copyright laws.
- only **use reliable information** (factually correct information that can be verified by multiple sources)
- sometimes reliable information can be **difficult** to find because a lot of information available online is **biased**.

Researching with social media

Social media are websites or applications that enable users to create and share information in virtual communities.

Social media has become increasingly popular for many reasons:

- it is easy to use
- it is designed to be fun
- it is free to access
- it reaches a lot of customers
- it can drive traffic to your website

Businesses have realised that this allows them to use social media as a platform to do **market research and access a large amount of people without much expense**.

Social media is a great opportunity to **promote products** and get **customer feedback**. It is useful to gain public opinion. It is very difficult to **verify** the **quality and accuracy** of information gathered.

Some of the key problems with researching via social media is that a **lot of the information** gathered is **opinion based** and **not factual**. This can lead to some **fake news** getting circulated. It is important to **use official sources** of information to get **reliable information**.

Social media contains a lot of opinions which means that the information presented can also be **bias**. It is important to remember that popular opinion does not make information factual.

Social media can also contain **content that is inappropriate**. Fake accounts can be easily created with misleading information.

Disadvantages of social media for research:

- **opinion based and not factual**
- **fake news**
- **bias**
- **inappropriate content**
- **misleading information from fake accounts**

Did You Know?

Social media platforms are **designed to keep users engaged and increase your screen time**. You should monitor your usage and not spend too much time using these platforms.

Theory

Activity 31

Theory

Activity 32

Researching with websites

Websites are a group of pages accessible from the world wide web containing information and providing services.

Websites can be very **useful for research**. Using websites is extremely popular for many reasons:

- **they are easy to find and use**
- **they are free to access**
- **they can be used to present key information**

Businesses use their website presence to represent them. It displays lots of information and visuals that help customers associate with their brand.

Using websites is a great way to source a very wide range of information, However, you must source factually correct information from reliable websites and verify the information using multiple sources.

Some of the dangers when researching information on websites include:

- **bias information that is not accurately representing the reality**
- **out of date information**
- **there can sometimes be too much information available**

Theory

Activity 33

Biased information

Biased information is **not factually correct** and **not verifiable**. Some reasons that information may be biased are:

- **sourced from an unreliable website.**
- **opinions rather than verifiable facts.**
- **author has an agenda (such as advertising).**
- **author has not considered other points of view.**

It means that the information presented is in favour of one thing more than another. This can sometime be on purpose, or sometimes it can be subconsciously.

When looking at websites, you have to consider if the **author has an agenda**. This can lead to **bias**.

A simple example of an agenda is that any company who want to sell their product will be bias towards it. In doing so, their website and advertising will only display information which is favourable towards their own company.

How to identify a website that is biased:

- The company is promoting their own product or using advertising
- The information is more opinion based than factual
- The information is one sided
- It is lacking solid evidence
- The language used is persuasive or opinion based
- The owner of the website has an alternative agenda rather than presenting the true facts

Theory

Activity 34

Using reliable websites

It is very difficult to avoid bias behaviour, so one of the best things that we can do is to be aware of what to look for on a website.

Some details can contribute to sourcing quality websites include:

- **contact details**
- **website prestige**
- **date information**

Contact details

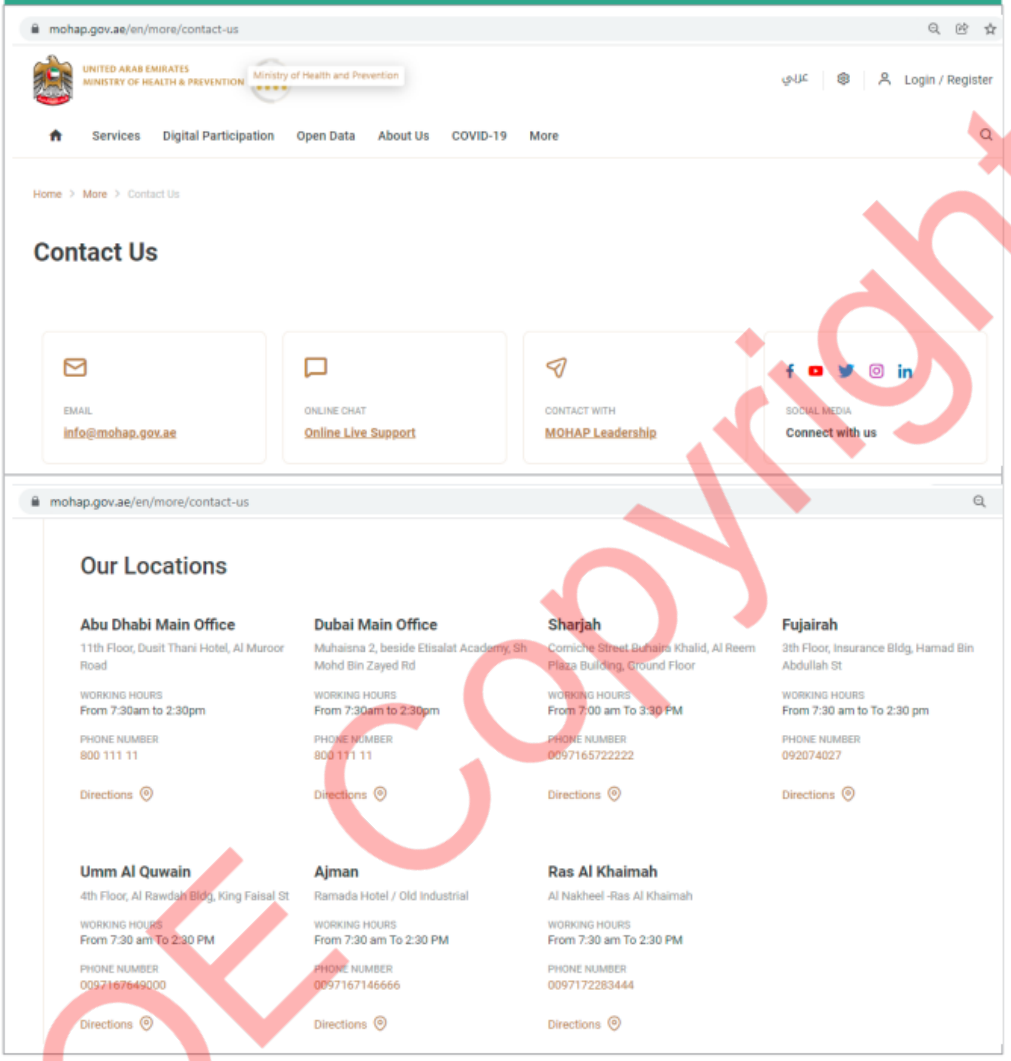
When you have found a website that you believe to be **reliable**, it is a good idea to verify the **contact details**.

The contact details often include the company:

- phone number
- email address
- location

If in doubt, it is a good idea to contact the company directly to verify that this website is genuine.

Website contact us page



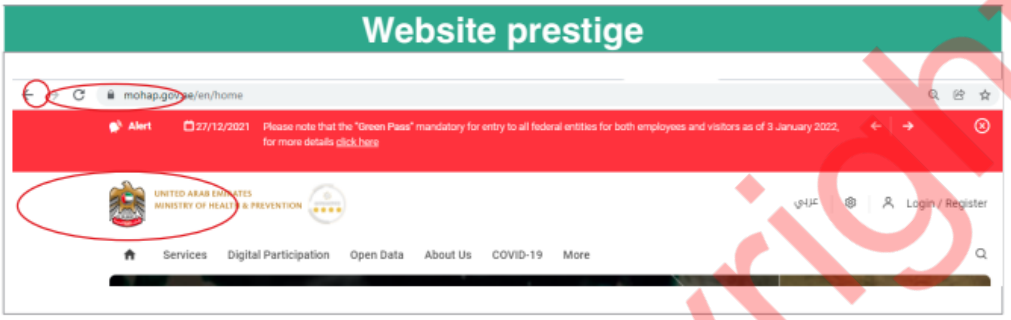
Website prestige

The prestige of a website is also a good indication as to how reliable the information is.

- It is better to use websites that are **secure.** These websites start with **https://**
- E.g https://mohap.gov.ae/en/home
- Website addresses usually use the company name or initials in the address

- A reliable website will look organised. It will have a clear logo, menu bar, name of the company and may also include some company information.

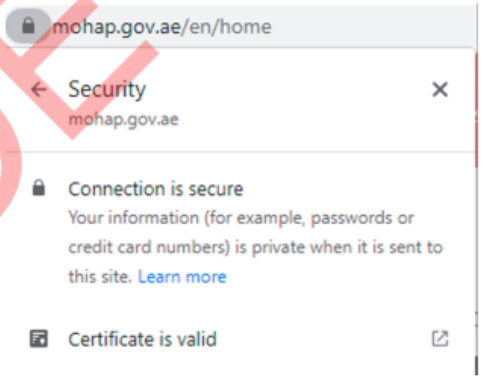
Be careful that **fraudulent websites** can sometimes **mimic** the real website with an aim to do **cybercrimes such as phishing**.



In further detail:

Secured site	Website address	Logo
https://mohap.gov.ae/en/home	mohap.gov.ae/en/home	UNITED ARAB EMIRATES MINISTRY OF HEALTH & PREVENTION

Checking to see if the certificate is valid is also a way to ensure the website you are looking at is reliable.



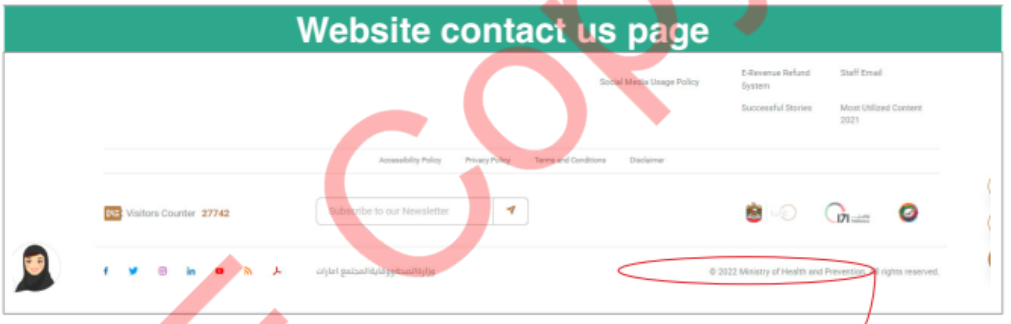
Outdated information

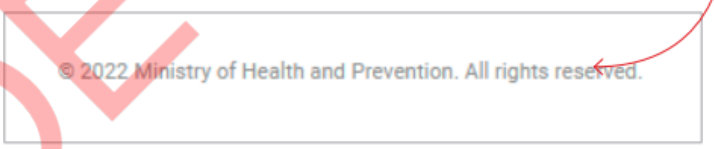
It is important to ensure that information found is **relevant to the current day**. The internet has so much information available that **some of it** is now **incorrect and outdated.**

How to identify if a website is outdated:

- There are other sources of reliable information that contradict it
- Find the published date
- Has the source published any data to support? Follow the links to find if it has been updated recently.
- A copyright © symbol and the date the website was last updated is displayed at the bottom.

Website contact us page





Computing, Creative Design and Innovation

Activity book

Grade 7
Volume 3

1445- 1446 A.H./2024- 2025 A.D

Security measures

Physical security measures

Theory

Activity 24

Noor has bought a new laptop and wants to keep it safe. Working in groups, explain how to use **one physical security measure** to keep her new device safe.

Remember, some physical security measures include:

- locks
- safe boxes
- alarm systems
- surveillance systems

What physical security measure have you selected?

.....

.....

.....

Explain how the measures you used can help to stop someone accessing devices or information.

Outline one flaw with the security measure you have chosen.

Digital security measures

Theory

Activity 25

Noor has started to use her new laptop. Working in groups, explain how to use **one digital security measure** to keep her new device safe.

Remember, some digital security measures include:

- passwords
- antivirus software
- firewall software

What digital security measure have you selected?

.....

.....

.....

S T R E A M

Explain how the measures you used can help to stop someone accessing devices or information.

Outline one flaw with the security measure you have chosen.

Activity 26

Interactive

Ahmed is learning about security measures.

Explain physical and digital security measures.

Use the words to fill in the blank spaces.

digital	information	firewalls
locks	physical	measures

Security ..... (also called cybersecurity) are physical and ..... methods used to protect electronic devices and information from harm, theft, and unauthorised use.

..... measures are used to stop someone accessing devices or information in person. Some physical security measures include:

- .....
- safe boxes
- alarm systems
- surveillance systems

Digital measures are used to stop someone accessing devices or ..... electronically. Some digital security measures include:

- passwords
- anti-virus software
- .....

Encryption

Activity 27

Interactive

Noor is learning about encryption.

Explain the words by matching them to the description.

Key words		Description
key		Encrypted messages are known as this
plaintext		Used to lock and unlock data
ciphertext		Unencrypted messages are known as this

Types of encryption

In groups, discuss whether you think symmetric encryption is more secure than asymmetric encryption.

When you are finished discussing, write down one advantage and one disadvantage of each type.

Symmetric Encryption
Advantage
Disadvantage
Asymmetric Encryption
Advantage
Disadvantage

The Caesar cipher

Theory

Activity 29

Noor has sent you this message: **"ghfubswlrq lv frro"**

Can you **decrypt it** using the **key**?

The first letter has been completed for you.

Decrypting the **encrypted** word "ghfubswlrq".

Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

g	h	f	u	b	s	w	l	r	q
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
d									

Decrypting the **encrypted** words "lv frro".

Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

l	v
↓	↓

f	r	r	o
↓	↓	↓	↓

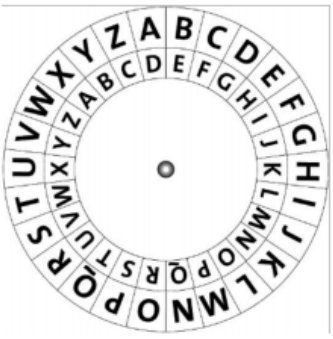
Theory

Activity 30

Use the Caesar cipher to write an **encrypted** message to your friend.

Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

When you are done, **swap encrypted** messages and see who can solve it first.



Online platforms for research

Researching with social media

Theory

Activity 31

Ahmed wants to get his **friends opinions** when buying a new laptop. He puts a photo of two different laptops on his Instagram page and starts a **poll**. His friends start to vote for the laptop that they prefer. The final vote is:

Laptop A = 52%

Laptop b = 48%

Ahmed is looking at the results of his social media poll. Help him to consider the following.

Do you think that Laptop A is definitely the best laptop? Yes / No

What information is **not** given to Ahmed in this poll?

.....

.....

.....

Do you think **social media** is a **factually accurate** method of **gathering research** information? Yes / No

What other methods could you suggest that Ahmed uses to get information?

.....

.....

.....

Do you think the information gathered is still useful to Ahmed? Why?

.....

.....

.....

Theory

Activity 32

Noor is learning about the use of social media for entertainment.

Explain how social media can be used for research.

Write your answer below.

Evaluate the use of social media for research by explaining some advantages and disadvantages.

Write your answers below.

Social media for research	
Advantages	**Disadvantages**

Researching with websites

Theory

Activity 33

Ahmed is using the internet for research. He wants to know about some of the advantages and disadvantages of this.

List 2 advantages of using websites for research.
List 2 disadvantages of using websites for research.

Biased information

Theory

Activity 34

Noor is researching on the internet and is cautious of bias information. Help her by explaining some of the reasons why a company creates biased information.

Why would a company create bias information?

S T R E A M

Using reliable websites

Theory

Activity 35

Ahmed has found a website on the internet that he wants to use as part of his research. Help him to do **3 checks** to ensure the website he is using is **reliable**.

What can Ahmed check to ensure the website is reliable?
1.
2.
3.

MOEUAEofficial