An intermediate guide to staying safe online

Helping you to stay safe whilst online

Publication date: February 2022

Contents

1. Doing more to stay safe online

1. Doing more to stay safe online

Hello,

Welcome to Age UK's intermediate guide to staying safe online. Now that you've read our beginner's guide to staying safe online, you'll be confident learning about security tools, like two-factor authentication and password managers.

Before I started using these tools, I was quite nervous about using the internet. Now I know how to create strong passwords and set up two-factor authentication, I feel a lot more confident getting online.

Learning at your own pace

Take your time working through this guide and repeat 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/**.

I hope you find this guide helpful and that it helps you feel more confident using the internet.

Elsie, 82

2. Using this guide

2. Using this guide

This is an intermediate guide for people looking for extra ways to stay safe online. In this guide, we'll introduce you to using a password manager, a type of program that manages your passwords for different online accounts so you don't have to remember them. We'll also explain what two-factor authentication and encryption mean.

Before reading this guide, you should:

- feel comfortable using a computer, laptop, tablet or smartphone
- have an internet connection
- be aware of the types of scams to look out for
- feel comfortable setting up a strong, secure password.

If you'd like to learn more about these things first, see Age UK's 'A beginner's guide to connecting to the internet' and 'A beginner's guide to staying safe online'.

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. Some of these were in Age UK's 'A beginner's guide to staying safe online' – it will be helpful to remind yourself of these when working through this guide.

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

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

Encrypted: If an app or a website is encrypted, it means all the communication between you and the website is secure and can't be read or heard by anyone else. Encrypted websites have web addresses that start with 'https'. The 's' stands for secure. A web address is at the top of the screen.

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.

Icon: An image or symbol which represents an app or function on your phone, tablet or computer screen.

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**.

Operating system: The software that manages different programs on your device. Examples include Android for certain smartphones, like Samsung, Google, Sony, LG and Moto, and iOS for Apple devices.

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.

Program: A catch-all term for something that runs on your computer, laptop, tablet or smartphone. Examples include apps on your phone and tablet, or anti-virus programs. You might also see them described as 'software'.

3. Understanding key terminology

Scam: A fraudulent act designed to trick people into sharing their personal information or money. In Age UK's 'A beginner's guide to staying safe online', we explained the different types 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.

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.

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', to use the device rather than using a keyboard and a '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.

Two-factor authentication: An additional form of online security that helps to verify who you are. You might be asked to do this when you try to log into an online account. Usually, once you enter your password, you'll need to type in a code sent to your email account or your phone to confirm your identity.

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. Creating online accounts with strong passwords

4. Creating online accounts with strong passwords

When setting up an online account on a website or app, such as a supermarket website or the NHS app, it's important to create a strong password. In 'A beginner's guide to staying safe online', we gave you some tips for creating strong passwords. Avoid weak passwords that people can guess, and don't use the same password for all your accounts – this makes it easier for someone to guess it and get into your accounts.

Using a password manager

Some web browsers have built-in password managers. These are programs that remember your passwords for different sites and fill them in for you automatically when you need them.

When you log in to a website for the first time, the password manager will ask you if you want it to remember your password. You can choose whether you want it to or not. It can save time to use this function, but only do this on your own personal computer rather than a device that others use or a community device, for example in a library. The next time you visit the same website, your email address and password will come up automatically. For example, when you type the beginning of your email address, your email address will appear.

Password managers make it easier to use different strong passwords for each online account you have, because it remembers them for you.

If you decide to use a password manager, make sure you set up a password or PIN to access your device. Your log in details will be available to anyone you share your device with so make sure you only share it with people you trust. Remember, don't use the password manager anywhere public, like the library.

There are also password manager apps which are available to download on your smartphone or tablet. These offer more security for your passwords. A good free password manager app is Bitwarden. See Age UK's 'A beginner's guide to using apps' to find out how to download apps.

Make sure you set up a password or fingerprint login for your device. If your smartphone or tablet is lost or stolen, it will prevent anyone from logging in to your accounts using the password manager.

5. Further security measures

Two-factor authentication

Two-factor authentication is an additional form of online security that helps to verify who you are. You might be asked to do this when you try to log into an online account. Usually, for two-factor authentication, once you enter your password, you'll need to type in a code that is sent to your email account or your phone to confirm your identity. It stops people from getting into your account with nothing more than your password.

You can choose to set up two-factor authentication on your device. See instructions below for how to do this:

Two-factor authentication on an iPhone, iPad and Mac

You can set up two-factor authentication for your Apple ID account. This will make sure you're the only person who can get into your account, even if someone else knows your password.

With two-factor authentication, only you can access your account on what is called a 'trusted device'. A trusted device is an iPhone or iPad (with an iOS 9 operating system or later) or a Mac (with OS X El Capitan or later) that you've already signed in to using two-factor authentication. It will be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser.

When you want to sign into a new device for the first time, you'll need to provide two pieces of information – your password and the six-digit verification code that's automatically displayed on your trusted device or sent to your phone number. By entering the code, you're verifying that you trust the new device.

This is how to turn on two-factor authentication on an iPhone and iPad:

1. Go to 'Settings' and then tap 'Password & Security'.
2. You may then be asked to enter your password for your Apple ID.
3. Next, tap 'Turn On Two-Factor Authentication'.
4. Tap 'Continue'.
5. Enter the phone number you want to receive verification codes on when you sign in. You can choose to receive the codes by text message or through an automated phone call.
6. Tap 'Next'.
7. Enter the verification code to verify your phone number and turn on two-factor authentication. You may be asked to answer your Apple ID security questions.

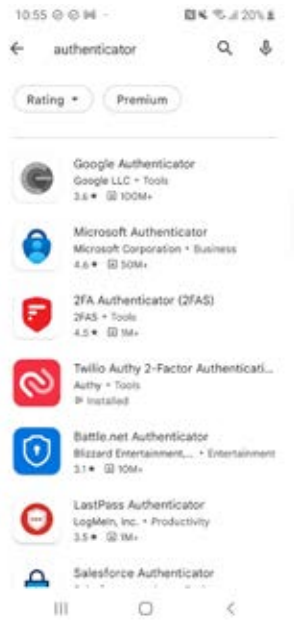
This is how to turn on two-factor authentication on your Mac:

1. Click 'Apple menu', 'System Preferences' and then click 'Apple ID'.
2. Click 'Password & Security' under your name.
3. Click 'Turn on' next to 'two-factor authentication'.

Source: Two-factor authentication for Apple ID – Apple Support (UK)

Two-factor authentication on an Android device

You need to download an app for an Android device in order to set up two-factor authentication. These include Google Authenticator and Microsoft Authenticator.



Downloading a two-factor authentication app on an Android phone or tablet

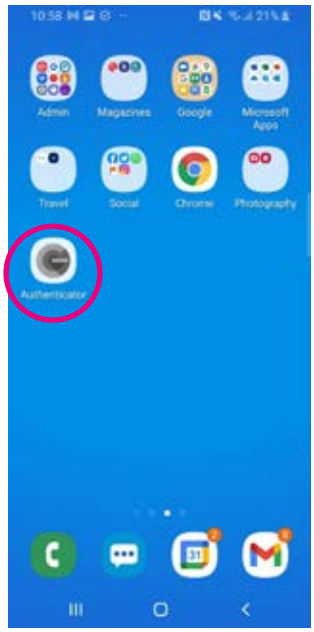
1. Open the Play Store from your phone or tablet's menu by tapping on the Play Store icon.

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 (see Age UK's 'A beginner's guide to email'). 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.

5. Further security measures

3. Search for the app by typing the name 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.



Turning on two-factor authentication on a Windows PC

You can set up two-factor authentication on Microsoft:

1. Go to your online Microsoft account and log in. If you don't have an account, follow the instructions to set one up at **www.microsoft.com**.
2. Click on the 'Security' tab in the menu and then click on 'More security questions'.
3. Next, click on the 'Two-step verification' option and then 'Set up two-step verification'.
4. On the next screen, choose an option under 'Verify my identify with'. You can choose an app, a phone number or an email address.
5. Once you've verified your phone number, email address or app, two-factor authentication is set up.

Encryption

If an app or a website is encrypted, this means that all the communication between you and the website is secure and can't be read by anyone else. Encrypted websites have web addresses that start with 'https'. The 's' stands for secure.

In Age UK's 'A beginner's guide to video calling', we talked about WhatsApp. This messaging and video calling tool is a good example of an encrypted app. Your messages and calls are automatically protected so only you and the person you're talking to can read what is sent or hear what is said. Be aware that encryption doesn't remove all risk so you should be careful of potential scams.

Other safety factors

It's important to be vigilant when using WhatsApp. There have been scams such as people posing as family members and hijacking accounts. If you receive a message asking you for money, call your friend or family member to check if it's from them. Also, never give a password or text message security code to anybody, including your friends or family.

Next steps

Once you feel comfortable with the information in this guide, you can put your knowledge into practice and read our other guides:

- A beginner's guide to shopping online
- A beginner's guide to my local services
- A beginner's guide to using apps

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**