# A beginner's guide to staying safe online

Helping you to stay safe whilst online

Publication date: February 2022

# Contents

# **1.** Introducing you to online safety

## 1. Introducing you to online safety

Hello,

Welcome to Age UK's beginner's guide to staying safe online. This guide contains practical tips and advice to help you stay safe when using the internet. By taking some simple steps, you can protect yourself online and feel confident that your personal and financial information is safe.

The internet is a fantastic resource. From finding out the opening times of your local shops to using games and puzzle apps, there is lots you can do online. When I first started using the internet, I was worried about entering my personal details as I wasn't sure if others could access them. But now I have lots of helpful information and know what to do to keep my iPhone and laptop safe. I use strong passwords for online accounts and make sure I don't use the same one all the time.

### Getting support

There's a lot of useful information in this guide. I'd recommend working your way through it at your own pace and repeating any sections you want to focus on. You can work through it by yourself, with the support of an Age UK Digital Champion, or with the help of friends, family and carers.

If you've got any questions as you work your way through the guide, you may be able to get support from your local Age UK or local Age Cymru. You can find your local Age UK at **www.ageuk.org.uk/services/in-your-area/**.

After reading this guide, I hope you feel more comfortable and confident using the internet.

**Elsie, 82**

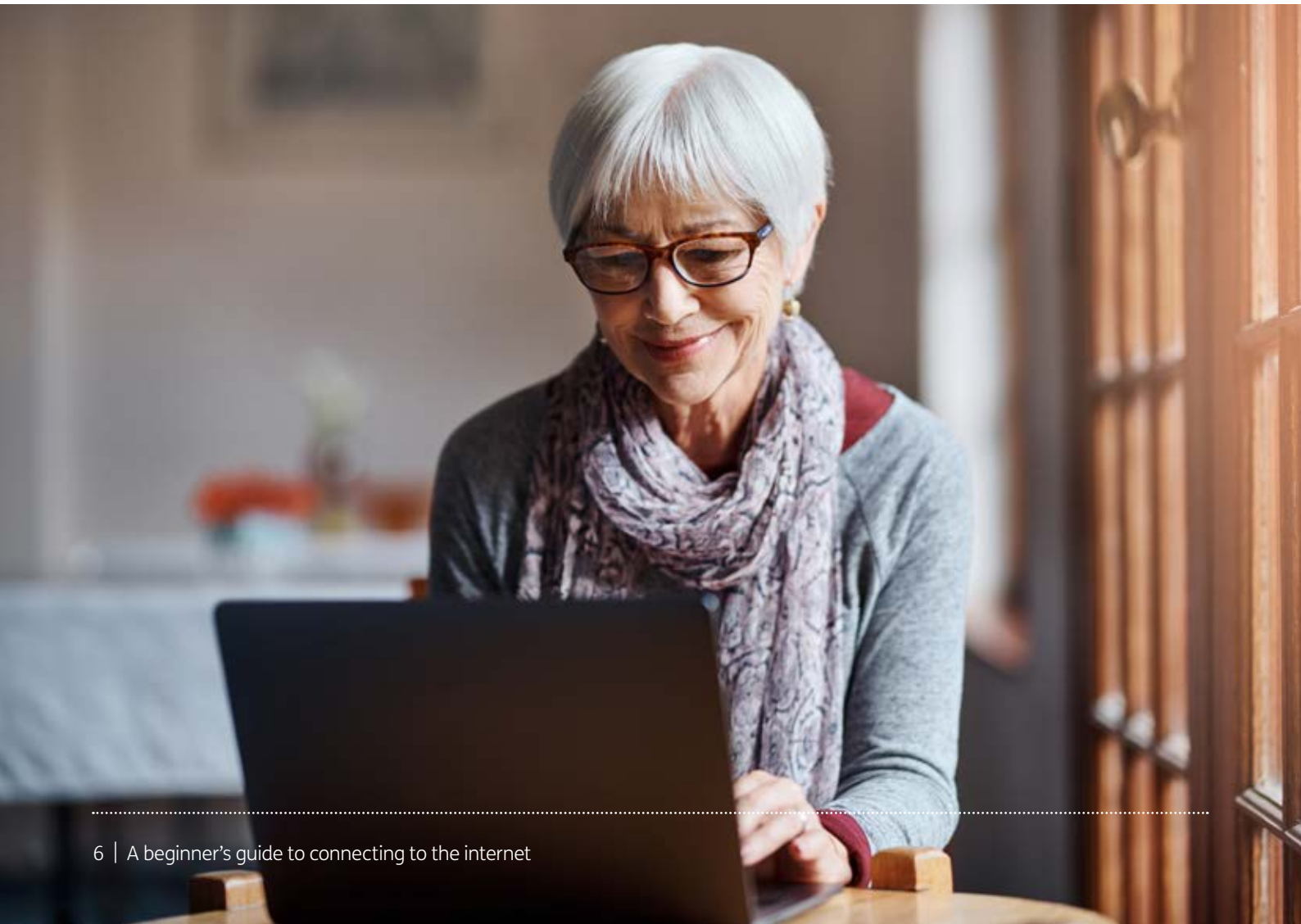
# **2.** Using this guide

## 2. Using this guide

This is a beginner's guide for people looking for practical tips to stay safe when using the internet. It includes sections on banking and shopping, with advice on how to manage your personal information and finances online.

Before reading this guide, you should:

- feel comfortable using a computer, laptop, tablet or smartphone
- have an internet connection.



# **3.** Understanding key terminology

## 3. Understanding key terminology

We've put together a helpful list of definitions which you can refer to while working your way through the guide.

**Address bar:** The bar at the top of your web browser, such as Google Chrome or Microsoft Edge. It's where the address of a webpage (also known as a URL) appears. You can type a web address straight into the address bar. For example, typing '**www.ageuk.org.uk**' and pressing the Enter key will take you to our website.

**Android:** The name of the software that many devices use to function. Phones and tablets from lots of different brands fall into the bracket of Android devices. These brands include: Alcatel, Google, HTC, LG, Moto, Samsung and Sony.

**Apple:** A brand of phones and tablets. Apple phones are known as iPhones and tablets are called iPads. If your device isn't Apple, it's likely to be an Android device.

**Device:** A general term for a smartphone, tablet, laptop or computer.

**Email:** It's a way of sending and receiving messages over the internet. It's free and quick to use and has replaced letter writing as the most common way to keep in touch.

**Fingerprint log in:** Instead of entering a password (see below), you place your finger on the screen or home button of your device to log in to an account.

**Hardware:** This describes the physical parts of a computer such as the screen, mouse and keyboard.

**Internet:** Also known as the world wide web, this a large network that connects computers and devices around the world through which you can access information. You'll see the abbreviation 'www' at the beginning of web addresses. For example, our website is **www.ageuk.org.uk**.

**Password:** Your password is chosen by you and keeps your email account secure. The National Cyber Security Centre recommends you use three random words as your password, for example, 'cupwalldog' or 'raincowbox'.

**Phishing:** A type of fraud where scammers trick you into clicking on a bad email link or giving away sensitive information. Often online phishing scams take you to a fake website or convince you to download malware onto your device.

**Scam:** A fraudulent act designed to trick people into sharing their personal information or money. In this guide, we'll explain the different type of scams and what to look out for, so you feel confident going online.

**Security certificate:** A piece of information on a website which shows that the website is secure and what it claims to be. If a website has a security certificate, you'll see a padlock symbol. This will be to the left of the website address in the address bar. A security certificate is also known as a digital certificate or a Secure Socket Layer (SSL) certificate.

## 3. Understanding key terminology

**Smartphone:** A mobile phone which connects to the internet. You can use it to do everything from sending emails to making video calls.

**Spam:** These are emails from people and organisations that you did not request. Usually, your email service provider will automatically filter these into your Junk folder. If in doubt, avoid opening any emails from unknown senders. Spam and junk emails are often used interchangeably.

**Spyware:** An unwanted program that runs on your device, which can make it slow and unreliable or make you a target for online criminals. Anti-spyware software helps protect your device against security threats caused by spyware.

**Swiping:** Moving your finger across the screen of a smartphone or tablet. You can read more about this in Age UK's 'A guide to making your device easier to use'.

**Tablet:** A small portable computer with a touch screen. You tap the screen with your finger or a special pen – often referred to as a 'stylus' – rather than using a keyboard and mouse.

**Touch screen:** A type of screen on a device that allows you to use your finger, or a stylus, to navigate and interact with content. This is an alternative to a mouse and keyboard.

**Viruses:** These are programs that spread from one computer to another by email or through websites. They can slow your computer down, display unwanted pop-up messages and delete files.

**Web/internet browser:** A program that runs on your device. It allows you to access webpages on the internet. Common web browsers include Microsoft Internet Explorer or Edge, Google Chrome, Mozilla Firefox and Apple Safari.

# **4.** Types of online scams

## 4. Types of online scams

Online scams are becoming increasingly sophisticated and many people are caught out, even those who are regular internet users. Getting online can make life easier in many ways, but it also comes with the risk of fraud. By knowing what to look out for and what to do if you suspect a scam, you can protect yourself and stay safe online. Here are some common online scams to look out for:

### Scam emails (also known as junk emails):

These are emails designed to trick someone into entering their personal or financial details. They may direct you to a fake website or tell you you've won a lottery or prize. Some emails may also have a link or file attached for you to click on or open. Opening these links or downloading the files may harm your device.

Scam emails can look genuine and appear to be from official places, like HMRC or a bank. But you can often tell it's a scam by looking out for the following:

- spelling or grammatical errors
- requests for personal information, such as your username, full password or bank details – genuine organisations will never ask for this
- threats that your account will be closed unless you take immediate action.

**TOP TIP**

If you see a suspicious email, don't reply with your details or open any links or documents. Delete the email straight away. If the email claims to be from an organisation, phone them directly using the phone number on their official website and ask them if they sent the email. To report a scam email, go to the Action Fraud website: **www.actionfraud.police.uk/report-phishing**

### Fake websites

These official-looking websites may ask you to provide personal or financial information. For example, a fake bank website may ask you to update your account or security information. Often, they will look very similar to the legitimate website and only a few details may be different.

There are also websites set up to look like a service offered by the government – for example, renewing a passport or getting 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.

**TOP TIP**

Visit your bank's website by typing their official web address in your internet browser. You can find this on letters from your bank. If you aren't sure which website to use for a government service, go to the UK government's official website – **www.gov.uk** – to find what you need.

## 4. Types of online scams

### Computer viruses

These are untrustworthy programs that spread from one computer to another. They might arrive in a spam email as an attachment, infecting your device when you click on it. Criminals might then use this to take control of your computer. A virus might also scan your computer for personal information, slow your computer down, send out spam email or delete files.

**TOP TIP**

Use anti-virus and anti-spyware to protect your computer from viruses. See page X for more information about this.

### Relationship scams

Scammers can use online social networks, like Facebook or dating websites, to trick you into giving them money. They'll often tell you an emotional or hard luck story to gain your trust. These tricks can be hard to spot, so it's always worth talking to a friend or relative about it – especially if things seem to be moving fast. A sign of this might be if the person wants to move away from the chat room or dating site to communicating by email or text message.

**TOP TIP**

If you start to talk to someone online, think very carefully before sending them money or giving them your account details. If you arrange to meet, make sure it's in a public place – and always tell someone else where you're going. Don't give away information too quickly.

### Health scams:

These are false and misleading advertisements for medical-related products, such as miracle health cures or fake online pharmacies offering medicines cheaply. The actual medicine delivered to you can be poor quality and even harmful to your health.

**TOP TIP**

Check if an online pharmacy website is legitimate by clicking on the 'Registered Pharmacy' logo on the website's home page. This should lead to the General Pharmaceutical Council website, which regulates pharmacies in the UK. You can also look for a pharmacy registered with the General Pharmaceutical Council on the regulator's website.

# **5.** Top tips to stay safe online

## How can I protect my privacy on social media?

Social networking websites, like Facebook and Twitter, can be a great way to keep in touch with family and friends, follow public figures and organisations, and meet people with similar interests or hobbies. But when using a social networking site, you should limit who can see your personal information. Sharing too much information can leave you at risk of fraudulent activity. Use the privacy features on the site to choose who can see your profile and the information you post. The security settings are different on each social networking website. Each has information on how to use the different privacy features. You should be able to find this information in the settings menu, under the 'Privacy' heading. Avoid publishing information that identifies you, such as your telephone number, address or date of birth.

## Top tips to protect your device

It's second nature to keep your valuables stored safely in your home and out of sight of burglars. But it's equally important to keep your personal information safe from criminals when you're online. As well as being alert to online scams, there are simple steps you can take to protect your device:

## Creating strong passwords for your online accounts

The National Cyber Security Centre recommends using three random words for strong passwords because they're easy to remember and strong enough to keep online accounts secure. For more helpful information, have a look at: **www.ncsc.gov.uk/section/advice-guidance/alltopics**.

Some websites might require you to use numbers, letters and symbols – in which case, you can incorporate these into your three random words.

Never write down your password. If you need a written reminder, try a hint that only you'll understand, rather than the actual password. If you do write anything down, keep that information somewhere safe and away from your computer.

## Installing anti-virus software on your computer

Going online can leave your hardware at risk from viruses. You can protect your device by installing anti-virus and anti-spyware software. Anti-virus software looks for and removes viruses before they can infect your computer. Anti-spyware software prevents unwanted adverts from popping up and stops programs from tracking your activities and scanning your computer for private data, such as bank details.

## Best buys: anti-virus and anti-spyware

You can buy a package from a reputable provider, such as McAfee or Norton, either online or from a computer shop. There are also free security software programs available online, such as AVG, Avast and Microsoft Security Essentials.

## How do I know if there is a virus on my device?

Here are some signs to look out for:

- Your device is running more slowly than usual.
- You have frequent pop-ups on your screen.
- You can't log into your computer or access your settings and files.
- Your security software has been disabled.
- Your battery life drains quickly.
- There are emails sent from your email account that you didn't send.

## Protect your tablet and smartphone

You can check emails, shop and bank online on tablets and smartphones, so they need protecting just like a desktop computer. Start by password-protecting any devices. You can download anti-virus and anti-spyware protection for tablets and phones and a lot of the apps are free. Some free, highly rated anti-virus apps are Avast mobile security, Kaspersky internet security and Norton mobile security.

## Protect your wireless network

You need to protect your wireless network, or wifi, so people living nearby can't use it. Read the instructions that come with your wireless router to find out how to set up a 'key' or password. If the written instructions don't come with the wireless router, your broadband provider will direct you to online instructions. Read Age UK's 'A beginner's guide to connecting to the internet' to find out more about this.

## Keep your device updated

Every device has an operating system, which is the software it needs to function properly. Computers use Windows or Mac OS, and tablets and smartphone use Android or iOS. Your device can be better protected from viruses if you keep the operating system updated. You should receive notifications when new updates are available, but you can also update your system manually. To discover if you need to upgrade your smartphone, check out Age UK's 'A guide to making your device easier to use'.

# **6.** Banking safely online

## 6. Banking safely online

Banking online is a secure way to manage your money from home or when you're out and about. There are steps you can take to keep your money and financial information safe.

### How do I set up online banking?

To access online banking, you'll need to register first. You need to have an account with the bank already, then register for online banking through their website. The safest way to find the website is to enter the web address into your browser's address bar – you should be able to find it printed on any letter you have from the bank.

Each bank has a slightly different process to set up online banking, and you should speak to your bank to find out about the process. Steps may include the following:

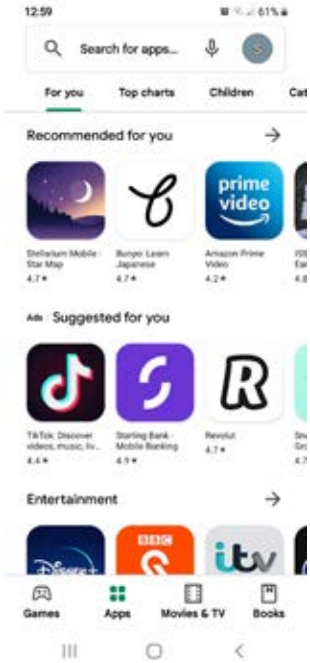
- Entering your personal details, including name, contact details and bank account details (sort code and account number).
- The bank arranging to call you and ask you some questions to verify your identity.
- Being sent an activation code, either in the post or by text message.
- Setting up a username and a secure password or passcode.

### How do I access my bank's app?

Most banks have their own apps for smartphones and tablets. Once you've set up online banking, you can download the app, which allows you to check your balance and send payments. You can find the apps in the Google Play Store for an Android phone, or the App Store for an iPhone.

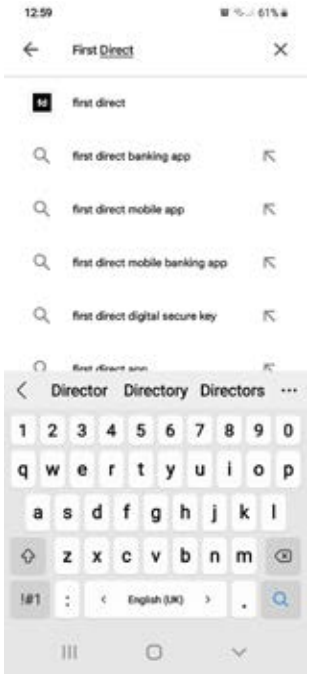
### Downloading a banking app on an Android phone or tablet

1. Open the Play Store from your phone or tablet's menu by tapping on the Play Store icon.



2. First, you'll need to set up a Google account or log in to your Google account. This is the account you'll use to access other Google services, like Gmail, a type of email account. It's important to set up a strong password to stay safe when using the internet and to never write it down – someone could find it and access your account. If you need a written reminder, write down a hint that only you'll understand, rather than the actual password. For more information, see page 14.

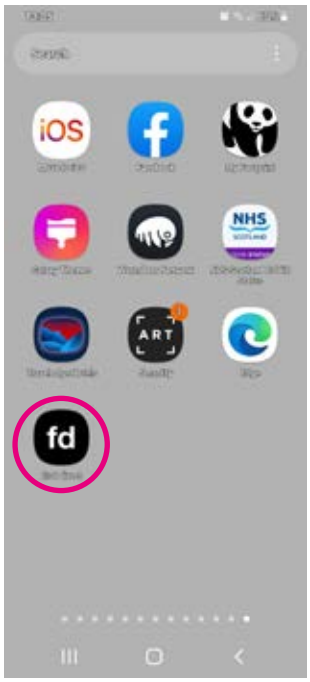
3. Search for a banking app, such as 'first direct' or 'Barclays' by typing it into the search bar at the top of your screen.




4. When you see it in the list that comes up, tap on the name of the app.

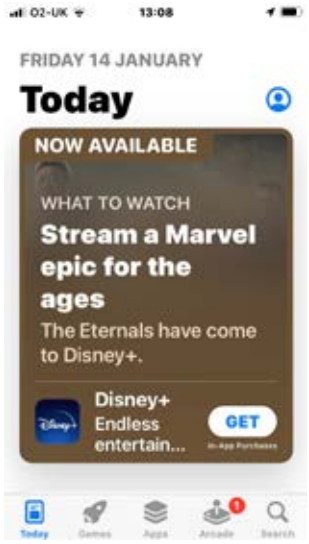
5. Tap 'Install', which is a green button underneath the app icon.

6. The app will download and automatically be added to your menu. If you've got a lot of apps already, you may run out of room for new icons. You'll need to 'swipe' across the screen to see the new app icon.



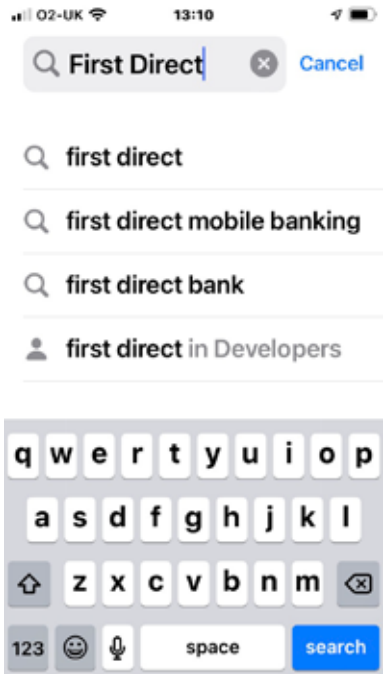

## Downloading a banking app on an iPhone or iPad

1. Open the App Store in your iPhone or iPad's menu by tapping on the App Store icon.

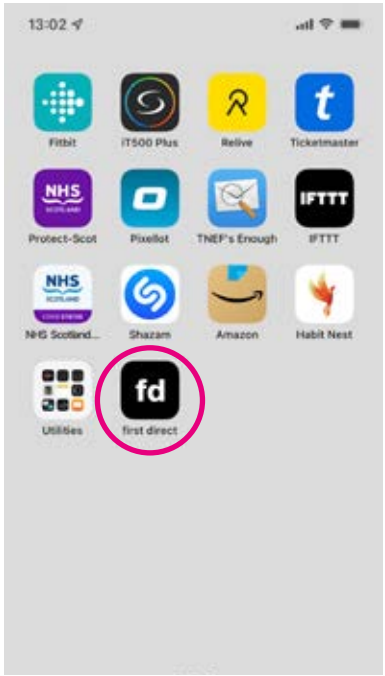



2. You'll need to set up an Apple ID or log in to your existing Apple ID account. This is the account you'll use to access Apple services. It's important to set up a strong password to stay safe when using the internet and to never write it down – someone could find it and access your account. If you need a written reminder, try to write a hint that only you'll understand, rather than the actual password. For more information, see page 14.

3. Click the 'Search' icon (the magnifying glass) at the bottom right of the screen. Search for a banking app, like 'first direct' or 'Barclays' by typing in the search bar.




4. Tap on the name of the app.
5. Tap 'Get' which is a blue button next to the app icon.
6. The app will download and automatically be added to your menu. If you have a lot of apps in your menu, you may run out of room for new icons, and you'll need to 'swipe' across the page to see the new app icon.



## 6. Banking safely online

### What can I use online banking for?

With most banks, you can use online banking to:

- check your balance
- check your bank statements
- transfer money between your bank accounts
- send money to people you know
- set up or cancel direct debits and standing orders.

### How can I check my bank transfer is safe?

Stop and double-check before making any payments. Do you know the person you're sending money to? Has someone phoned you out of the blue asking for money or claiming to be from your bank? Have you been put under pressure to make a payment? If something doesn't feel right, it's fine to stop and check the situation with someone you know and trust.

Some banks now have a warning when you transfer money to someone. This prompts you to think twice that the person you are sending money to is genuine and to double-check the details are correct.

If you're happy that the payment is to someone you know and trust, check the amount, name and account details of the recipient before you send it. Most banks now check account details against the name you enter. If this isn't available, ask the person who you're sending money to repeat their bank details. If you enter the details wrongly, it can be very difficult to get your money back

### What can I do to keep my money and identity safe?

There are steps you can take to protect your finances:

1. Don't re-use the same passwords for different accounts.
2. Use a strong password. The National Cyber Security Centre recommends using three random words for strong passwords because they're easy to remember and strong enough to keep online accounts secure.
3. Never share your full password or PIN number. Banks will never ask for your full PIN or password – instead, they will ask for specific numbers or letters, for example, the first and third character from your password.
4. Always log out of your online banking session once you're finished, especially if you use a device that others have access to.

5. Be cautious when using a public computer to access your online banking – for example, a library computer. They may not have the right level of security software. Ask the library staff for more information. Also, when using the internet in a public place, look over your shoulder to make sure no one is watching what you're doing.
6. Only use secure wifi networks to access your online banking. Don't use public networks, such as those in cafés or train stations. This is because it may be possible for people on the same network to access your details.
7. Check your balance and transactions regularly, and report anything you don't recognise to your bank.
8. Regularly check that your personal details are correct and up to date.

## How does the bank keep my money safe?

Banks take security very seriously and invest lots of time and money to make sure your online account is safe:

- **Bank websites are encrypted.** This means they are well protected from anyone seeing the information on the page or your personal details. The website address should start with 'https' – the 's' stands for secure.
- **Websites and apps have timed logout**. If you have been inactive for a set amount of time, it will automatically log you out, meaning that no one else can get into your account.
- **There are multiple steps to log in.** As well as entering your username and password, some banks send a text message with an access code.
- **Some banks will send you a card reader.** This provides an additional level of security to use when logging into your online banking. It's a small gadget that you enter your PIN number into. It then generates a unique passcode when you log in to online banking or make a payment online.
- **Some banks now have a warning when you transfer money to someone.** This prompts you to double-check the details are correct and to make sure that the person you're sending money to is genuine.

# **7.** Shopping safely online

## 7. Shopping safely online

Online shopping can make life much easier and takes the hassle out of going to the supermarket or shopping centre – but it's important to use safe and genuine websites.

You can shop online from most major supermarkets and high street shops, as well as smaller independent shops. Goods can be delivered directly to your house, usually for a small fee or for free, or you can also use a service called 'click and collect' where you order online but collect items in-store, or even from a local convenience store or newsagent. You can read Age UK's 'A beginner's guide to online shopping' for more information about setting up an online account with a supermarket.

### Tips for protecting your money and personal information when shopping online

- Use online retailers with a good reputation, such as well-known supermarkets, high-street shops or established online stores.
- Look for the company's full contact details. A reputable company will always display this information on its website.
- Search for the name of the company on the internet to see if anyone has experienced problems with the retailer.
- Beware of pop-up messages that warn you about a website's security certificate. They may direct you to a fake website that's designed to get you to hand over your security details.
- If a deal looks too good to be true, it probably is. Be cautious of anything offered in an unsolicited email.
- Use the same card for internet transactions only. Check the bank statement for this card regularly for any unusual transactions and contact your bank immediately if there's a problem.
- Use a credit card, rather than a debit card, for internet transactions for additional protection. If your purchase costs more than £100 and you use a credit card, the seller and your card company are equally responsible if anything goes wrong. It's important to remember to pay off credit cards on time to avoid additional costs.
- Consider using a PayPal account. This is an online account that you link to your bank account or payment card to pay for online purchases. It's secure and comes with more payment protection than a debit card. For more information, go to: **www.paypal.com**.

### What information will I give when I pay for something?

You'll never be asked for your card's personal identification number (PIN) when you pay for something online. Instead, you'll be asked for:

- the 16-digit card number on the front of the debit or credit card
- the expiry date
- the three digits on the back of your card, known as the security number, or 'CVV', 'CVC' or 'CVV2'.

## 7. Shopping safely online

When purchasing something online, you can set up an account with the retailer, which allows you to save your details and makes it quicker to place an order the next time you shop with them. Make sure to use a different password for each account, and always use a strong password.

Sometimes the website or your internet browser prompts you to save your card details for next time. Never do this on a shared computer, and make sure your device is protected with a password, PIN or fingerprint log in if you do save your card details.

### How do I know if a website is secure?

Make sure that you're using a secure website before entering any personal details. There are ways to spot that a website is secure, including:

the web address starts with 'https' – the 's' stands for secure

there's a padlock symbol in the address bar

there's a current security certificate registered to the correct address – this appears when you click on the padlock.

### Who to contact for help

If you've been a victim of an online scam, it's important to report what has happened. This will help stop other people being a victim too. You can report it to:

- the police on 105 (non-emergencies)
- Action Fraud on 0300 123 2040.

You can also talk to a loved one, friend or your Digital Champion about your concerns.

If you're worried that your computer isn't working properly and/ or think that it may have a virus, then talk to the stores where you purchased your device.

You can also contact the manufacturer of your device to find reputable computer technicians in your local area.

If you have an iPhone, iPad or Mac, Apple is the manufacturer: **https://support.apple.com/en-gb/contact**.

If you have an Android device, the main manufacturers include Huawei, Lenovo and Samsung: **https://support.google.com/android/answer/3094742**

For Windows devices, go to h**ttps://support.microsoft.com/en-gb**

## Next steps

Once you feel comfortable with the information in this guide, read our intermediate guide to:

- learn how to safely set up accounts on websites and create strong passwords.
- use security measures such as encryption and two-factor authentication.

We hope you've found this guide useful and feel more confident about using the internet safely.

If you feel you need some extra support, your local Age UK or local Age Cymru may be able to help. You can find your local Age UK at **www.ageuk.org.uk/services/in-your-area**

**My Age UK Digital Champion**

Telephone number:

**Notes**

We provide advice and information for people in later life through our Age UK Advice line, publications and online.

**Age UK Advice: 0800 678 1602**

Lines are open seven days a week from 8am to 7pm.
You can find more information at **www.ageuk.org.uk**