How to use the internet safely

VODA

Keep your system up to date

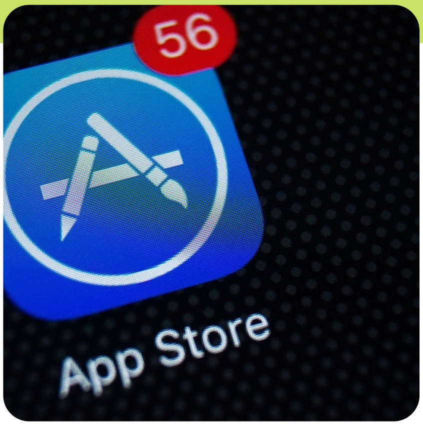
Malware is software intentionally designed to cause damage to a computer.

You can protect your system installing an **anti-malware** software.
Most computer come with anti-malware software already pre-installed, like Microsoft Defender.

Automatic updates allow users to keep their softwares updated without having to do it manually. It is a good idea to activate automatic updates for your anti-malware and operating system.
Updates not only bring new features but also security fixes.

VODA

Only download apps from the app store

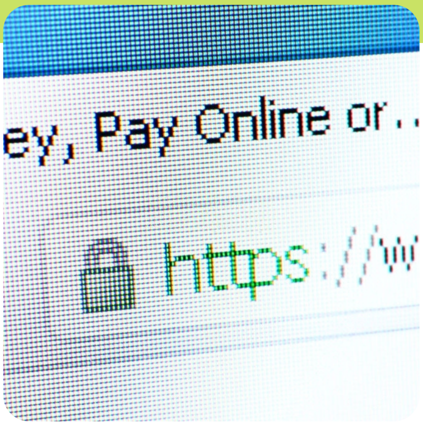


Digital distribution services, commonly known as **app stores**, are pre-installed on your devices. They allow to download new software.
Examples are Microsoft Store on Windows, App Store on iOS and Google Play on Android.

It is strongly recommended to only download software from the app stores, as apps go through a thorough testing and verification that they are free of any malware.

VODA

Only browse secure websites



Websites that have an address starting with **https** prevent malicious users from being able to intercept the data you share. They may also be marked by a padlock icon next to the address bar.

Choose only secure websites, especially when you are making online purchases and sharing sensitive information.

Check also that the website's address seems to be genuine by looking for **subtle misspellings**, extra words, characters or numbers or a completely different name from that you would expect.

VODA

Choose strong passwords

Passwords are like keys that help you protect your information online.

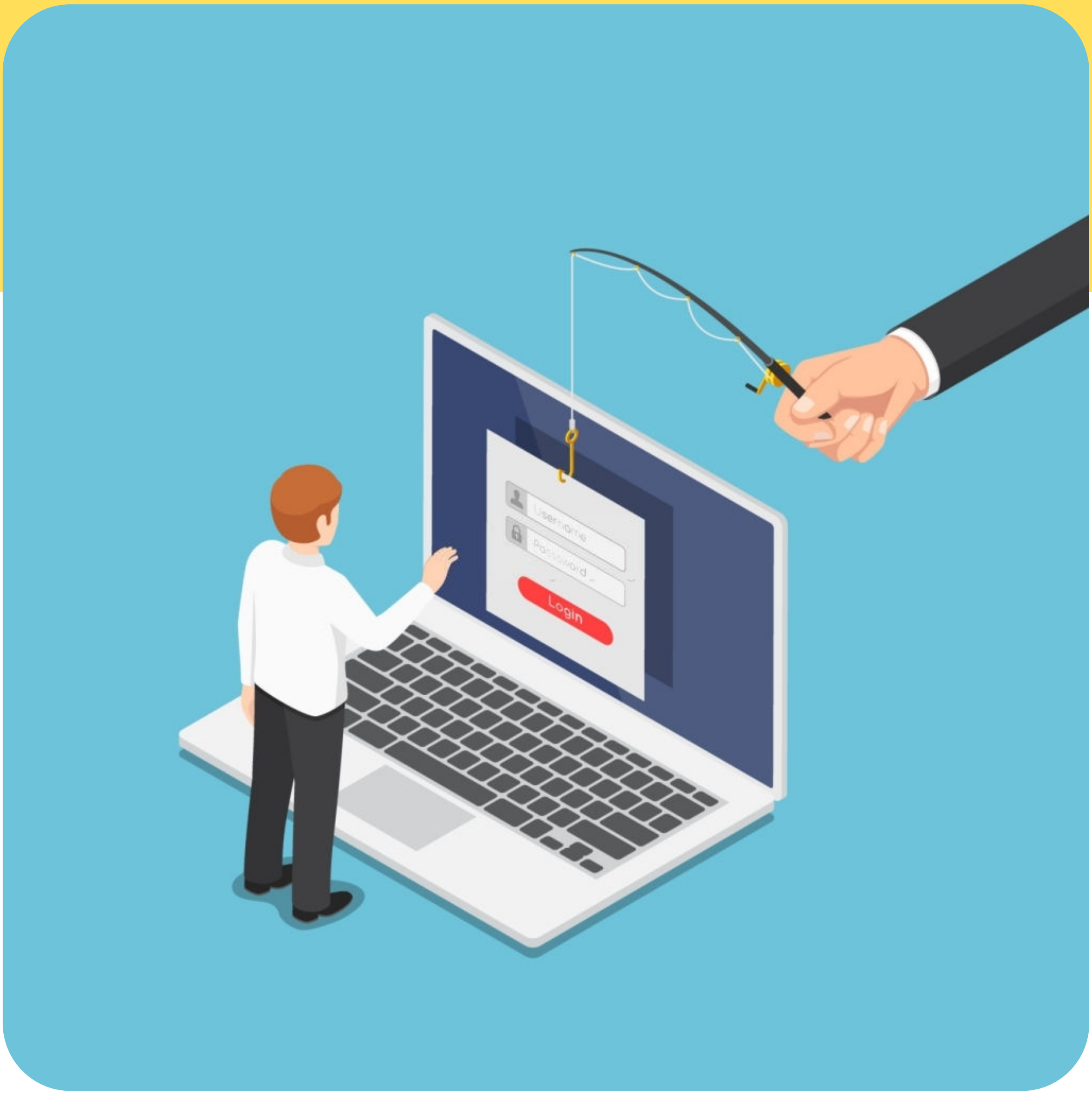
A good password is easy to remember but hard for someone else to guess.
They should not contain personal information like your date of birth or common words because it might be too easy for someone to guess.

It's a good idea to use at least 8 characters, mixing lowercase and uppercase letters, digits and special characters.

Use a **different password** for each website.

VODA

How to be aware of cyber scams



VODA

Know what phishing is

Phishing is when scammers send you an email pretending to be someone you know or a company that you recognise, with the goal to obtain your personal or financial information.
The bogus emails might ask you to reply, open an attachment or may contain an url to redirect you to a fake website.

Scam emails can look genuine and appear to be from official places, like your bank.
To distinguish between legit and fake emails look out for errors in the spelling or grammar. In addition, genuine organisations will never ask for your password or bank details.

If you see a suspicious email, do not open any links or attachments and delete it straight away.
If you are in doubt, **phone** the organisation directly using the phone number found on their official website and ask them.

VODA

Fake websites

Scammers create **fake websites** which look official, requesting you to provide login information.
To make sure you are on your bank's real website type their official web address in your internet browser. You can find this on letters from the bank.

Other websites may offer to help you apply for a passport renewal or a new driving licence. Although they are not illegal, these websites charge **extra money** if you use them, rather than going directly through the official government department where the service is free of charge.
If you aren't sure about which website to use for a government service, go through **GOV.UK**, the Government's official website, to find what you need.

VODA

Relationship scams

Scammers can use social networks or dating websites and connect with you. Once they have gained your trust they will start **asking for money**, often by telling you an emotional or hard luck story.
These tricks are hard to spot, so it is always worth talking to a friend or relative about it, especially if things seem to be moving fast.

Be careful if the person wants to move away from the social network or the dating site to communicate by email or text message.
Never send the person money or give them your account details. If you arrange to meet, make sure it is in a public place, **tell someone else** where you are going and do not give away information too quickly.

VODA

Health scams

False and misleading claims may be made about medical-related products, such as **miracle health cures**.

Fake online pharmacies may offer medicines cheaply. However, the actual medicine delivered to you can turn out to be poor quality and even harmful to your health.

Legitimate online pharmacies must show on their website's homepage a 'Registered Pharmacy' logo. Clicking on this should lead to the **General Pharmaceutical Council** website.

How to share information about yourself

VODA

Always know who you are talking to

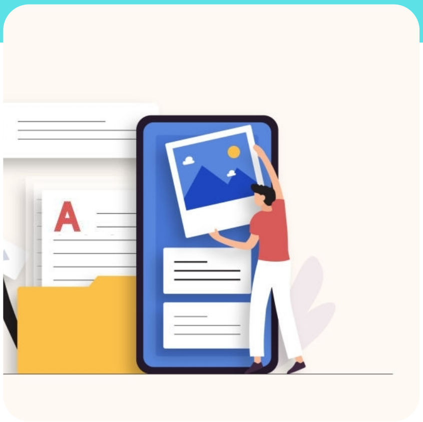
Social networks allow you to communicate with friends and relatives.

Avoid sharing personal information with **strangers**.
Do not accept friend requests from people you do not know.

The people you are friend with can see any personal information you share.

VODA

Be careful of what you post



Any comment or image you post online may stay online **forever** because removing the original does not remove any copies that other people made.
There is no way for you to "take back" a comment you wish you had not made or get rid of an embarrassing photo.

It is not a good idea to post personal details like email address, home address, phone number and date of birth.

Do not write on social networks things you would not tell to a stranger.

Check and edit your **privacy settings** on social networks to control who can see the things you share.

VODA

Your digital footprint

Your **digital footprint** is everything on the internet about you:

- The things you say on social networks or the things people say about you
- The photos you share
- Your personal interests
- Reviews you leave about something you bought or a place you visited

It is important to think about what you want other people to know about you.

VODA

Avoid sharing your location

Sharing your **current location** or pictures could potentially lead to dangerous situations.

Scammers or burglars could be monitoring popular venues on social media for potential targets.

Do not make your holiday plans public and check who can see the events you would like to attend.

VODA

VODA