



SMART 04

# Personal mobile security

This module describes some things to be careful about when you are using mobile technology.

[Start course >](#)



Co-funded by the  
Erasmus+ Programme  
of the European Union

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.





**SMART**

**MODULE 4**

## Personal mobile security

Over the past few decades, mobile devices have advanced from just facilitating making calls to many other uses. This has brought mobile access to banking, apps, Internet. With these new features, comes concern about data security. In this module we will explain about data protection, how to create and change passwords, secure Wi-Fi navigation, and how to protect yourself from cyber bullying and internet trolls.

## Intended audience

---

This module is intended for everyone who wants to learn about safe navigation online, data protection, cookies and how the law protects their personal information (GDPR).

This material may be challenging for some learners. In that case, it would be useful to work through the content with a companion or friend.

Facilitators will be able to use this material to inform themselves and to provide advice about security aspects of digital technologies.



# What will you learn in this module

- 1 EU/ US data protection GDPR and cookies consent.
- 2 How to create and change passwords.
- 3 What is hacking and how can you protect yourself?
- 4 How to protect yourself from cyberbullying.



# Chapters in this module

---

**1**

Introduction to mobile security and data ownership

---

**2**

Authentication: how to create and change passwords

---

**3**

Protecting a mobile device

---

**4**

Cyberbullying and dealing with inappropriate content



SMART

MODULE 4

CHAPTER 1

# Introduction to mobile security and data ownership

“Information is power!” Personal information is one of our most valuable possessions. In the modern era, this important resource is completely undervalued by consumers, but not by companies! Some of the biggest companies in the world have been successful through clever use of your data. This chapter explains data ownership in the age of mobile computing and “the cloud”.

# What will you learn in this chapter

- 1 What is the General Data Protection Regulation.
- 2 Personal data protection under GDPR.
- 3 How to manage cookies.
- 4 Types of personal data.
- 5 Where is your data stored.
- 6 How to back up your mobile device.



## Data analytics – one of the fastest growing new industries

---

The gathering and analysis of data is important for businesses to understand customer's needs. Data analytics has helped companies to improve their services for customers.

Data analytics makes websites and apps more usable, and, for example, allows a smart watch user to see the number of steps taken in a day. Data analytics is often applied to (your) **personal data**.





## Personal data and mobile and wearable devices

---

**Personal data** is information that relates to an identifiable individual.

Companies must protect personal information of citizens under the **General Data Protection Regulation (GDPR)** law by encoding sensitive **information** that is stored or is sent over public networks.

GDPR will be discussed later in this chapter.



## Why it is important to secure data collected by mobile devices

---

Where a person or organisation gets access without consent or permission to personal information – address, age and gender, health issues, financial status, interests, etc. - this can cause problems for the person whose data is collected.

**Personal data** is data that relates to an identifiable person. Such information helps to personalise a service for you. Companies must protect your personal information under **GDPR** law by encrypting sensitive **information** like the personal data examples shown above, sent to third parties over public networks.

More information on this can be found at <https://gdpr-info.eu/>.





## What is GDPR?

To prevent companies gaining personal data from citizens without their consent, the European Commission introduced the **General Data Protection Regulation (GDPR)**.

GDPR protects the personal data of citizens who live and work within the European Union. Organisations operating in the EU must have consent to process personal data.

# GDPR – what rights does it offer within the EU?

---

GDPR offers the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification and erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights about automated profiling



## What types of data could qualify as personal data?

---

In order to understand the importance of rights of data privacy in the EU, we need to know types of personal data that could be affected by GDPR.

Let's look at some typical examples of types of data that could be considered as personal data and so are worth protecting.



# Examples of personal data

---

1

2

3



## Demographic information is personal data

When a person completes a form to, for instance, apply for a grant, they are trusting the organisation who makes the form to treat sensitive information in confidence. This is a type of personal data.

## Examples of personal data

---

1

2

3



### Healthcare records contain personal data

A visit to a doctor is considered to be a confidential experience. The data that is recorded about an individual patient is also highly confidential and so can be considered personal data.

## Examples of personal data

---

1

2

3



**A record of daily activities is personal data**

A record of purchases made, locations visited and journeys taken by a known person is also personal data.



DAILY

ROUTINE

1

2

3



## Daily activities

Mobile devices and wearables record an extraordinary level of detail about a person's daily activities. Much of this personal data ends up in the cloud databases of mobile and wearable apps. By having this data, technology companies can provide detailed information to you about your activities.

## Types of personal data

4

5



Individual financial information is personal data. Financial statements, credit ratings and bank balances are another category of personal data. It can be used to categorise you as a big spender, or careful purchaser.

## Types of personal data



### Images or recordings of people are personal data

Owners of security cameras must be careful about storing video footage, as it can contain personal data. The same applies to sound recordings. Both should only be kept with the consent of those who are recorded.

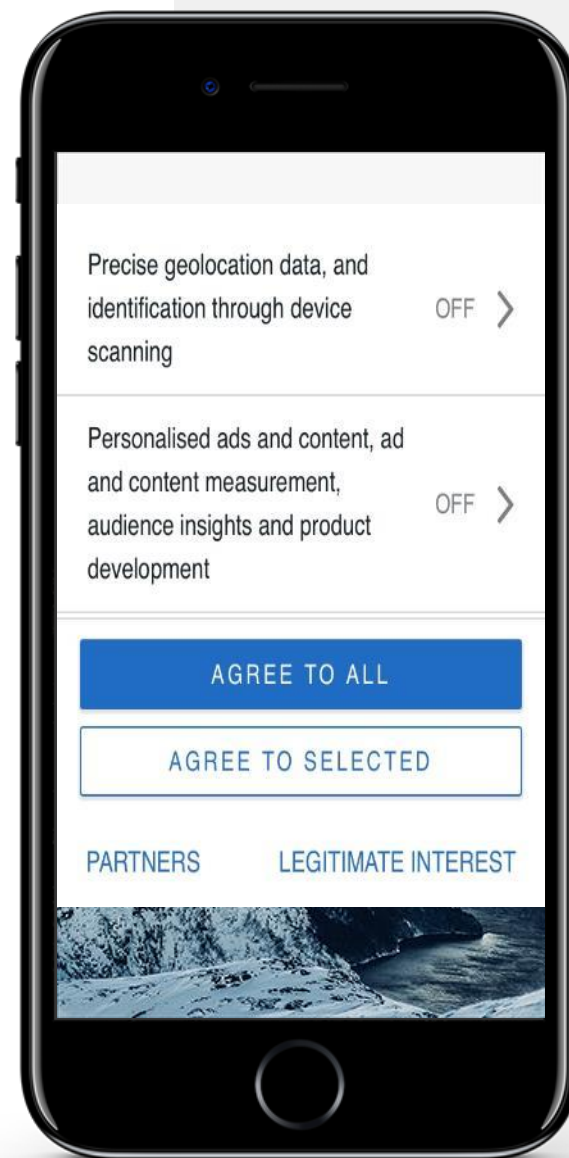
# Cookies: agreements to give personal data to a company

---

Cookies are small files that websites send to your device to remember certain information about you. For example, your sport preferences or log in details.

Under GDPR regulations, a website must get a user's consent to install cookies on their device.

If you are concerned about your data being analysed, then you can select either the "Reject All" or "Agree to Selected" options (as shown in the image here). Disabling cookies means that the website is not personalised and cannot recall details such as a password or purchases.



## Fake messages – a warning!

---

Sometimes interesting messages appear on your mobile device. When you see a message for a prize or story which seems too good to be true, it is usually a trick maybe to steal your money.

When a message like this is received, it is important to **not** fill out a form, to **not** click a link or to **not** share personal information, such as phone numbers, e-mail, or address, unless you know it came from a valid source.

Similarly, news items that you read on your phone may be “fake news” - news that is false or fabricated.



### CONGRATULATIONS!

You have won an Apple iPhone 12 Pro!

1. Click on "OK" to visit our sponsors page.
2. Enter your address and pay 1€ shipping to get your iPhone 12.
3. Your Apple iPhone 12 Pro will be delivered within 3 to 5 days by the courier service.

OK





## What is the cloud?

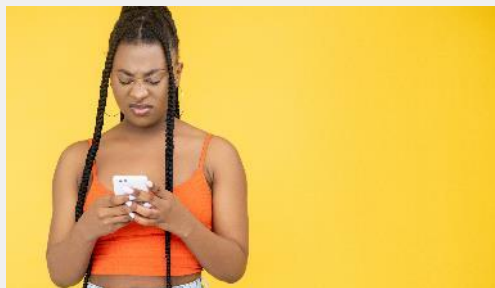
The so-called cloud is a worldwide network of powerful computers, and the software that runs on those computers. Your personal data can be collected from you and stored in a cloud computer anywhere in the world. Data created by you can also be stored in the cloud and you can access that data from multiple devices.

The storage and analytics happen on cloud computers in a data centre, instead of locally on the user's device.

<https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud>

# The cloud is very useful for mobile devices

---



## Problem: device storage is limited

Most mobile devices have only limited storage and computing power. At some point, storage space will run out and processing will be slow.



## Solution: store and analyse data in the cloud

Files, photos, videos can be copied to the cloud. It's good to keep copies and cloud computers are very powerful. However, it is important to remember that cloud security can be an issue.



## **Cloud security**

So, how secure is data when it has left your mobile device and is stored on a cloud computer?

Even apart from companies using user's data to sell more products, personal data on the cloud can be hacked and used for criminal purposes. Cloud security is important for personal data and mobile devices. Make sure your service provider and data is EU-based.



# Cloud data: where to keep your files? Local or cloud?

---



## Advantages

- Personalisation and better service
- More storage space, as a mobile device has limited storage
- More data means “smarter” decisions
- All the data appears to be “in one place”




## Disadvantages

- The user is accepting a loss of data privacy to the cloud provider
- Possibility of theft and fraud
- Once data is in the cloud, it is extremely difficult to delete it

# Quiz

Click the **Quiz** button to edit this object



**SMART** **MODULE 4** **CHAPTER 1** Introduction to mobile technology: personal mobile security

GDPR protects your right to be informed about how your data would be used.

True

False

# Chapter summary

---

**1**

Data privacy.

---

**2**

How the general data protection regulation protects your data.

---

**3**

Managing cookies.

---

**4**

Understanding the cloud.

**5**

Understanding how your data is stored in the cloud.

---

**6**

From this chapter you will have a working appreciation of privacy of mobile data.

---

# Chapter completed!

---

Congratulations! You have successfully completed this chapter!

## Summary of acquired skills

---

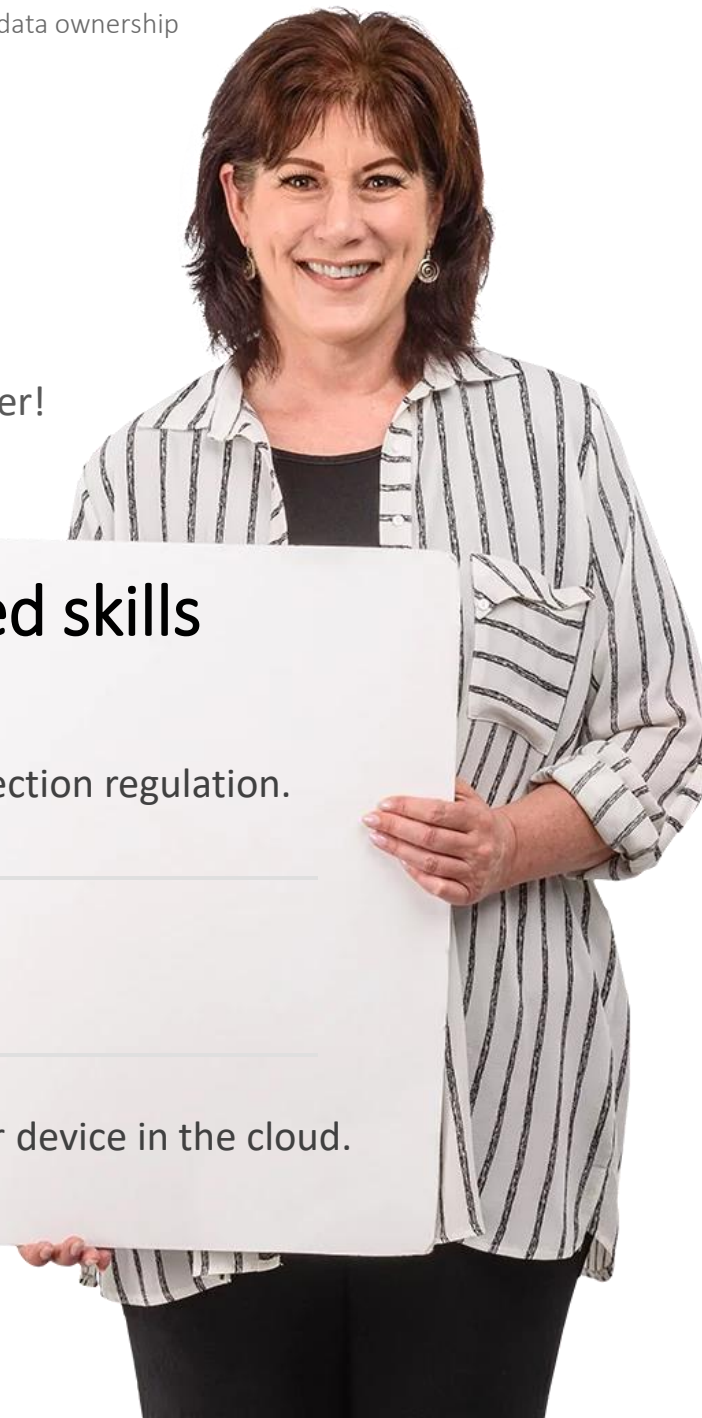
- 1** The general data protection regulation.

---

- 2** Managing cookies.

---

- 3** Storing data from your device in the cloud.



## What is next?

---

Now you can either repeat this chapter or follow our study recommendation by clicking on one of the buttons below:

[Restart](#)[Next](#)



SMART

MODULE 4

CHAPTER 2

## Authentication

In this chapter you will learn about authentication, which is the process of recognising a user's identity to grant access to services. Authentication technology supports safety and protection of personal information. Here you will learn types of authentication and of biometric approaches to authentication and how to create strong passwords.

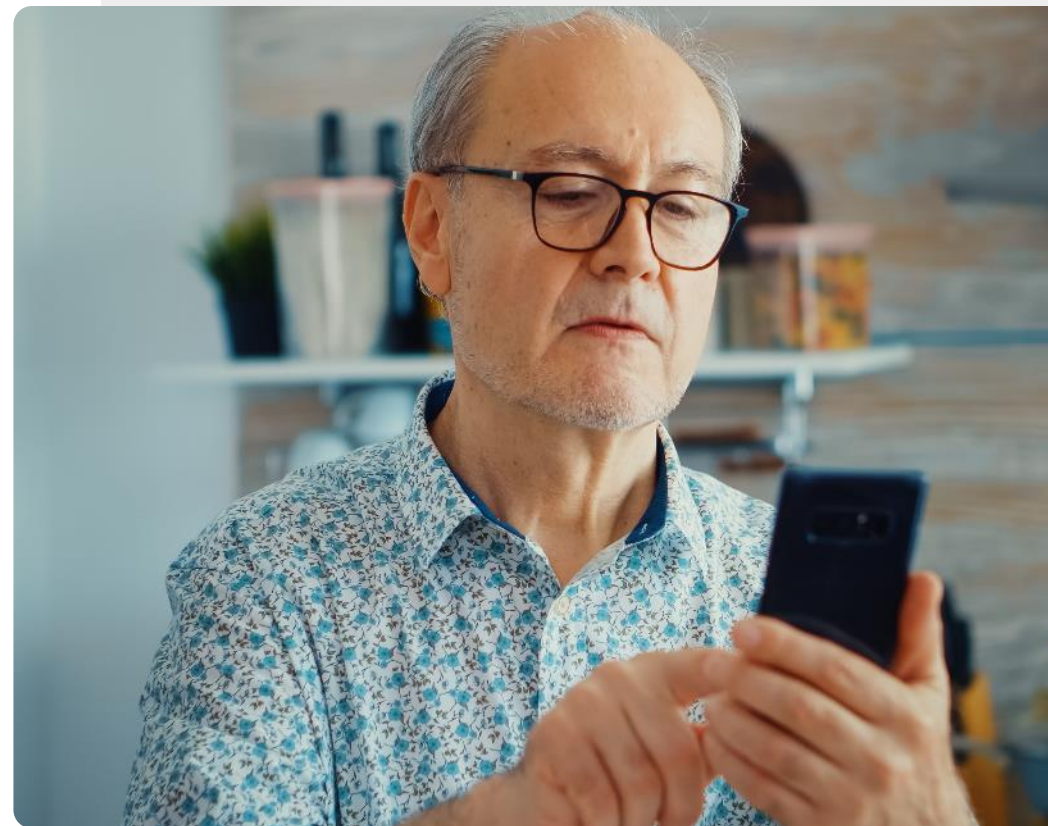
# Authentication – how devices know who the current user is

---

**Authentication** is the procedure of recognizing a user's identity. It often happens when an app is opened and validates users to make sure that some other user is not looking at their data.

Different systems require different information, called **credentials** to confirm an identity. This credential is often a password, but it can also involve other forms of authentication.

<https://www.veriff.com/blog/what-is-authentication>



# What will you learn in this chapter

- 1 What is authentication and why do you need it?
- 2 Types of authentication.
- 3 How to create strong password .
- 4 Different types of biometric authentication.



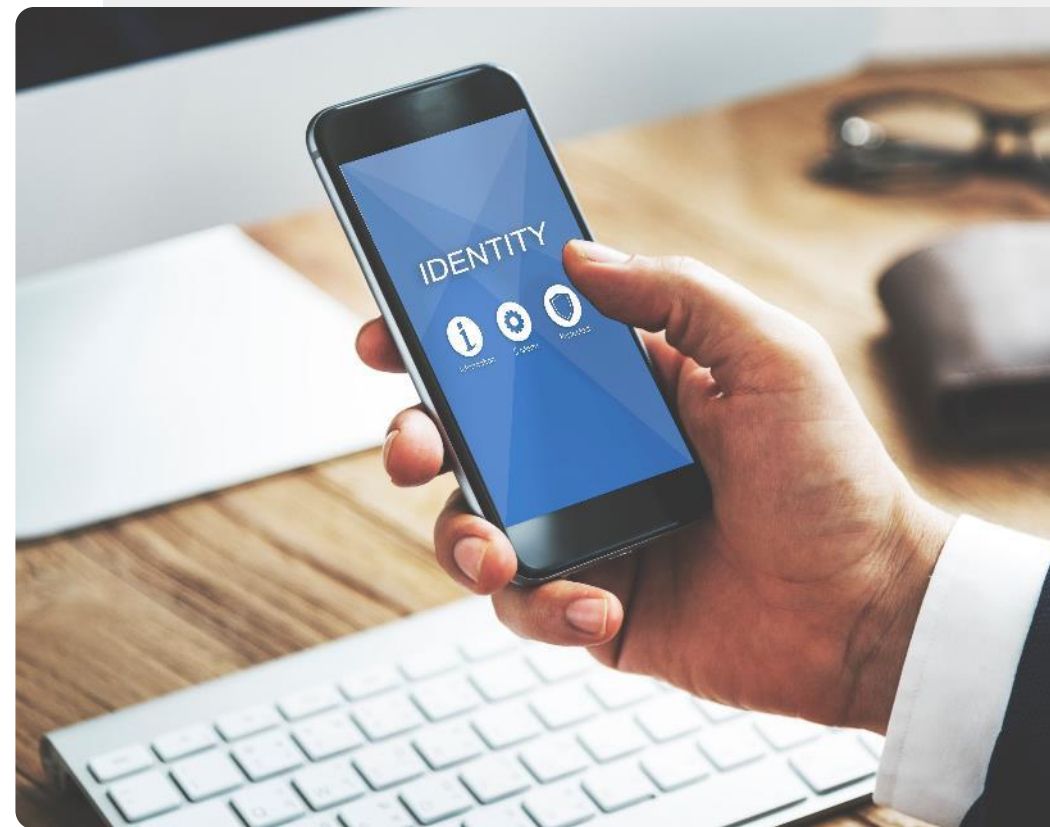


## Types of authentication

---

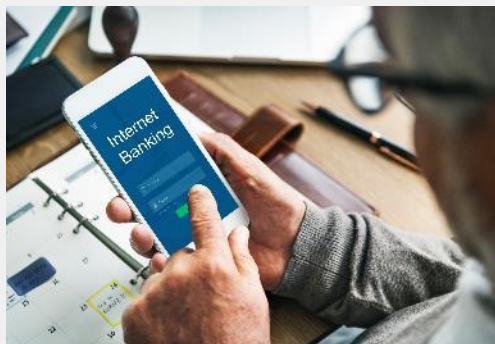
The number of ways to authenticate a mobile device user has expanded rapidly over recent decades.

Let's quickly review some of the main types of authentication that may be available on a mobile device.



# Some types of authentication

---

**1****2****3**

## Password based authentication

Passwords are probably the most common form of authentication. Secure passwords generally contain letters, numbers and other characters. This topic will be covered later in this chapter.

# Some types of authentication

---

1

2

3



## Certificate-based authentication

A digital certificate is an electronic document based on the idea of a driver's license or a passport. An example is the digital certificate which shows the full vaccination details for a COVID-19 vaccine.

# Some types of authentication

---

1

2

3



## Biometric authentication

Biometric authentication is a security process that relies on unique traits of the device owner such as face, voice or fingerprints. We will see that mobile devices support different types of biometric authentication approaches.

## Some types of authentication



### Token-based authentication

This approach allows users to enter credentials just once and creates a secret digital key – the **token**. The user can use the token just like this train ticket to access systems instead of entering credentials again.

## Some types of authentication



### Multi-factor authentication (MFA)

Once the user has been identified in one way, a code is sent to the mobile device for the user to enter in an app or website. This is **two factor authentication**.

## Password authentication

---

Let's select a couple of these types of authentication and look further into them.

Probably the most popular type of authentication, and the one that has been used on mobile devices for many years, is the password.

The password in the picture is an easy one to guess, so it is not very secure. Can we do better?



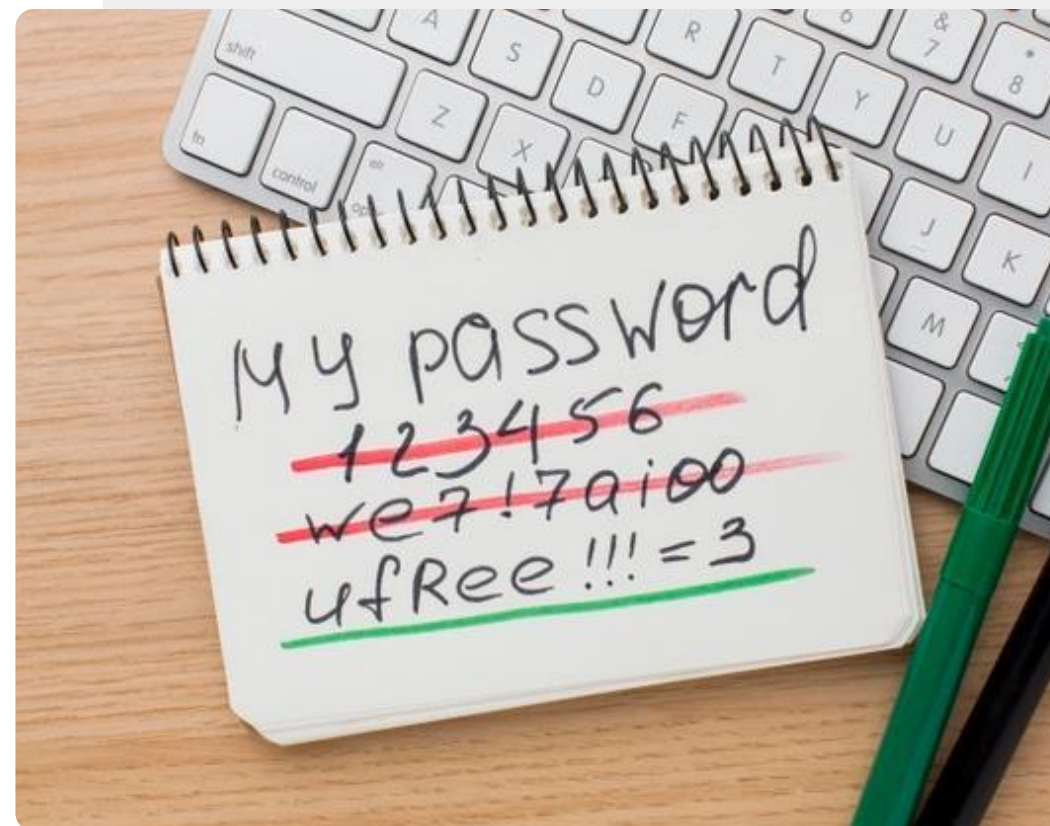
## Password authentication: stronger passwords

---

Many websites require that you select a password that has some of the following properties

- At least 8 characters long
- Contains capital and lower-case letters
- Contains a number
- Contains a punctuation character

Let's look now at how an easy-to-remember password can be made using these elements.





# Making a strong password

---

**1****2****3**

## Pick a word that you know

Take out a pen and a piece of paper. Write down a long word or words with strong meaning for you, but would not be obvious to anyone else. It could be “patience” or “Byzantium” or “antelope”.

# Making a strong password

---

1

2

3



Replace some characters in the word or phrase

Use character substitutions, for example:

1 = ! e = 3 a = @ 8 = % E = £ l = | S = \$ S = 5

C = ( T = + G = 6 O = 0 l = 1 Z = 2 B = 8

For example, **Caroline** could become **(@rol1nE**

# Making a strong password

---

1

2

3



**Use the password for a device or a website**

Now carefully destroy the password on the paper or put it in a very secure place such as a safe.

You can now enter the new strong password on a device or website.



## Protect your password

Once you have created your password, you need to protect it.

It is best to try to just remember it, but if you decide to write it down, it should be stored in a really safe place.

You should **NEVER** store a password anywhere with or near your phone.

## Do the task!

---

Antonio wants to make a secure password. How should he do it?



- ✓ Meet and get to know António. [You can find information about António here.](#)
- ✓ António chooses the phrase **nolimits** as the basic word for his password.
- ✓ Use the steps described to help António make a strong password from **nolimits** using this approach.

## Phone passwords and SIM codes

---

Mobile devices can be set up with **passwords** to protect files. **SIM cards** on a device connect it to a phone network and come with a **PIN code** that you enter to access the network. They give access to contacts on your SIM and if the device is stolen, the SIM can also be moved to another device to use your credit. If the PIN code is entered incorrectly 3 times, a second code called a **PUK code** is needed. For this reason, it is important to keep your PIN code and PUK code in a safe place once you get them with your device or SIM.



## Biometric authentication

---

We have mentioned that a biometric authentication system recognises unique features of the device user to allow them to access the device or system.

Let's review some of these approaches now.



# Biometric authentication for mobile technology

---

**1****2****3**

## Fingerprint scanners

Fingerprints are unique so they can be used to identify a user. Many modern mobile devices have fingerprint scanners built in, and the phone can be unlocked by the user placing their finger over the fingerprint scanner to unlock the phone.



# Biometric authentication for mobile technology

---

1

2

3



## Retina scan

Just like fingerprints, the patterns in the eye are unique to each person. The camera in some mobile devices can recognise the retina pattern of the owner and use it to unlock the device for the owner.

# Biometric authentication for mobile technology

---

1

2

3



## Facial recognition

Another similar user authentication approach is a facial scan. Again, a camera is used to recognise the unique facial characteristics of the device owner to unlock the device.



## Do the task!

---

Tom wishes to use authentication on his phone. Can you help him pick a suitable approach?

- ✓ Meet and get to know Tom. [You can find information about Tom here.](#)
- ✓ Tom used to work with an IT company, so he is a confident user of technology, but he is not familiar with modern authentication approaches. He would like to secure his smart phone, so that others cannot access his information.
- ✓ From the information you learned in the previous slides, provide TOM advice on which authentication approach he might wish to use.



## Authorisation



Once the device has authenticated the user, the user has **authorisation** (permission) to access the device or system.

A user may have authorisation to use all device features, or only some of them.

It is easy to mix up **authentication**, which identifies the user, and **authorisation**, which happens after.

# Quiz

Click the **Quiz** button to edit this object

 **SMART** **MODULE 4** **CHAPTER 2** Authentication

Authentication is designed to protect your data.

- True
- False

# Chapter summary

---

**1**

You have learnt about authentication and how it is used to protect your access and information.

---

**2**

You have seen a number of types of authentication.

---

**3**

You have learnt how to create and remember your passwords.

---

**4**

Please, try out the security features of your mobile device. They will protect it.

**5**

We hope that you will practice the password creation technique to create secure passwords.

---

# Chapter completed!

---

Congratulations! You have successfully completed this chapter!

## Summary of acquired skills

---

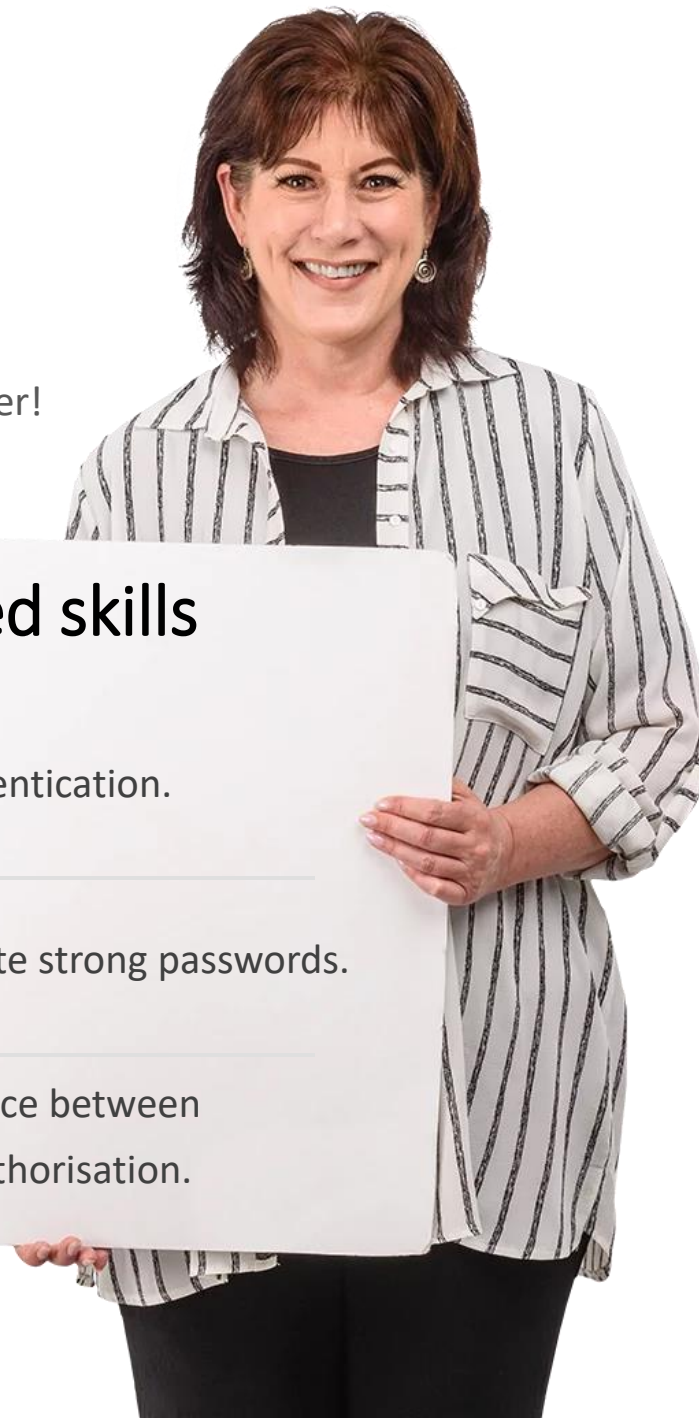
- 1** You learnt about authentication.

---

- 2** You know how to create strong passwords.

---

- 3** You learnt the difference between authentication and authorisation.



## What is next?

---

Now you can either repeat this chapter or follow our study recommendation by clicking on one of the buttons below:

[Restart](#)[Next](#)





SMART

MODULE 4

CHAPTER 3

## Protecting a mobile device

In the physical world your possessions, including your mobile device, can be robbed. In the digital world your device is also vulnerable to hacks and viruses. This chapter is about how to protect your smartphone, privacy and information from cyber attacks, such as viruses.

# What will you learn in this chapter

---

- 1 How to protect your devices from unauthorised access.
- 2 How to protect your devices from viruses.
- 3 About ransomware, malware and DDoS.
- 4 How to use a hot spot safely.



# How to protect a mobile device from unauthorised access

---

**1****2****3**

## Lock your mobile device

Lock your mobile device with passwords or even better, with biometric authentication switched on. Lock your SIM using a PIN code and keep your PIN and PUK codes in an easy to remember but safe location.

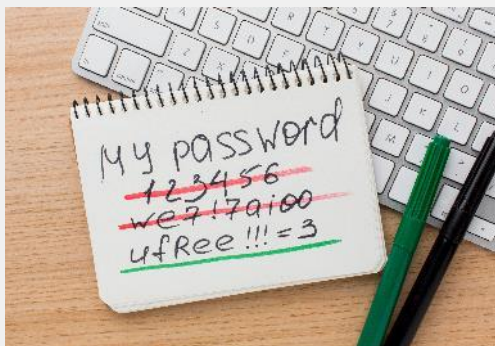
# How to protect a mobile device from unauthorised access

---

1

2

3



## Use strong passwords

In the last chapter you learnt to create and use passwords that are strong, with upper and lowercase letters, numbers and special characters. It is worth sitting down with a pen and paper to do this.

# How to protect a mobile device from unauthorised access

---

1

2

3



## Watch your downloads

Only download files, like documents, videos, music or images, from websites that you trust, such as device makers, big software companies or media companies. Some files that are downloaded from untrusted sites can contain viruses and damage your hardware. Websites with addresses that begin with **https**, protect against this.

DATA LEAK

1

2

3

EXPLOIT FOUND

VIRUS DETECT



## What are viruses?

Viruses are self-replicating programs that are spread from one device to another through e-mail links and malicious downloads.

# How to protect a mobile device from unauthorised access

---

4

5

6



## Keep the device up-to-date with software updates

The mobile device maker will send notifications about new software updates. Updates help protect a device from security flaws that could allow someone to take data from your device. Download these software updates onto the device and update it.

# How to protect a mobile device from unauthorised access

4

5

6



## Encrypt the data on the mobile device

Most mobile devices have an option to encrypt your data. If a phone gets stolen, encryption will make it more difficult for someone without authorisation to see the data stored on the device. An authorised user will be able to use the device as normal.





4

5

6

## What is encryption?

Encryption is the method by which information is converted into unreadable codes that hide the information's true meaning except from the user who has the key.

Facebook's social media App WhatsApp has end-to-end encryption so that the communication between two users cannot be 'listened to' by another person.

# How to protect a mobile device from unauthorised access

4

5

6



## Be careful of public Wi-Fi

Wi-Fi in public spaces like airports and cafes can be risky. Sometimes, what you think is the Wi-Fi of the café is actually the laptop of a hacker who can use the connection to your phone for improper purposes. If in doubt, don't connect!



## Wi-Fi and crime

Cybercriminals sometimes spy on public Wi-Fi networks and collect data that is transferred by Wi-Fi.

In this way, the criminal can get bank details, passwords and other sensitive information.

## Pros and cons: use public Wi-Fi or not?

---



### Advantages

- Free
- Your mobile data allowance is not used
- Easy to connect
- Available



### Disadvantages

- Not secure
- Wi-Fi of an organisation's "hot spot" could be faked
- Usually, less speed than your own mobile coverage



## What is a hack attack?

The purpose of a hack attack is to gain access for mischief, theft of data or intent to destroy an organisation's data.

# Malware, Ransomware, DDoS

---

*“Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, wiper and scareware” (Source: <https://en.wikipedia.org/wiki/Malware>)*

*“Ransomware is a type of malware that prevents the victim from accessing many files on their computer. It is usually downloaded via a link in an email, on a website or on social media. Once downloaded, it encrypts all data files on the computer and a blocking screen then appears, demanding a ransom payment to allow the files to be released. **DO NOT** click links in suspicious texts or emails!” (Source: <https://www.bankofireland.com/security-zone/protect-your-business/ransomware/>)*

*“DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack. By utilizing specially designed network equipment or a cloud-based protection service, a targeted victim is able to mitigate the incoming threat.”. (Source: <https://www.cloudflare.com/en-gb/learning/ddos/ddos-mitigation/>)*

## Do the task!

---



Tom has added authentication to his phone. Can you suggest other ways to protect his information?



- ✓ Meet and get to know Tom. [You can find information about Tom here.](#)
- ✓ Tom used to work with an IT company, so he is a confident user of technology. He is now using authentication but wishes to use his smart phone in a secure way so that others cannot access his information.
- ✓ From the information you learned in the previous slides suggest other actions that Tom can take to protect his information.

# Quiz

Click the **Quiz** button to edit this object

  **SMART** **MODULE 4** **CHAPTER 3** Protecting a mobile device

A DDoS a cyber-attack occurs when a person tries to disrupt the normal traffic of a targeted server.

True

False



# Chapter summary

---

**1**

You have learnt how to protect a mobile device.

---

**2**

You have learnt the difference between viruses and hack attacks.

---

**3**

You have learnt about ransomware, malware and DDoS.

---

**4**

You are aware of the hazards of using public Wi-Fi.

# Chapter completed!

---

Congratulations! You have successfully completed this chapter!

## Summary of acquired skills

---

1

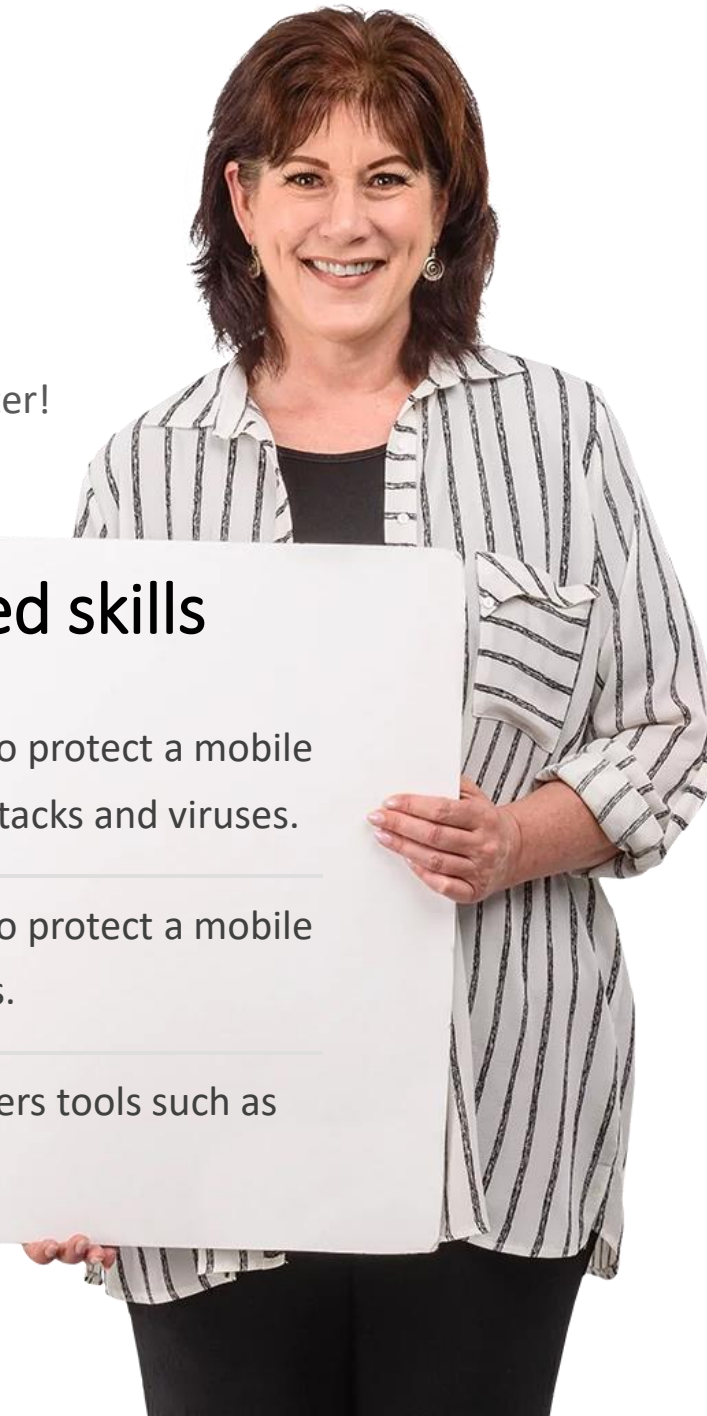
You have learnt how to protect a mobile device against hack attacks and viruses.

2

You have learnt how to protect a mobile device in public places.

3

You learnt about hackers tools such as malware.



## What is next?

---

Now you can either repeat this chapter or follow our study recommendation by clicking on one of the buttons below:

[Restart](#)[Next](#)



CYBER BULLYING



SMART

MODULE 4

CHAPTER 4

## Cyberbullying and dealing with inappropriate content

What should you do if you become a target of cyberbullying? If people do not see the person, it's easier not to realise the harm that is done by cyberbullying. In this chapter we will review human aspects of digital communication and what is appropriate or not to share online.

# What will you learn in this chapter

---

- 1 To be aware of cyberbullying.
- 2 How to deal with inappropriate content.
- 3 What to share or not online.
- 4 Friends online: how safe it is?



## What is cyberbullying?

---

Cyberbullying is defined as *an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend himself or herself.* - Smith 2018

Cyberbullying is usually said to involve three elements:

1. intent to harm
2. imbalance of power
3. repetition of the act



## Types of cyberbullying

---

Cyberbullying can happen through text messages, phone calls, e-mails, instant messengers, social media platforms, or in chat rooms.

It can take the form of hurtful words, derogatory comments, posting fake information on public forums or blogs, hacking accounts for personal threats of a violent or sexual nature.

– Rao 2018



## How to deal with cyberbullying

---

According to experts there are a number of ways to deal with a cyber bully.

**Ignore:** Where possible, ignore and cut-off the bully.

**Record:** Keep a note of the time, date and content of all bullying content, so that you can report it if you need to.

**Support of friends:** share your experience with friends and relatives, so you don't feel isolated.

**Report:** Contact the moderator of the site or board.





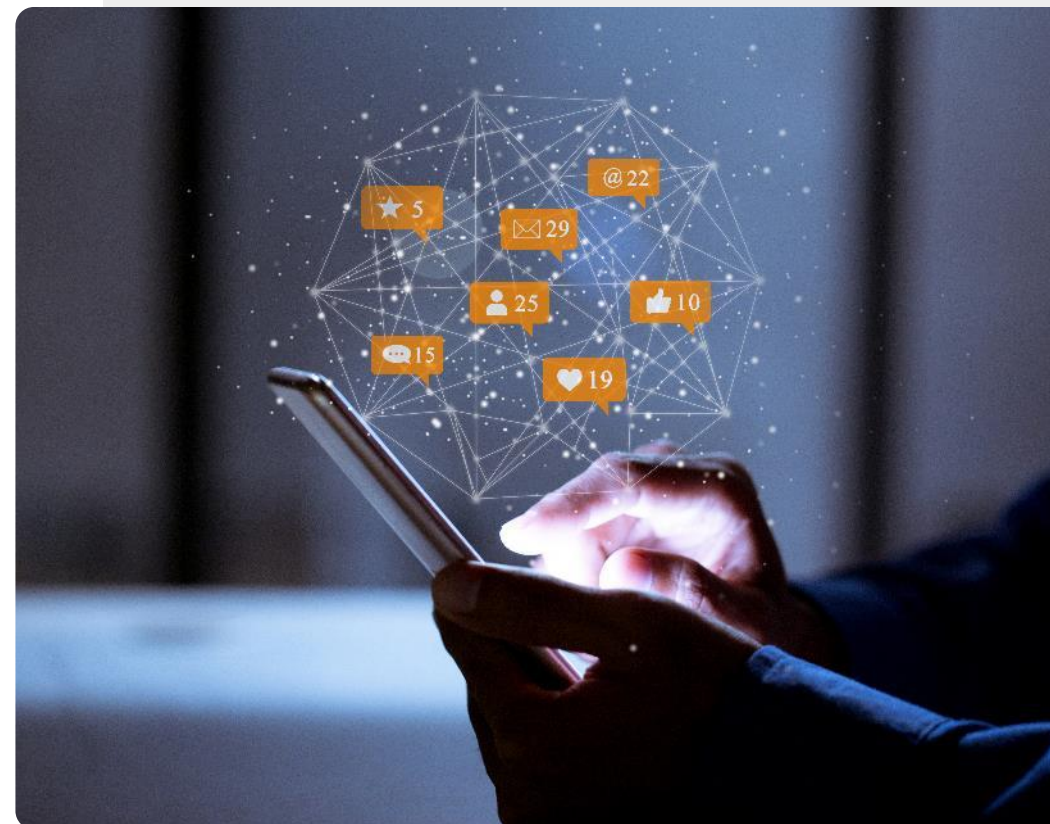
## Sharing personal information on social media

When you share information on social media, you should assume that it will be there for a long time. Think about whether your post will cause problems.

*“While it may seem like the information is being shared with only your friends and family, it can also be shared with hackers and scammers who troll the social media sites”.*

*“Once your data is in the wild, it stays in the wild and can be used by any number of unscrupulous characters.”*

Joseph Turow – Penn State



## Where to report cyberbullying

---

Your service provider or social media network can help you to block unwanted messages and calls.

If the situation is more serious, the local police can investigate threatening communications.



## Removing online identities

---

On social media apps you can often change your profile, so that it is not visible to the general public.

It may not always be possible to delete your social media or internet forum posts, but you can delete your identity, so that those posts become anonymous.

In some cases, you can send a request to a **search engine**, such as Google, so that your data does not appear in searches.



## Have you been pwned?

---

If someone gets access to your e-mail or social media account, they can use it to send fake mails to your contact and cause other mischief. This is called **pwning** (pronounced *pawning*).

One way that this can happen is when a large data breach for an online service includes your password. If you use the same password for different accounts, such as e-mail, then your account could be hacked.

<https://haveibeenpwned.com/>



## Choose your online friends carefully

---

Choosing online friends: cross check the information you received from “new” friends.

Do not share your personal information, make neutral conversations.

Do not lend money to any “new” friend.

A real friend will be interested to know your interests and not use you to solve their problems.



# Making new friends online

---



## Advantages

- You can connect with people all over the world.
- You can discover many more friends who share your interests online than in a local community.
- Online chats can be easier than in person.
- You can close your account if something goes wrong.



## Disadvantages

- You may prefer to communication in person, the distance might be a problem.
- You have to be careful not to disclose personal information to a stranger. Their ID could be false.
- It's easier for people to offend online, when they do not see the other person.

## What is inappropriate content?

---

Inappropriate content includes footage of “*terror attacks, beheadings and bombings; cruelty to humans and animals; self-harm sites; pro-anorexia and eating disorder content; pro-suicide content; sexual abuse and rape; violence and distressing content; hate sites; online porn*”.

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/>

In Internet slang, a person who posts inappropriate content with the intent of provoking or insulting other readers is called a **troll**.



## Dealing with inappropriate content

---

Most search providers have features to support this. For example, Google's SafeSearch is located at <https://www.google.com/preferences>.

It's the first thing on the page. Open that page and click on the icon located adjacent to 'Turn on SafeSearch.'

You can also choose to lock SafeSearch, and Google will block both texts on adult websites and images associated with these sites.

<https://www.dragonblogger.com/how-to-block-inappropriate-content-on-google/>







## Do the task!



---

Teresa is upset about a cyberbullying incident. Can you help her?

- ✓ Meet and get to know Teresa. [You can find information about Teresa here.](#)
- ✓ Teresa uses technology to keep in contact with her friends, but recently she was affected by cyberbullying. So far, it is not a serious case, but still, she would like to know how to handle it – especially if it continues.
- ✓ From the information you learned in the previous slides, provide Teresa advice on how to deal with cyberbullying.
- ✓ If the cyberbullying gets more serious, whom should Teresa contact?

# Quiz

Click the **Quiz** button to edit this object

  **SMART** | **MODULE 4** | **CHAPTER 4** | Cyberbullying and dealing with inappropriate content

Which elements that normally apply for cyberbullying? (tick three elements):

- It is someone you know
- the act is repeated
- intent to harm
- Imbalance of power

# Chapter summary

---

**1**

You learnt about cyberbullying, how to recognise it and report it.

---

**2**

You learnt about inappropriate content and how to block it.

---

**3**

You learnt how to be safe when meeting new friends online.

---

**4**

You learnt to be careful about sharing data online - once posted, it is difficult to remove it.

**5**

If you don't like something: you can block it, report it or close your account.

---

# Chapter completed!

---

Congratulations! You have successfully completed this chapter!

## Summary of acquired skills

---

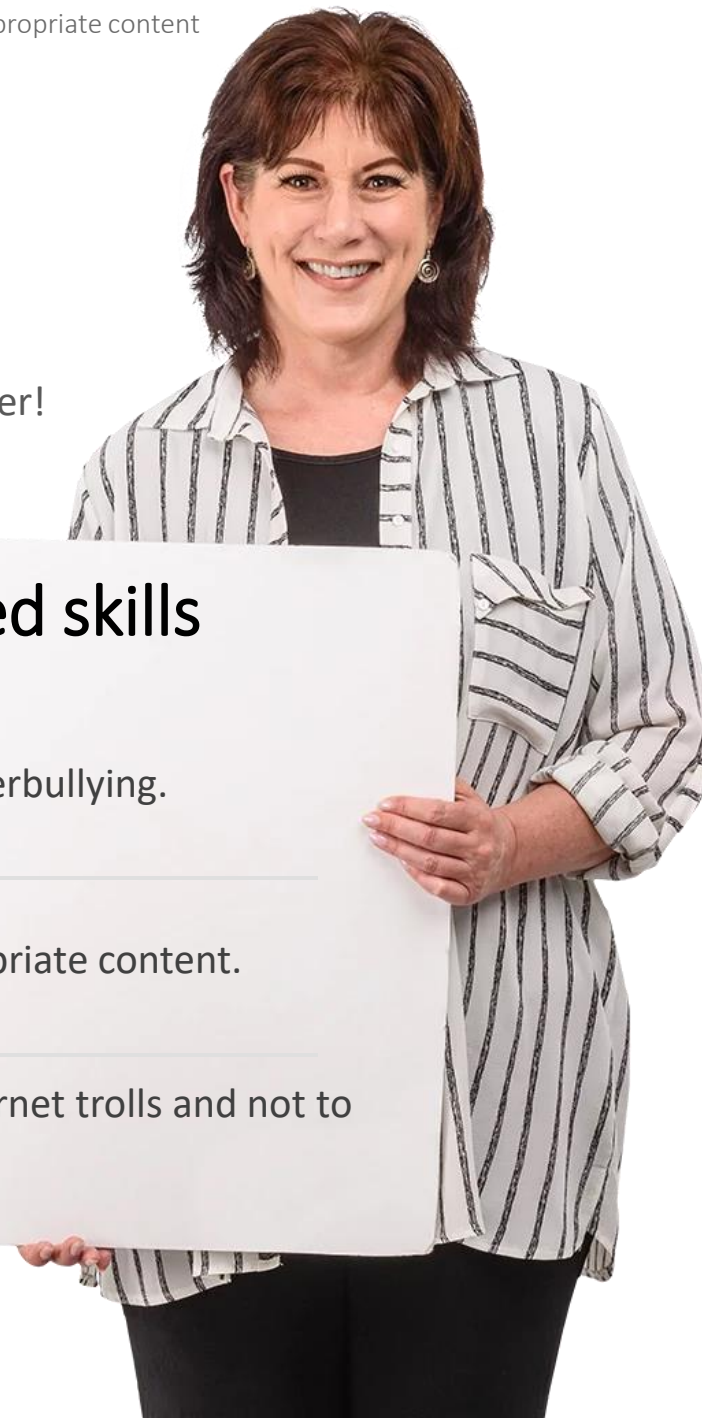
- 1** How to recognise cyberbullying.

---

- 2** How to block inappropriate content.

---

- 3** How to recognise internet trolls and not to fall into the trap.



## What is next?

---

Now you can either repeat this chapter or follow our study recommendation by clicking on one of the buttons below:

[Restart](#)[Next](#)

# Module summary

---

**1** You learnt about mobile phone security.

---

**2** You learnt about General Data Protection Regulation, GDPR.

---

**3** You learnt about types of authentication.

---

**4** You learnt how to create strong passwords.

**5** You learnt about the tools of hack attacks: malware, ransomware, DDoS.

---

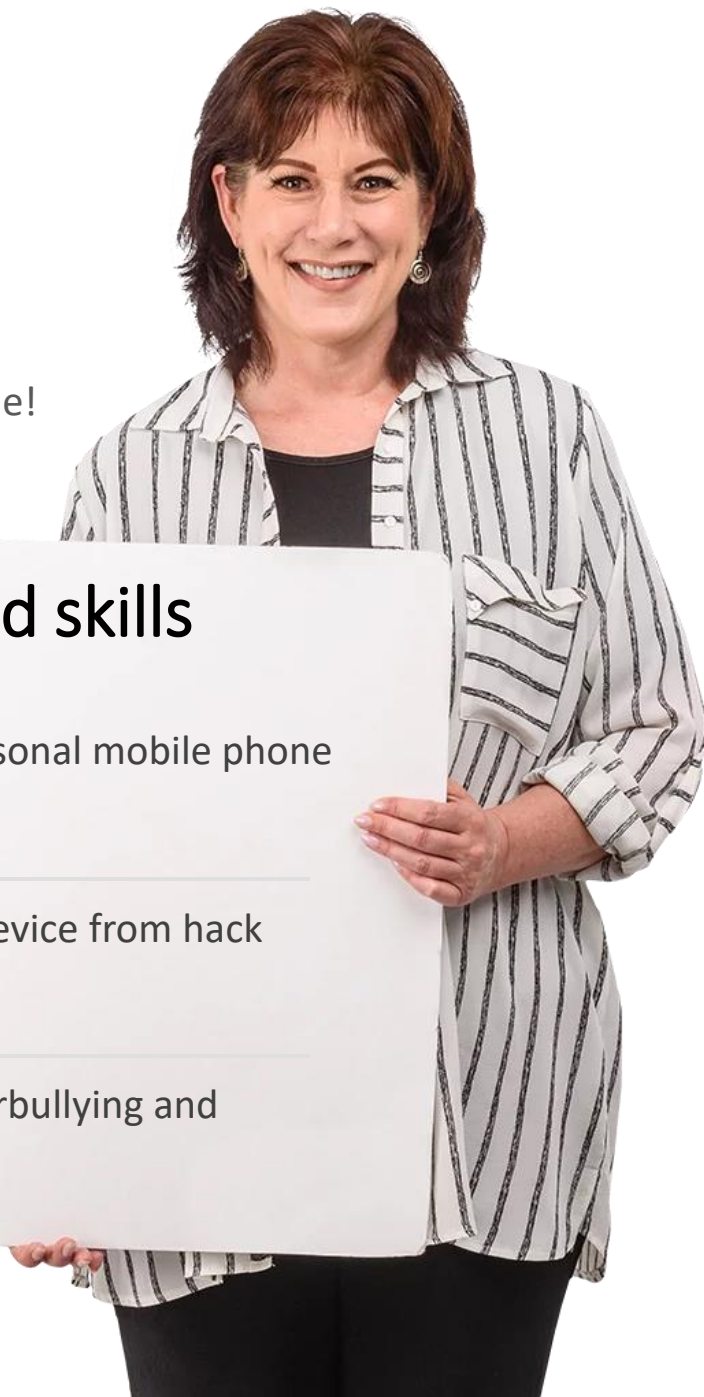
**6** You learnt about cyberbullying and how not to become a victim.

---

**7** You learnt how to adjust Google's SafeSearch settings to prevent inappropriate content.

# Module completed!

Congratulations! You have successfully completed this module!



## Summary of acquired skills

- 1 You learned about personal mobile phone security and GDPR.
- 2 How to protect your device from hack attacks and viruses.
- 3 How to deal with cyberbullying and inappropriate content.

# What is next?

---

Now you can either repeat this module or follow our study recommendation by clicking on one of the buttons below:

[Restart](#)

[Next](#)

