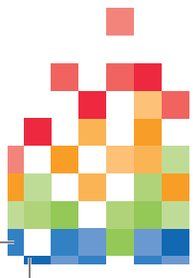
STAYING SAFE ONLINE

Simple steps to staying safe online

By wearedigital



Contents

Introduction

The Internet has changed the way we live, work and communicate e.g. better communication; greater access to information which enables us to widen our knowledge and expand our learning; work from home and banking and shopping online. Whether we like it or not – it's here to stay.

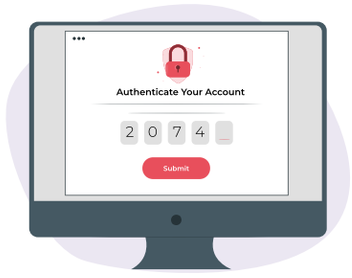
However, the Internet has a dark side.

Unfortunately, some people abuse these online services and use them to exploit others. And it's important that we are aware of these dangers to prevent being exploited online.

This leaflet will help you do just that.

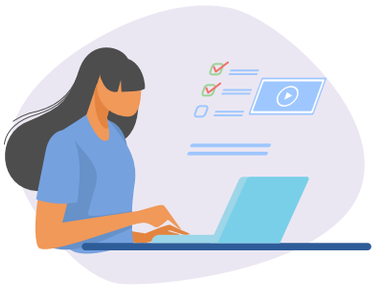
In it, we'll cover some crucial elements of online security, including:

Keeping your accounts & passwords safe

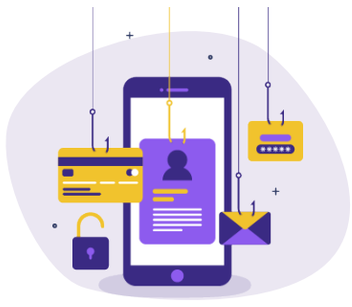


Multi factor authentication

Setting safe & secure passwords

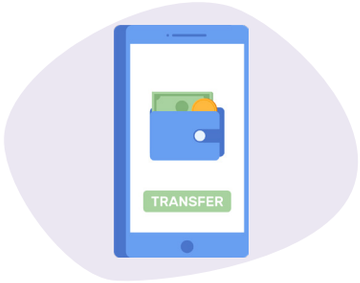


Browsing the internet safely



Avoiding phising attacks

Using social media safely



Using online banking safely

Accounts & Passwords

In order to access most online services, you'll need to set up an account to prove you are who you say you are and to keep your information safe.

You will first need to select a **username** to sign in (you can often choose this yourself or use your main email address).

Secondly, in order to keep your account secure, you will be asked to set up a password.

When setting up a password, it's important to keep these things in mind to protect your data:

Do not use personal information that is common knowledge to those around you, such as your surname or the name of your pet

Never tell anyone your password

Don't use the same password for different companies or products. If a company is hacked, the passwords are often sold on and hackers can try these on other systems

Put a special character in your password. Such as '*', to make it more difficult to guess

Fun fact: The UK National Cyber Security Centre found 3 million user accounts had the word 'Password' as their password. Not something we'd recommend if you're trying to keep hackers out of your accounts.

Creating a complex password:

Rather than using one word, try using a phrase or three random words that only mean something to you e.g.

wPlane*CarFilm60

Or use a unique random generated password such as

snY6mW*5

(you likely won't remember it, but you can use a password manager to allow secure use without needing to. More on this later)

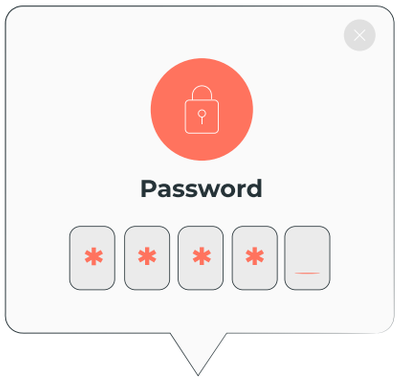
If you can't use complex passwords for all your accounts, it's a good idea to make sure you have more difficult passwords for your most important accounts, such as:

- **Online banking account**
- **Any account you make payments from** (e.g., PayPal, Amazon)
- **Your main email account** because if someone gets access to this account, they can often reset the password to any accounts linked to the email address

Multi Factor Authentication

Multi-factor authentication (MFA), otherwise known as two-factor authentication (2FA) is a simple way of adding an extra layer of security to your accounts online.

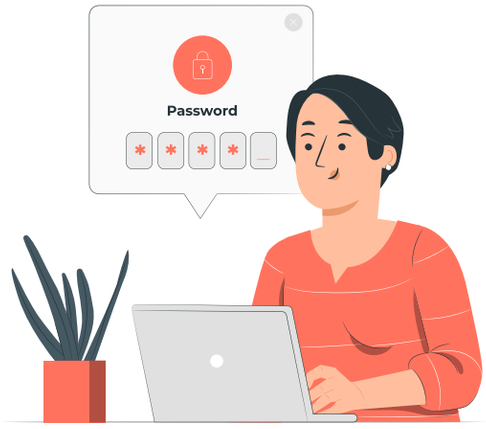
It's actually quite a simple idea, meaning that in order to sign into an account you use two things:



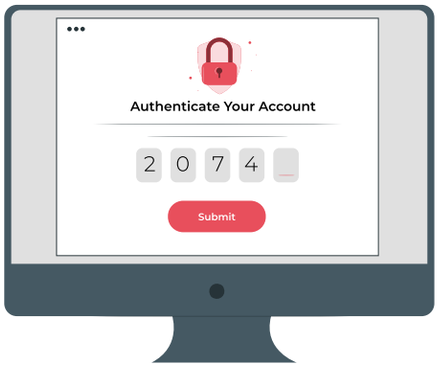
Something you know
(usually a password)

Something you physically have on you
(usually a phone)

When you log onto an important service such as your bank account or main email from a new device with 2FA, you will need to:



Know your password



Be able to enter a unique code sent to your phone

Meaning, unless you're the account holder, or somehow a hacker managed to get hold of your password and your phone – there's no chance of gaining access to the account.

We would strongly recommend using 2FA/MFA whenever you can. Especially on your more important accounts like your bank, main email and PayPal account.

Further advice on setting up two-factor authentication can be found on National Cyber Security Centre website here:
https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

Password Managers

For extra security on your accounts, we recommend using password managers.

Password managers allow you to save all of your passwords on your phone behind one extremely strong password. Meaning you only need to remember one password in order to access them all.

While password managers are a great way to optimise your account security, if you happen to forget or lose your main password, retrieving all of the others hidden behind it can be a difficult task.
Some of the best-rated free password managers on the market right now include LastPass and Norton Password Manager.

LastPass •••|

Norton™

More information on password managers can be found here:
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

Protecting Devices

As well as protecting your accounts, it's important that you protect all of your devices too. This could be your phone, tablet, or PC.

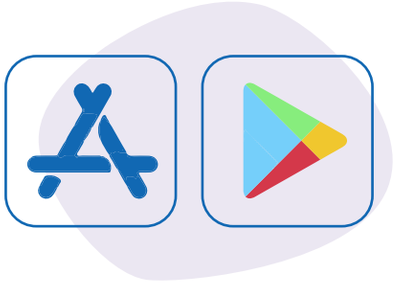
Protecting your device doesn't take much. But you'll be grateful you had precautions in place if something were to happen to it.

Some common ways include:

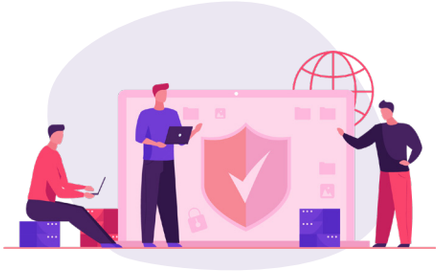
Protect it with PIN or password

Set it to auto-lock after a inactivity

Make sure the device has the latest software



Only download apps from reputable app stores



Install a trusted antivirus software

There are other ways to ensure you're keeping your information safe online, such as:

Avoiding public Wi-Fi Networks

These are Wi-Fi networks or hotspots that you can use in public places such as coffee shops, hotels and libraries.

It's a good idea to avoid these open networks where possible, as connecting to them could make you more vulnerable to threats.

Avoid opening any accounts with sensitive information on these Wi-Fi networks, such as online banking. If you really need to use a public Wi-Fi network, it's a good idea to install a VPN (Virtual Private Network) that protects your communication.

NOTE: A VPN creates a secure link across the Internet, protecting you from some of the risks when working using Public Wi-Fi Networks.

Backup all important files on your device

It's important to always backup your work. Daily if possible. If your device gets lost or stolen, you'll thank yourself for having made copies of everything so you can easily access your files from another device.

Cloud systems are another great way to ensure all of your data is protected if something was to happen to your device. 'The Cloud' is essentially a huge computer that stores large amounts of data.

When you create an account, you can upload files, data and any private information securely and access it from any device in the world (so long as you gave your login details) meaning you can always be confident that your data is safe if something were to happen unexpectedly.

Backups will also be our best form of protection against a Ransomware attack a very nasty form of malware

Be cautious when using shared devices

Using a shared device, for example a computer at a nearby library, can pose numerous threats to your accounts and personal information.

To keep your accounts and information secure, only use them in a location you trust and always log out before you leave. Also, never save your passwords on the device and avoid doing any sensitive work (i.e., online banking).

Safe Web Browsing

While most websites are safe, hackers can set up fake websites to trick us into entering information and use them to download viruses and malware onto our devices. So, it's important we are aware of what these dangers can look like to prevent us from being attacked.

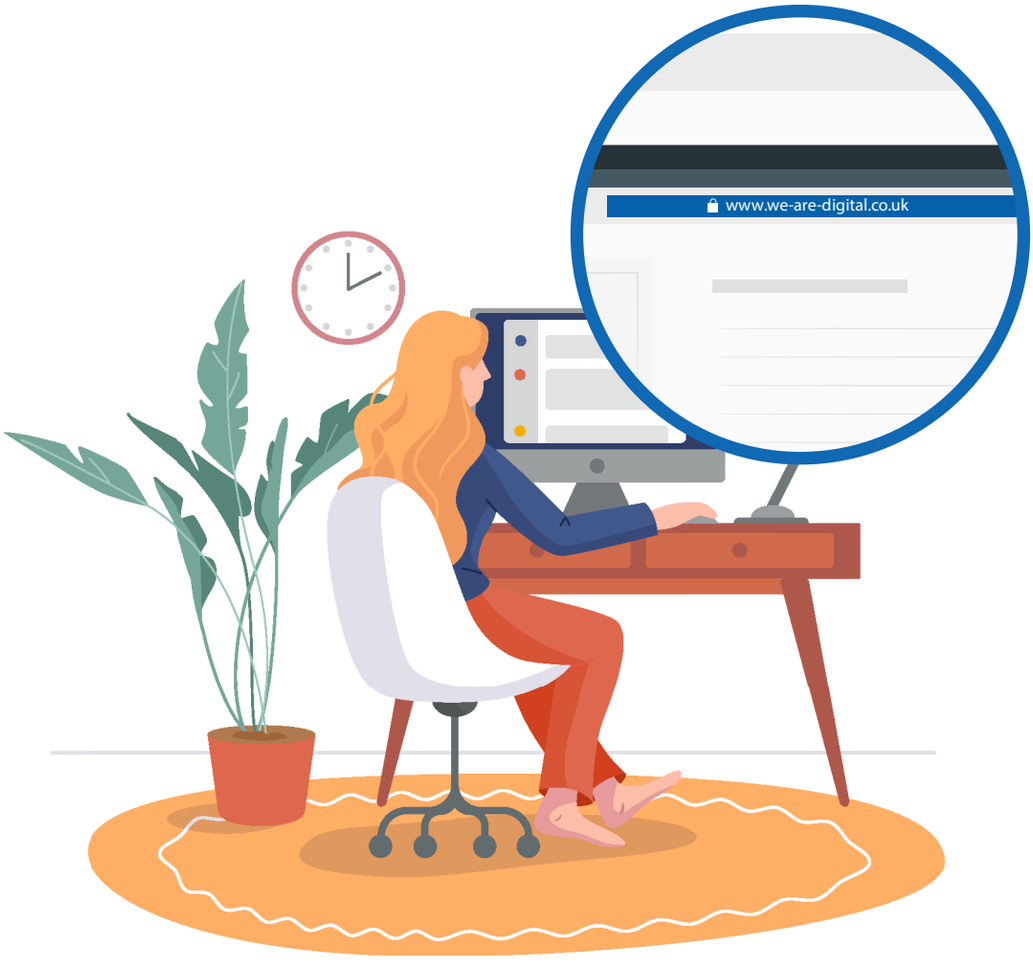
Firstly, try and visit websites that you either know the URL (address e.g., bbc.co.uk) for, or when you search you're confident that the URL that comes up in Google or any other web browser looks legitimate.

Look out for any names that seem to have spelling mistakes in their web address as these are likely to be fake and dangerous.

Our devices are usually able to spot a bad site and will notify you if something is wrong. Always heed these warnings unless you are 100% certain that where you're going to is where you need to be.

Installing safe browser add-ons or extensions can also help protect you against suspicious websites that have been reported previously by other users.

A great way to tell if a site is trustworthy is to look out for the lock symbol at the top left of the screen, just before the URL. If you are entering info into a page make sure the lock symbol is there. When the lock is closed, this means your information is being transferred securely across the Internet to the company you are dealing with. And that you can input any sensitive information securely.



Phishing

Phishing is where attackers try to trick us into entering a dangerous site.

They may set up a bad link that, when clicked, will either download a virus, malware, take us to a dodgy website or ask us to enter personal information such as our logon IDs and passwords.

It is by far the biggest security threat to us as online users today.

These links can be sent by email, SMS message or via links in social media or WhatsApp. They try to make the message or SMS that they send look as realistic as possible, and the web page they take us to look like the one we would normally sign into. However, there are a number of key things we can check to reduce the risk of falling for their scam:

- Does the message or text message come from an unusual email address or phone number?
- If you look carefully at the email address, often it may look to have an official company name with a typo or two
- They often pretend to be legitimate companies, and while they just send these to everyone, sometimes it might be a company you are familiar with
- On a PC, you hover over the email address with your mouse to see if there's a hidden email and unusual address behind it
- These emails are often not addressing you by name, so be cautious of anything that doesn't
- Check for bad grammar or unusual spelling mistakes
- Phishing emails sometimes include urgent requests to try and get us to react without thinking e.g. your account is overdue or about to be closed
- If something in the email sounds too good to be true, it probably isn't true

Do you want to know how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses, and many other problems encountered online? This website gives detailed information about online chats/forums and many other topics and often informs users of the viruses in circulation at a given time - https://www.getsafeonline.org/

Phishing Emails

Email providers such as Gmail or Outlook are constantly checking for Phishing emails and block most of them before the email sender gets to you. This is another area where 2FA/MFA discussed above can be a great help. Even if the email sender tricked you into typing in your password, they won't be able to access your account without the code sent to one of your devices.

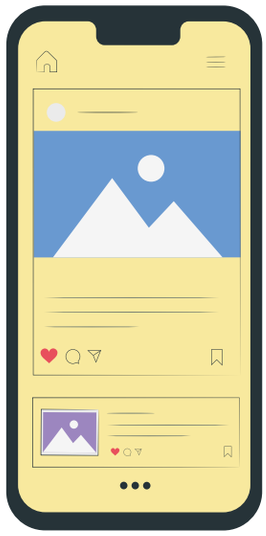
If the email contains one or more of the above clues (that we mentioned on page 11), and you aren't sure that it is a legitimate email **never** click on the link or download the attachment you have been sent, especially if you were not expecting to receive an email of this type.

If you do click on an email and are asked to enter personal details such as passwords and credit card details, **don't do that** unless you are 100% certain that is the web page you were expecting to be taken to. Or if the sender is making a statement such as your account being closed or receiving a fine if you don't click it, try and check it out another way by phoning the company. They would rather you do that and check, than fall foul to a Phishing email in their name.

Even if the email is from a friend be careful as their phone may have been hacked and will be sending out these dodgy emails. If you can contact your friend by another method (not using their email address) and ask if it is valid, if it isn't they may thank you for bringing it to their attention.

Indeed, it is especially important to be wary of unusual emails from friends as this is often how they spread. The hackers takes control of their email and sends it to all their contacts to try and catch more 'Phish' and spread the scam.

Social Media



Social Media is a new way of communicating and connecting with people all over the world from our devices.

But while it can be a lot of fun, you should still be incredibly careful what you publish on your social media accounts.

You really should avoid making extreme or offensive posts. Firstly, because your opinion might change in the future. And once it's out there, it may come back to haunt you. And secondly, employers often check social media accounts before hiring. Which could cost you a great opportunity.

Personal info such as birthdays, your location, and photos of where you live may be used by hackers in a targeted phishing attack (spear phishing) where they use your information to make it look more realistic.

It could also be used for identity theft. So always be cautious about how much information you put on these platforms.

Staying safe on social media doesn't have to be difficult. Here are some things to consider:

Privacy Settings
Use your privacy settings to control who can see your information and posts

Phishing Scams
Look out for the phishing scams discussed above

Think Carefully
Think carefully about what you post

Consequences
Think about the consequences if one of your posts goes further than intended

Strong Passwords
Protect your account with strong passwords and 2FA/MFA if possible

Internet Banking

Internet banking is an easy way to manage your money and finances using your phone, tablet, or laptop.

The banks have built real time checks and use technology to check you are who you say you are, as they understand all the information you use to login is extremely sensitive. Like 2FA, for example.

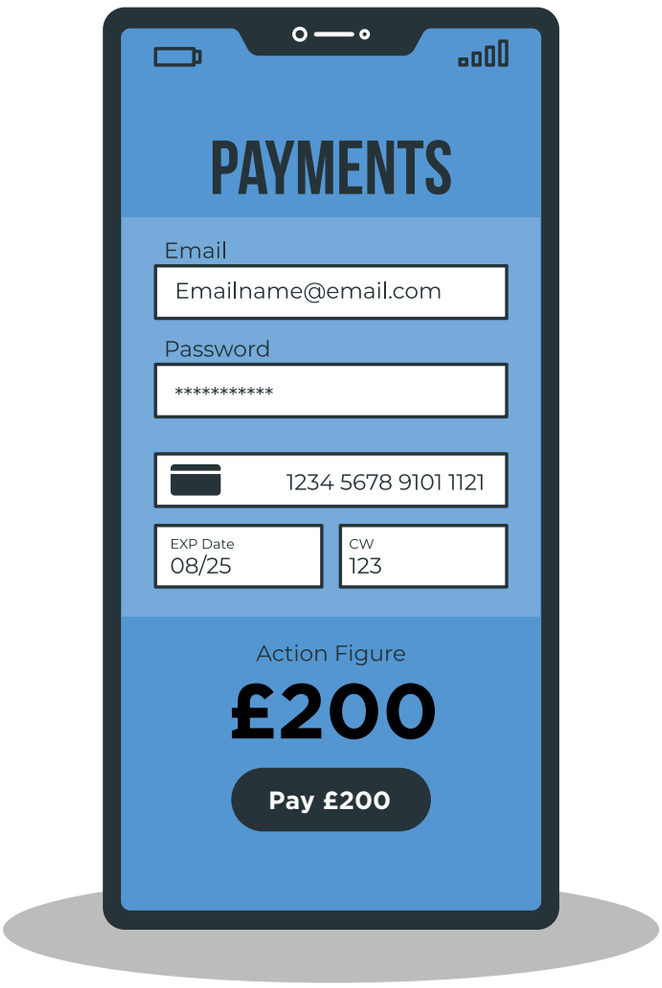
Using a mobile banking app is simpler and more secure than using a website on a laptop, as the phone/tablet acts as that form of 2FA/MFA.

However, there are some important things you should do to keep yourself safe.

- Keep passwords and devices secure with the tips mentioned above
- Never share any of your personal details, passwords or codes with anyone
- Always get your banking app by downloading it from a safe source

i.e., the Google Play or Apple Store

- Always sign out (and double check you have) once you're finishing using it



Notes:

03333 444 019 | info@we-are-digital.co.uk
www.we-are-digital.co.uk