Staying Safe Online

Who we are

Age Scotland is the Scottish charity for older people. We work to improve the lives of everyone over the age of 50 and promote their rights and interests.

Our vision is a Scotland which is the best place in the world to grow older.

Our mission is to inspire, involve and empower older people in Scotland, and influence others, so that people enjoy better later lives.

We have three strategic aims:

We help older people to be as well as they can be

We promote a positive view of ageing and later life

We tackle loneliness and isolation

How we can help

We know that growing older doesn't come with a manual. Later life can bring changes and opportunities to your life and you may need to know about rights, organisations and services which are unfamiliar to you.

That's why we provide free information and advice to help you on a range of topics including benefits and entitlements, social care, legal issues such as Power of Attorney, housing and much more. All of our guides are available to download for free from our website, or you can contact our helpline team to have copies posted to you for free.

Our **helpline** is a free, confidential phone service for older people, their carers and families in Scotland looking for information and advice.

Later life can bring times when you just need someone to talk to. Our **friendship line** is part of our wider helpline and older people can call us for a chat. We're here to listen, provide friendship and offer support.

Call us free on: 0800 12 44 222
(Monday – Friday, 9am – 5pm)

Visit agescotland.org.uk to find out more.

Contents

Introduction

The internet can be a fantastic tool. At the touch of a few buttons it can give us access to information, save us time and money, and connect us to friends and family. But using the internet comes with some risks.

As technology becomes more advanced, criminals are finding more ways to carry out crimes involving computers and other devices that use the internet. This is often called cybercrime.

Many cybercrimes are types of fraud that involve criminals getting hold of personal information or money through dishonest means. These include scams, hacking and credit card fraud. Other types of cybercrime include unauthorised phone tracking, damage to computers or disruption to an internet connection.

While this can sound frightening, there are many ways to protect ourselves from cybercrime. This guide will help you understand the risks and how to minimise them.

We are grateful to CyberScotland for their support in producing this guide.

Glossary

Software – software packages are sets of computer programmes that can be loaded onto your computer or other device. They give your device the ability to do, or be used for, specific tasks. This could include writing a letter, accessing the internet, connecting to a printer or scanning for viruses.

Application / App - a type of software that allows you to carry out a specific task. It usually refers to software for smartphones and tablets.

Hardware - the physical parts of your computer or other device. This includes accessories such as a keyboard, mouse, pair of speakers or printer.

Window - a rectangular box on your screen that opens when you start up a software programme. It contains all you need to use the software for its intended purpose.

Internet / web browser – computer software that allows you to search the internet and access websites, or 'browse' the web.

Address bar / URL bar – a horizontal bar that you will find near the top of an internet browser. Typing a website address into this bar and pressing enter will take you to the web page. You can also type keywords into the address bar and press enter to search for web pages that mention a particular topic.

Cybercrime – any criminal activity involving computers and the internet. It can affect individuals, businesses or entire corporations. Types of cybercrime include theft of data or money via hacking or scams, and damage to a device using harmful computer programmes.

Spam - emails or text messages you did not request. Spam messages are sent to large numbers of people, usually by businesses trying to sell something.

Scam - any type of fraudulent scheme aiming to get people to hand over money, personal information or valuable items.

Malware - short for malicious software. This is the broad term for software that intentionally causes harm. Different types have different effects including damaging your device, sending your data to criminals or blocking access to your files.

Virus - a type of malware that infects and damages files. A virus becomes active when you click on a link or open an attachment infected with the virus. It can then replicate and spread to other files causing further damage.

Installing – loading software onto your device or computer.

Uploading – adding a document or file to a website, for example adding photos to a social media site.

Downloading – getting an app, file or programme from the internet onto your computer. Once downloaded, you can open or save files or install programmes.

Swipe – this means running your finger across a touchscreen device. This changes what you can see on the screen. It is sometimes used on smartphones as part of unlocking the screen.

The National Cyber Security Centre (NCSC) provides further terms. Search 'glossary' at **www.ncsc.gov.uk**.

Understanding and dealing with cyber scams

Scams are a type of fraud that trick you into providing money or personal information. The next section explores what to look out for and what to do if you are affected by a scam.

Spotting and avoiding cyber scams

People of all ages get fooled by scams. They are becoming harder to detect as criminals find new ways to make them even more convincing.

Many scams are carried out via email, including those that try to trick you into entering personal details. You should also be careful about links or attachments sent with emails. They can contain malicious software such as viruses that will be activated if you open the link or attachment.

Other scams are carried out through social media. Beware of adverts or offers that look too good to be true; they often are.

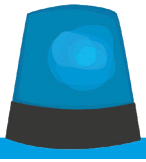
You should report any type of suspicious email to the **National Cyber Security Centre (NCSC)** by forwarding them to **report@phishing.gov.uk**. They will investigate the message and try to put a stop to the scam.

Stop! Think Fraud

The advice of the Government's **Stop! Think Fraud** campaign is to **STOP!** if you've seen something that doesn't feel right:

- don't click on any links
- don't give out any personal or bank details
- break contact if needed
- tell family and friends to make them aware
- if you've lost money, call **Police Scotland** on **101**

Visit **www.mygov.scot/staying-safe-online** to read advice from the **Scottish Government** about protecting yourself online.



The Cyber and Fraud Hub

The **Cyber and Fraud Hub** is a charity that launched in 2024. They keep on top of the latest developments in fraud and online scams by working closely with the banking industry and partners in policing and technology.

Their advice is to look out for contact that:

- is **Unexpected**
- makes a **Demand** of you
- puts you under **Time Pressure**

You can report any type of fraud or online scam to their **Incident Response Helpline** on **0808 281 3580**. They can provide victim support if you have been affected by cybercrime and will report the crime to the police on your behalf if you have not already done so.

They offer a range of guides on cyber security including **A Guide to Avoiding Fraud and Scams for Older People**. Visit **cyberfraudhub.org/scamsguide**.

They also provide links to **online tools** that can help you check for scams and whether you have been affected by fraud. Visit **cyberfraudhub.org/self-help**.

Types of cyber scams to be aware of

'Phishing' emails – this is one of the most common ways scammers trick people into giving out their personal details. The message will pretend there is a good reason for you to provide or 'confirm' your bank details or personal information.

They can be hard to spot as emails are often made to look very official. They may look like they have been sent from a recognised business, bank or even a government department. However, organisations will never ask you for this information unless you contact them first.

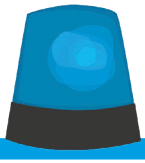
Emails may tell you that you need to act quickly because there is a problem, for example:

- someone has accessed your account
- a payment has failed, and services will stop
- a delivery is waiting for you but does not have enough postage

If you want to check whether a message like this is genuine, you should contact the company it seems to be from by looking up their official contact details. DO NOT use contact details provided in the message.

If you receive an email saying you need to change your password for an online account, you should do this by visiting the official website. Do not click any links in the message; they may send you to a fake site that is set up to steal your login details when you enter them.

Unexpected phone calls can also be phishing scams. See our **Avoiding Scams** guide for more information. To order a copy, call the **Age Scotland helpline** on **0800 12 44 222** or visit **age.scot/information**.



Department for Work and Pensions scam

Beware of a scam text message saying it is from the Department for Work and Pensions (DWP), encouraging you to apply for the winter heating subsidy. It contains a link leading to what looks like an official DWP web page. This opens to a form that asks for your name, contact information and the details of your bank card.

The DWP would not need this information to pay you a winter heating benefit and would never ask for personal details of any kind unless you contacted them first. In addition, both types of winter heating payment will now be paid by Social Security Scotland to anyone living in Scotland who is entitled.

For the latest information about the new **Pension Age Winter Heating Payment**, visit **www.mygov.scot/pension-age-winter-heating-payment**; and for **Winter Heating Payment**, visit **www.mygov.scot/winter-heating-payment**.

Ask Silver is a new phone app that can be used to check text or WhatsApp messages for signs that they could be a scam. The app can also alert you to new types of scams to be aware of and can be used for reporting scam messages. Visit **ask-silver.com** for more information.

Money requests from friends or family – scam messages can be made to look like they are from a friend or family member by using their email address. The message may be asking you to send money to them urgently because of an emergency, or to make a purchase for them for which they will pay you back.

Do not respond to the message but contact the person it seems to be from using another method of contact. If they did not send the original message, they should change the password on their email account and use security software to scan their devices for malware. See page 19 for more information about security software.

Investment scams – be suspicious of **any** email or online advertisement that offers you the chance to invest, especially if the offer is time limited or sounds too good to be true. Investment scams include those offering opportunities in whisky, wine, cryptocurrency and gold.

Some may offer high returns for investing your pension fund, or access to funds before you retire. You can check an investment firm is genuine using the **Financial Conduct Authority Firm Checker** tool at **www.fca.org.uk/consumers/fca-firm-checker**.

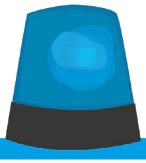
Online sale of goods or tickets that do not exist – being sold by private sellers, for example on eBay or Facebook Marketplace. Check the reviews of the seller and be particularly suspicious if you are pressured to buy quickly.

Advance payment scams – beware of being told you need to pay something up front to receive a prize, job offer or service. This is not normal practice and is likely to be a scam.

Romance fraud – criminals create fake profiles and use the information you provide to pretend you have lots in common. These can be social media profiles as well on dating websites. Be particularly careful if someone is very quick to express interest or intense feelings or tells you they are in a sad or difficult situation.

The person will typically start asking for small amounts of money after gaining your trust, or for money to come and visit you, promising to pay you back. They may ask for increasing amounts as time goes on or ask you to take out a loan for them in your name that they will pay off. Visit **cyberfraudhub.org/romancefraud** for more information about this type of scam.

For more information about the different types of fraud and scams, visit **www.takefive-stopfraud.org.uk/protect-yourself**.



Scam alert emails

You may like to sign up to emails about the latest scams to look out for. Examples include:

- **Which? Scam Alerts**: visit **which.co.uk/scamalert**
- **Trading Standards Scotland Bulletin**: to sign up and view past bulletins visit **www.tsscot.co.uk/bulletin**

You can also follow **Cyber and Fraud Hub** on Instagram or LinkedIn for updates about scams to look out for.

What to do if you are affected by a scam

There is no need to feel embarrassed if you become a victim of a scam. The most important thing is to **act quickly** to secure your accounts and data and to report the crime.

Contact your bank immediately if you:

- think you might have made a scam payment
- think someone might have your financial details
- notice any unusual activity on your account.

Your bank can freeze your account and cancel your cards if needed.

DO NOT use any contact details from the email or text message. You can contact most UK banks by calling **159** and giving the name of the bank when asked, or look up the number in the phone book, on a letter or on the bank's official website.

You should also:

- **change relevant passwords** straight away
- **report any type of cybercrime** to:
  - **Police Scotland** by calling **101**
  - **Cyber and Fraud Hub Incident Response Helpline** on **0808 281 3580**.

Cyber and Fraud Hub will provide you with support and try to remedy the situation where possible. They will also report the crime to **Police Scotland** if you do not want to do this yourself.

Reporting quickly is important because there may be immediate actions that can be taken. It will also help others to be protected from the same type of scam.

Other types of cybercrime

Scams are just one type of cybercrime. Other types include credit card fraud, hacking and attacks from malicious software, including viruses. Some of these attacks give criminals access to information they will use to carry out fraud. Others can damage your device or files.

You should report all types of fraud to **Police Scotland** by calling **101**. You can also report them to **Cyber and Fraud Hub** on **0808 281 3580**.

Some types of cybercrime involve criminals gaining access to your email or social media accounts. They may carry out scams by sending messages to your contacts that look like they are from you.

If someone receives a message from one of your accounts that you did not send, you should change your passwords immediately. You should also scan your devices using security software. See page 19 for information on security software.

You can protect yourself by making sure your devices are secure, and you are using the internet safely. The remaining sections of this guide provide information and guidance on how to do this.

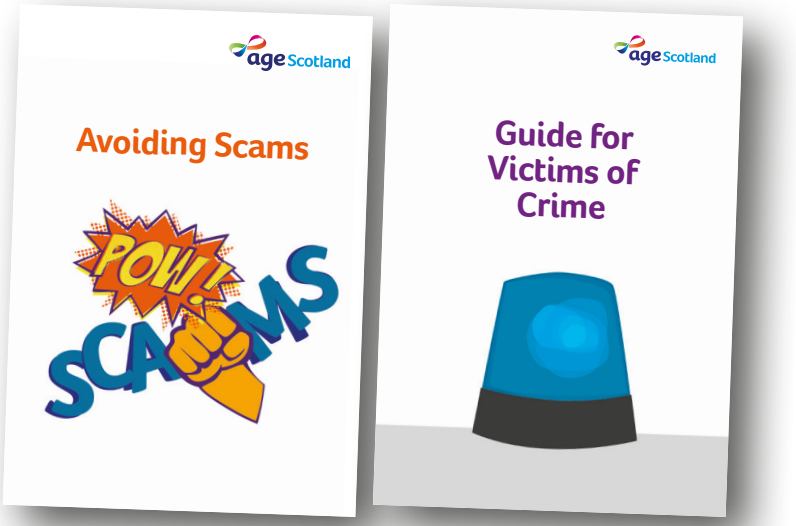
Additional resources

Cyber and Fraud Hub has a guide on protecting your personal data and what to do if it is compromised.
Visit **cyberfraudhub.org/databreach**.

The **Take Five Stop Fraud** website provides further information on how to protect yourself from fraud.
Visit **www.takefive-stopfraud.org.uk**.

The **National Cyber Security Centre (NCSC)** provides step by step actions to take after being affected by specific types of fraud. Visit **www.ncsc.gov.uk/section/respond-recover**.

Our **Avoiding Scams** guide and our **Guide for Victims of Crime** also provide further information on these topics.
Visit **age.scot/information** or call the **Age Scotland helpline** on **0800 12 44 222**.



Protecting your devices & data

Using the internet often requires you to enter personal information, such as your name, address, date of birth and bank or card details. If your devices and accounts are not protected well enough, cyber criminals could steal your personal data, money or identity. So online security is vital.

Tips on using passwords

Passwords are one of the most important tools you can use to protect your information online. However, they are only effective if you protect them well and they are difficult to guess. Using a **password manager** – explained below – is the best way to have strong passwords for all your accounts without you having to remember them.

A password manager is a type of online account that can securely store passwords for all your other online accounts. It will store your passwords on the **cloud**, a very large type of data-storage software that can be located almost anywhere, or even across several different locations, and is accessed using the internet.

There are many password managers available, and each works slightly differently. Generally, they create different long and random passwords for each of your online accounts, store these for you and enter the right one automatically when you visit the login page. You just need to set and remember a very strong master password for the password manager itself.

If you do not want to use a password manager, you should follow the rest of the guidance in this section to make sure your passwords are protecting your data as well as possible.

Create strong passwords: it is worth taking the time to make sure your passwords are as strong as possible. Here are some tips for creating strong passwords:

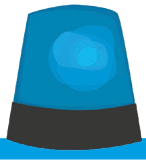
- Don't use obvious passwords, such as PASSWORD or 123456
- Don't use personal information, for example, your name, your date of birth, or the name of your partner, child or pet – these are easy to find out and another obvious thing for a hacker to try
- Use long passwords where possible – at least 8 characters, but ideally more
- Use a mixture of lower- and upper-case letters, numbers and special characters (punctuation and other symbols)
- Change your passwords regularly, and immediately if you think someone might know what they are

Passphrases: these are passwords that include three random and unrelated words. Passphrases are difficult to guess but easier to remember than a random series of characters. They should still follow all the other rules of a strong password.

Use a different password for each account: even if you have a particularly strong password and protect it well, you should not use it for more than one account.

Passwords can be stolen if a company you have an account with is hacked. There have been several recent examples of this in the media. If you use the same password across multiple accounts, hackers of one of these will have your password for all of them.

Never write your passwords down: this creates a huge security risk. It is much better to use a password manager, explained on page 14.



Protecting your email

It is particularly important that your email account is well protected. Make sure you set a very strong password that you do not use for anything else and use multi-factor authentication. See page 17 for more information about this.

You should also set up a recovery email address or phone number. This will be used to alert you if someone logs in from a new location or device or tries to change your password.

Without these security measures, someone who gains access to your email could easily reset your password and lock you out of your email account. They could also gain access to any other online accounts that were set up using that email address, and reset your passwords for those accounts too.

On top of this, they would be able to send messages to your contacts and access a broad range of your personal information, putting you at risk of many types of fraud.

Visit **www.ncsc.gov.uk/cyberaware** for further information about securing your email account.

For more information about creating secure passwords, visit **cyberfraudhub.org/passwords**.

Biometric logins

A biometric login allows you to access or unlock an account or device using a feature unique to you, such as your fingerprint, face or voice. This is particularly common when using a mobile phone or tablet to access online accounts.

Devices with this capability can be set up to scan and recognise your unique feature. You can then use the device to scan your chosen feature when you want to log in. The account or device will unlock if the scans match.

Biometric login is not 100% reliable so it is still important to make sure your device and passwords do not fall into the wrong hands.

Two-factor authentication

Two-factor authentication, or multi-factor authentication, is when an account is protected with more than one type of security. This means that if someone were to find out your password, this alone would not be enough for them to access your device or account.

You will usually need to enter your password as normal and then do something else. This could be entering a code sent to your mobile phone for example, or using your phone to scan your fingerprint.

The **Cyber and Fraud Hub** website provides guidance on setting up two-factor authentication. Visit **cyberfraudhub.org/2fa**.

Safeguarding portable devices

It especially important to protect devices that you take out of your home. Set a secure screen lock so your data will be protected if your device is lost or stolen.

You should carry devices in a sealed pocket or a fastened bag. Try not to carry them in your hand for any length of time as this makes it easy for someone to snatch them as they walk past.

Make sure nobody can see your screen when you use your device in public. Be especially careful on public transport; people sitting behind you may have a view over your shoulder, or via the reflection in the window.

Public WiFi networks

Public WiFi networks can be useful if you do not have network data as part of your mobile phone package. But you should be careful how you use them.

Public networks are not as well protected as private ones. This makes it easier for others to see your internet activity and any data you share. For this reason, you should never carry out any sensitive transactions over public WiFi networks.

Examples of sensitive transactions include logging into your internet banking, or entering your card details to buy something online. If you do need to use the internet while out and about, it is more secure to use the data provided by your phone network if you have this.

You should never connect to public WiFi that asks for personal information before allowing access. This immediately gives potential hackers a head start and may be a sign the network is part of a scam.

Security software

Security software can help protect your computer from viruses and other online threats. Types of security software include:

Antivirus – scans your computer to check for viruses and other types of malicious software, also referred to as malware. Antivirus software can remove malware before it does any harm. Different types of malware do different things. They might damage your device, steal your data, or lock you out of your device. Some send themselves to other people you know, to try to infect their devices too.

Firewall – this can be a piece of software on your device, or a piece of hardware built into a larger computer network. It checks data that is being received by the computer as it comes in, to make sure it is safe. This helps to protect you from malware and hackers.

Most computers and devices bought new will already have a firewall and antivirus software. It is important not to put more than one piece of antivirus software on your device. These types of software often recognise each other as potential threats, and can stop each other from working, leaving your computer unprotected.

If you need to install your own security software, make sure you get it from a trusted source. Guidance on getting the right protection for your device is available at **ncsc.gov.uk/antivirus**.

Updates to security software

Most antivirus software will scan your computer regularly without you needing to do anything. It will also work in the background, checking files as you open or download them.

Your security software will be updated regularly by the manufacturer to protect against new methods of attack from cyber criminals. The updates should be sent automatically to your computer via the internet. You may occasionally be asked to restart your computer so these updates can take effect.

Good practice for using your device

Safe use of software

There are many types of software available. The software you will need depends on what you'd like to be able to do. Devices bought new usually come preloaded with a basic package of software. This will generally allow you to open, create and store documents, such as letters, spreadsheets or slide presentations. It will also allow you to use the internet, including sending emails.

If you want to be able to do anything more on your computer, you will usually need to install additional software. For example, you may want to connect a printer to your computer, edit photos or make video calls.

Downloading software

You will need to download most software from the internet. Some basic software is free to download, but you should only download it if you are sure it is from a trustworthy source. Even if you have security software, there is a possibility that a virus or other type of malware could get onto your computer.

The software packages for devices such as tablets or smartphones are called applications, or 'apps'. Apps are available from the app store of the phone you are using. This will be the **Apple App Store** if you use an iPhone or the **Google Play store** if you use any other type of phone.

You should only download apps from trusted companies. Criminals can use unofficial apps to place tracking software on your phone. This will send your device's location and other data to hackers who can use this to target you for scams or fraud.

Signs your phone may be affected include the battery suddenly running down, data being used up unexpectedly fast or your phone becoming very hot. You should contact the customer service team for your device if you think this has happened.

Avoid downloading software you do not need

When you download software onto a computer, the provider will sometimes try to get you to download additional software that you do not need. Having extra software can slow down your computer and may interfere with its other functions.

When you download software onto your computer, you will be shown a series of pop-up boxes. These will give you information and options to choose, including the option to click for the next step when you are ready.

Before clicking the 'next' button, you should check the options you are given for mentions of additional software. You might need to click on tick boxes that already have a tick in them, to stop additional software from being included in the download.

Updates to your software

Just like security software, other types of software get updated regularly by their provider. You may need to allow permission for your device to install these updates. They are important because they often include protection against new types of malware. But check you recognise the software any time you see a message on your computer asking you to agree to an update; some viruses use this type of message to trick you into activating them.

Using a device that is up to date

Software is always becoming more advanced so that it can keep up with new security threats and other changes in technology. Over time, computers and other devices become less able to handle this more advanced software.

For this reason, devices generally need to be replaced every three to eight years. This includes smartphones as well as computers and tablets. A more basic device will need replacing sooner than a higher-tech model. This is worth keeping in mind when deciding what kind of device to buy.

It is possible to buy computers and other devices second hand. However, second hand devices are also more likely to be infected with malware, so be cautious about this.

For advice on buying (and selling) second hand devices, search 'second hand' at **www.ncsc.gov.uk**.

Why do devices go out of date?

The background system that makes your computer work, called the operating system, only has so much capacity. This is also true for the physical parts of a device. You may notice after a few years that your device becomes slower to work. This is because the updated software becomes too complex for your device and the older operating system to manage.

Even if your device still works fine, the operating system might stop being updated by the provider. The operating system receives automatic updates to protect it from new threats, just like software does. New operating systems are launched once every few years, and older systems eventually stop being updated. This means your computer will no longer be properly protected.

Your computer itself will show a notification message in good time, telling you what to do. However, you may need to get a new device if your current device is too old. **Beware of emails asking you to click a link that will update your operating system; these are likely to be scams**.

Turn off and restart your computer regularly

Closing your computer down properly after you use it allows any security updates to finish installing. Without this step, the updates may not be operating on your computer even if you have agreed to them.

It is also important to close your internet browser windows when you finish using them. Hackers are sometimes able to access web pages that are open on computers and change the website, without the webpage or web address looking any different. This can allow them to see any data you enter.

Backing up your data

If you do experience online crime and lose access to your device or data, having your files backed up will help you to recover them more easily. You can do this using an external hard drive or 'the cloud'.

An **external hard drive** is a small device usually about the size of a mobile phone that you can plug into your computer. You can use it to store copies of important documents, or you can store a backup of the entire contents of your computer.

Cloud storage is a very large piece of software where files and data can be stored. You do not download this type of software; it is kept centrally by the company that runs it, and you access it via the internet.

The software for the cloud can be located almost anywhere and is sometimes stored across multiple locations. If your device is damaged or locked by a malware attack you will still be able to access any files you have stored in the cloud.

Three of the biggest cloud storage platforms are Google Drive, Dropbox and Microsoft OneDrive. You can set up an account for free using an email address.

The **National Cyber Security Centre** provides top tips for staying secure online, including how to back up your data. Visit **www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online**.

Using the internet safely

Secure internet connections

If you have a wireless internet connection in your home, you should make sure it is password protected. Most wireless internet connections are set up with a secure password that will be printed on the back of the internet router. The router is the device that connects to the internet and creates a wireless signal in your home.

Your internet provider will usually send you a router that you can use all the while you use their internet service. They are usually about the size of a hardback book.

Without a password, other people may be able to connect their device to your wireless signal and use the internet you are paying for. This also means they can access your internet activity and data. If no password is set up, you should check the installation manual for instructions or contact your internet provider for help.

Understanding your digital footprint

Whenever you use the internet, whether on a computer or another device, you leave a data trail of your activity. This is called your digital footprint.

You create an **active footprint** whenever you interact with a website, for example by logging into an account, posting on social media or making a purchase. You also create a **passive footprint** whenever you visit a website or search for information. Some apps and websites automatically track your geographic location, including after you have closed them.

Some parts of this data trail can be helpful. For example, websites will ask at the beginning of your visit if you want to allow cookies to be collected. Cookies are small packages of information about you, including the country you are visiting the website from, and your username for online accounts.

Agreeing to cookies means you don't have to start from scratch every time you visit the same website. But the more information held about you online, the higher your risk from cybercrime.

It is important to think carefully about what kind of information you share on the internet, and where you share it. The next section explores things to watch out for.

How to spot fake websites

Not all websites are safe and secure. It is especially important to check you are using a legitimate website if you plan to enter personal information. This is important for protecting your identity, your money and the device you are using.

Even just clicking a link to a scam website can be harmful. Be careful about clicking links in adverts, including pop-up ads and those on social media. Be extremely cautious about web links sent to you by email or text message.

You should also be careful about scanning QR codes. These are square barcodes made from a unique pattern of black and white squares. They can be scanned using a smartphone to open a particular website. QR codes are often used in restaurants to open the menu on the restaurant website, or on adverts to take you directly to further information. Make sure you only scan QR codes from sources you trust; they could easily be used to send you to a scam website.

Get Safe Online has a tool that allows you to check a website for signs it could be a scam. Enter the address of the website you want to check at **www.getsafeonline.org/checkawebsite**.

Check the website address

The website address, also called the URL, should begin with https://. The S stands for secure and means that the information being transferred between you and the website is encrypted.

Encrypted data is converted into a code that can't be read or understood by criminals who might be trying to access your details. There is sometimes a small padlock icon to the left of the web address to show it is secure.

If the website address begins with only http://, the website is NOT secure, and your information may be visible to others. The http:// may be shown in red text to alert you to the fact that the website does **not** have a security certificate.

You should also check that the web address exactly matches the one you are expecting. Watch out for spelling mistakes, extra characters or addresses that are slightly different to the official web address, including differences to the end of the web address. These signs may mean that someone has set up a fake site.

Check the content of web pages

Some websites are set up to **look** like the one you were expecting and will often also use a very similar web address. Even if the address is secure, you should still take care that it is the official website.

Signs a website might not be legitimate include blurred or incorrect logos, spelling and grammar mistakes, broken links, pop up messages and the content not looking as you expected.

If in doubt, don't enter your details. Close the page and find the web address from a source you trust, such as a printed advert or an official letter. You should then type the web address carefully into the address bar of your browser.

Additional resources

The organisations below provide further information and guidance about online safety:

Police Scotland:
visit **www.scotland.police.uk** and search 'keep secure online'

Scottish Government:
visit **www.mygov.scot/online-safety**

National Cyber Security Centre (NCSC):
visit **www.ncsc.gov.uk** and search 'top tips'

You should report any suspicious websites to the **National Cyber Security Centre** at **www.ncsc.gov.uk/report-scam-website** or call the **Cyber and Fraud Hub Incident Response Helpline** on **0808 281 3580**.

Making payments online

If you order products or services online, be extra careful to check that the website where you enter your payment details is secure. Look for the padlock symbol to the left of the web address or make sure the web address includes an S in the https:// at the beginning.

Be very cautious about buying products that you see advertised on social media. These can often be scams and the products either do not exist or are of very low quality. It is safest to stick to brands you know and to find their website by typing in their official address.

Check product reviews – most websites show these below the information about the product. Check whether there are lots of reviews with a low number of stars. Some reviews will have comments about the product. These should give you an idea of the problems people have experienced.

Pay with a credit card if possible – this provides you with some protection if you fall victim to fraud. Consider using the same card each time and making a note of each of your purchases. This will make it easier to check all your online purchases against your credit card statement.

Check your bank statements regularly – make sure you recognise all the payments and contact your bank immediately if you do not, even if the amount is small. Some criminals begin by taking small amounts and then take larger amounts if the smaller amounts have not been reported.

Never make a bank transfer when buying online – when making an online purchase, you should only ever be asked to give your long card number, the card expiry date and the three digit security code on the back of the card. If a website is asking you to make a direct bank transfer, do not use it. You should close your browser straight away.

You should also report the website to the **National Cyber Security Centre** at **www.ncsc.gov.uk/report-scam-website**.

Some websites will offer to remember your card details for when you next make a purchase. This can be helpful for websites you use a lot and trust, but you should never do this on a shared computer.

Banking online

Online banking allows you to do most of the things you would want to do in person or on the phone. You can set up an online banking account with your bank or building society by registering on their website. The website will provide instructions on how to do this.

Banks use very secure online systems. However, you should still be especially careful not to write down any of your banking passwords. You should also never carry out banking transactions over public WiFi networks.

Make sure you log out of your online banking account each time you finish using it and close the internet browser. It is also very important to keep your devices up to date. Some types of malware can track your login details when you enter them, even if you are using the official website, for example.

If you would like to know more about internet banking, ask your bank about their system. They will be able to show you how to sign up via their website and how to download the official apps for smartphones or tablets.

Beware of any emails or phone calls that say they are from your bank, especially if they ask you to confirm your details. If your bank does contact you, they will never ask you for your account details or any personal information.

Using email safely

Email can be a useful way to send detailed information quickly to another person, or to many people at once. There are a few things to be careful of that will help you to protect your own data and the data of the people you email.

Use a trusted email provider – there are many websites that offer email services, but some offer better data security than others. Sites like Gmail, Outlook, Yahoo Mail and ProtonMail are all good options. They have inbuilt spam filters that will spot emails that look suspicious and separate them from your main inbox.

Report any spam email you receive – most mainstream email providers have an option to 'report spam' so your email provider can investigate the email and recognise it as spam in future.

Do not click links you are sent in emails – or open attachments you weren't expecting to receive. Be particularly careful of emails that say you need to do something urgently or ask you for personal information, even if the email looks legitimate. More advice about this can be found on page 6.

Use the Bcc option – if you are sending an email to many different people at once, especially if they don't know each other. This stands for 'blind carbon copy'. You will find this beneath the space where you would normally type the recipient's email address. When you use the Bcc option, the people you email will not be able to see each other's email addresses. This is important for protecting the privacy of the people you are messaging.

Be careful about using 'reply all' – if you reply to an email that was sent to you and others, you will have the option either to 'reply' or 'reply all.' Be careful to check who else received the original email; they will also see your reply if you 'reply all'.

Using video calling safely

Video calling is a great way to stay in touch. However, it can be easy to forget that it is a form of data sharing. A video call can feel private, but keep in mind that still pictures or the whole call can be recorded. As well as what you actively share, you should be careful of what might be seen or heard in the background. Be especially careful if you are talking to someone you have met online.

Using social media safely

Social media can be a fantastic way to keep in touch with friends and family you don't see regularly. However, it is important to remember that social media is public, and the information you share can often be seen by more people than you intend.

Privacy settings

Without privacy settings, anyone can see your full profile, even if they do not know you personally. It is your responsibility to turn on privacy settings for your account.

Even with some settings turned on, your information could go further than you mean it to. For example, on some platforms, if a friend likes your social media post, all their friends can then see it. If a friend of theirs likes it, all of that person's friends can see it too, and so on.

Privacy settings can change from time to time. It is worth checking regularly whether you are happy with the settings that are in place. For more information about social media privacy settings, visit **www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely**.

Think carefully before you post

It is important not to share any information you wouldn't be comfortable telling a stranger. Even if you have privacy settings turned on, your information could easily get into the wrong hands. For example, if someone in your network has not secured their account properly, your information will also be at risk.

Take particular care if you are using social media when you are upset or angry; if you are feeling emotional, it can be easy to post more information than you intend.

If you have professional connections as well as friends and family on your social media, think about whether you are comfortable with all your connections seeing what you post. It is possible to set up different profiles for different purposes, or to use privacy settings to make sure only the people you choose can view your more personal content.

Social media housekeeping

You should be careful who you connect with on social media. Keep in mind that anyone you connect with will be able to see anything you have posted in the past as well as the future. Never connect with anyone you do not know in person as they may be trying to steal information from you.

If you no longer use a social media account and don't want people to be able to see what you posted in the past, you should close it down. This is sometimes called 'deactivating' your account. How you do this will differ for each social media platform, but you can often find the option in settings, under account details or privacy settings. Many platforms have a help function where you can search for settings you can't find easily.

Useful resources

Cyber and Fraud Hub

A charity that works closely with banks and Police Scotland to stay updated on the latest fraud and online scams. You can report fraud and cyber scams to them. They also provide victim support and support to recover funds where possible.

0808 281 3580
www.cyberfraudhub.org

National Cyber Security Centre

Provides advice and guidance on avoiding fraud and scams and what to do if you are affected. They will also investigate cybercrime and any type of scam reported to them.

www.ncsc.gov.uk

Consumer Advice Scotland

Provides advice for all types of scams. You can also report scams to them, either online or by phone; additional support can be offered when reporting by phone. They will alert Trading Standards if appropriate.

www.consumeradvice.scot
0808 164 6000

Victim Support Scotland

Provides support if you have fallen victim to fraud or any type of crime. They can signpost sources of emotional support and give practical advice.

0800 160 1985
www.victimsupport.scot

Financial Conduct Authority

Provides reporting for scams involving pensions, insurance, investments and other financial services they regulate. They also provide a financial Firm Checker tool and listings of registered Financial Advisors.

www.fca.org.uk/consumers
0800 111 6768

Get Safe Online

Provides information about many different areas of online safety, including tools to check if websites are genuine and how to keep yourself safe online.

www.getsafeonline.org

Information Commissioners Office

Offers advice on protecting your personal information and about your rights concerning your personal data.

www.ico.org.uk
0303 123 1113

How you can help

Our vision is a Scotland which is the best place in the world to grow older.

All the information we provide is free and impartial. It helps older people access their rights and entitlements and can be life changing.

We are also a lifeline for older people who are feeling lonely and isolated. You can help us to support older people who need us most.

Together, we can make a difference.

Make a donation

No matter how small or large, donations make a massive difference and help us continue our important work.

- Call **03330 15 14 60**
- Visit **age.scot/donate**
- Complete the **donation form** and return by Freepost

Fundraise

Whether it's having a bake sale or running a marathon, there are so many ways to raise vital funds to support our work. To find out more, call **0333 323 2400** or visit **age.scot/fundraise**.

Leave us a gift in your Will

By choosing to leave us a gift in your Will, your legacy will help us to continue being there for older people for generations to come. To find out more, call **0333 323 2400** or visit **age.scot/legacy**.

Please donate today

Complete the form and return by Freepost to RSBS-KEHC-GBBC, Age Scotland, Edinburgh, EH9 1PR

Your details

Title: | Forename: | Surname:

Address:

City:

Postcode: | Date of birth:

By providing us with your telephone number and email address you are consenting to us contacting you via phone, text and email.

Email:

Home tel: | Mobile tel:

I WOULD LIKE TO DONATE

£75 ☐ £50 ☐ £25 ☐ Other (£)

I wish to pay by (please tick):

MasterCard ☐ Visa ☐ CAF ☐

CharityCard ☐ Cheque ☐ (payable to Age Scotland)

Name on Card

Card No.

Expiry date | Security code

Signature | Date

I prefer not to receive a thank you acknowledgement for this donation ☐

I would like information about leaving a gift in my Will ☐

I WOULD LIKE TO MAKE MY DONATION WORTH 25% MORE

giftaid it

I want Age Scotland** and its partner charities to treat all donations I have made for the four years prior to this year, and all donations I make from the date of this declaration until I notify you otherwise, as Gift Aid donations.

I am a UK tax payer and understand that if I pay less income tax and/or capital gains tax than the amount of Gift Aid claimed on all my donations in that tax year it is my responsibility to pay any difference.

Yes, I want Age Scotland to claim Gift Aid on my donations** ☐

I do not wish you to claim Gift Aid on my donations ☐ **Date**

Keeping in touch

We will stay in contact by post unless you ask us not to. We will never sell your data and we promise to keep your details safe and secure. You can change your mind at any time by emailing us on contact@agescotland.org.uk or calling us on 0333 323 2400.

You can read Age Scotland's privacy policy at **age.scot/privacypolicy**.

**Age Scotland, part of the Age Network, is an independent charity dedicated to improving the later lives of everyone on the ageing journey, within a charitable company limited by guarantee and registered in Scotland. Registration Number: SC153343. Charity Number: SC010100. Registered Office: Causewayside House, 160 Causewayside, Edinburgh, EH9 1PR

Age Scotland is the Scottish charity for older people. We work to improve the lives of everyone over the age of 50 so that they can love later life.

Our vision is a Scotland which is the best place in the world to grow older.

Let's keep in touch

Contact us:

Head office
0333 323 2400

Age Scotland helpline
0800 12 44 222

Email
info@agescotland.org.uk

Visit our website
www.agescotland.org.uk

Sign up to our newsletter

Our regular newsletters by email contain details of our campaigns, services and how you can support our work.

Sign up today at **age.scot/roundup**

Follow us on social media

Our social media channels are a great way to keep up to date with our work and issues that affect older people.

CyberScotland

We are grateful to CyberScotland for their support in producing this guide.

We are grateful to the Scottish Government for part-funding this publication

The Scottish Government

LEG 14 Oct 2025