A be e de
a a e e

Helping you to stay safe whilst online

Publication date: February 2022

Contents

1. Introducing you to online safety

1. I d c e a e

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 inform-2.34k8d as wuninoo 5 (w I h)-.34k8 3 Tm[(t)1duts

2.

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: 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,SQ1 0 0 1 261.0236 116.3682

3. Understanding technical terms

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.

Swipe: 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.

Touchscreen: 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.

Virus: 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/ web 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. T e e ca

C e

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.

Re a ca

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.

Hea ca :

5. Top ti. 5.

5. T a a e e

H ca I ec ac c a ed a?

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.

T ec de ce

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:

C ea a d e acc

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.

I a a - a e c e

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.

Be b :a - a d a - a e

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.

H d I e e a de ce?

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.

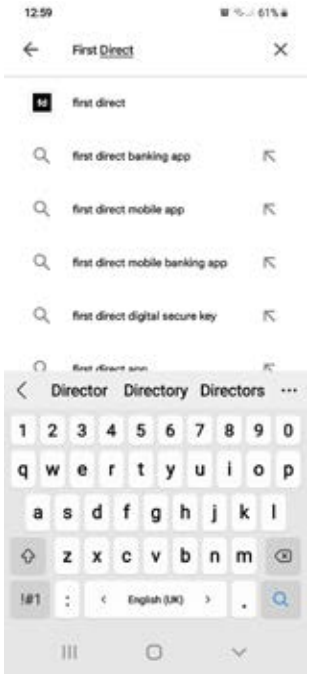
P ec ab e a d a e

You can check emails, shop and bank online on tablets and smartphones, so they need

6. Banking safely online

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.

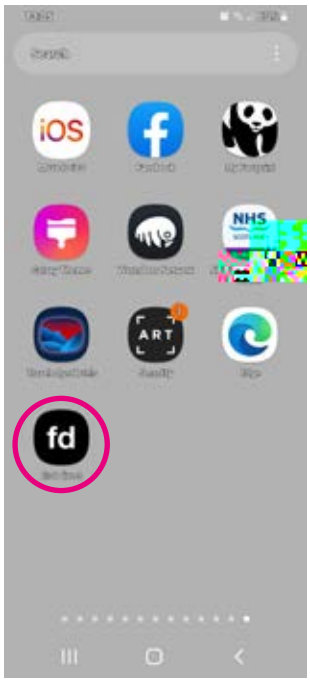
3. Search for a banking app, such as 'first direct' or 'Barclays' by typing it into the search bar at the top of your screen.



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

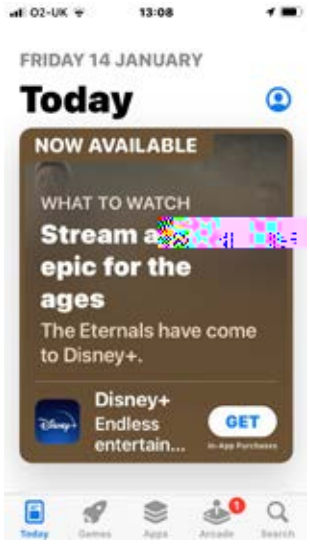
5. Tap 'Install', which is a green button underneath the app icon.

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.



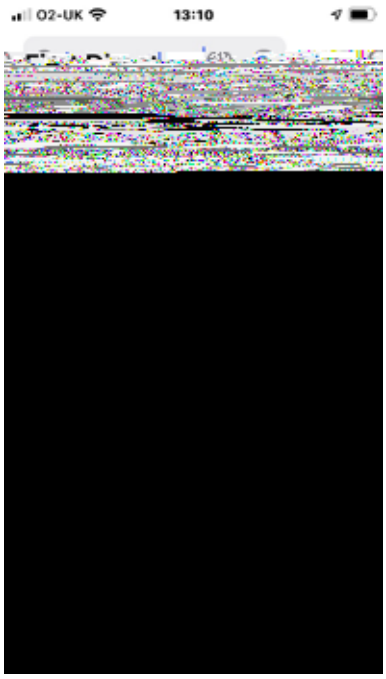
D ad a ba . a P e Pad

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

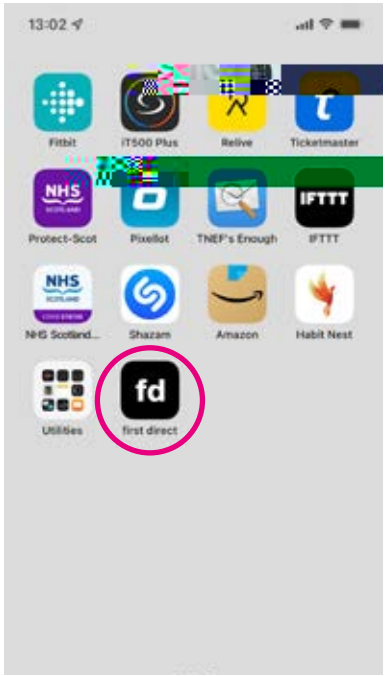


2. You'll need to set up an Apple ID or log in to your existing Apple ID account. This is the account you'll use to access Apple services. It's important to set up a strong password to stay safe when using the internet and to never write it down – someone could find it and access your account. If you 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.



W a ca I e e ba ?

With most banks, you can use online banking to:

- check your balance
- check your bank statements

7. Shopping safely online

7. S[illegible]

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

7. S[illegible] a[illegible]e

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.

H[illegible] d[illegible] I[illegible] [illegible] a[illegible] eb[illegible] e[illegible] ec[illegible] e?

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.

W[illegible] [illegible] c[illegible] ac[illegible] [illegible] e[illegible]

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**

7. S

Ne

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**

M A e UK D a C a

Telephone number:

N e

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

A e UK Ad ce: 0800 678 1602

Lines are open seven days a week from 8am to 7pm.
You can find more information at .a e