An advanced guide to email

Helping you to stay in touch

Contents

1. Sharing your email address and spotting scams

1. Sharing your email address and spotting scams

Hello,

Welcome to Age UK's advanced guide to email.

In our beginner's guide, we showed you how to set up an email account and send an email to family and friends. We followed up with an intermediate guide, where we explained how to do tasks like replying to messages and organising your Inbox. We also showed you how to identify and flag spam and junk emails.

In this guide, we'll show you how to use your email address to sign-up to email newsletters and activate online accounts, such as shopping accounts.

Keeping your email safe

You might be wary of sharing your email address with others, which is completely understandable. I felt the same myself. But, once I got the hang of setting up online accounts using my email address and familiarising myself with basic web security, I realised it's not as daunting as I first thought.

This guide will take you through the basics of sharing your email address and spotting scam websites so you feel more confident setting up online accounts. We'll also give you some tips on how to keep your email account safe and secure.

Learning at your own pace

You can go through the guide by yourself, with the support of an Age UK Digital Champion, or with the help of friends, family and carers. Work through each section at your own pace so you can familiarise yourself with what you need to do and practise.

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/**

Enjoy making the most of your email account.

Dereck, 75

2. Using this guide

2. Using this guide

This is an advanced guide for people who want to learn more about using email. To use this guide, you'll need to have already set up a Gmail or Outlook email account. If not, please go to 'A beginner's guide to email' to learn how to do this.

You should also have a basic understanding of how your email account works and feel confident sending and replying to emails. If you're unsure, please see 'An intermediate guide to email' for tips.

In this guide, we'll talk you through examples of when you might share your email address with others and things to look out for if you're sharing your email address online. We'll also explain how to keep your personal information safe online.

Before reading this advanced guide, you should feel comfortable:

- using a computer, laptop, tablet or smartphone
- connecting to and browsing the internet
- logging on to your Gmail or Outlook email account.

3. Understanding key terminology

3. Understanding key terminology

To help you get to grips with sharing your email address and understanding basic website security, we've put together this useful list of common words and phrases that you may come across. These are in alphabetical order so can you refer to them easily when working through this guide.

Attachment: Any file, photograph, video or document you add to your email is known as an attachment. An email with an attachment is indicated by the symbol of a paperclip.

Cloud storage service: This is a way of storing and saving your files remotely on the internet, rather than on your device. It means if you damage or lose your device, your files will still be available. Examples of cloud storage services are Dropbox, Google Cloud Storage and iCloud.

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.

Email address: When you set up an email account, you'll choose an email address. This is how people send you email and is similar to a postal address in that it's unique to you. An example is joe.bloggs@gmail.com (the '@' sign is pronounced 'at').

Email app: Most email service providers have their own apps. These are a good way to access your emails quickly without logging into emails through your web browser.

Email newsletter: These are emails you receive from a business or organisation that shares the latest news and offers about their product or services. You should only receive email newsletters from companies you have signed up to.

Email service provider: To send an email you need to have an account and email address with an email service provider like Gmail or Outlook. These are online services that let you send, save and organise your emails and keep your account secure.

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.

Inbox: The virtual folder in your email account where any emails you receive are stored. Any new and unopened messages will sit in your inbox.

JPEG: A type of image file. When you upload or download images to your device they will usually save as a JPEG or a PNG file.

3. Understanding key terminology

Junk: Like the unsolicited mail you get through your letterbox, junk emails are messages from businesses advertising products and services. You can easily unsubscribe from these emails at any time.

Malware: This is malicious software intentionally designed to cause damage to your device. Cyber criminals will use malware to access sensitive data from your computer, such as your online banking information.

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.

Opt-in and opt-out: Often when you carry out a transaction online, like buying a product or booking tickets, you'll be asked if you'd like to opt-in to email communications from that business. If you opt-in, they'll add you to their mailing list and send you emails from time to time. If you choose to opt-out, you won't be added to the mailing list.

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'.

PDF: This is short for Portable Document File – a useful way of saving documents you wish to send as attachments in an email.

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.

PNG: A type of image file. When you upload or download images to your device they will usually save as a PNG or JPEG file.

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

Search bar: A box in a search engine where you can enter a topic to search for information on the internet.

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.

Subject line: A short summary or title of what your email is about, for example 'Holiday update'. You can enter this into the subject box at the top of the email.

3. Understanding key terminology

Subscribe: To sign up to receive emails from people, businesses or organisations. By sharing your email address and opting in to their mailing list, you are subscribing to their marketing emails.

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 'mouse'.

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

Unsubscribe: If you no longer wish to receive emails from a particular business or organisation you can opt out of their mailing list. Usually, you can do this by clicking the 'Unsubscribe' link at the bottom of their last email.

Username: When you set up your email account, you might be asked to enter a 'username'. You can choose your username, assuming what you want isn't already being used by someone else. You might want your username to be your name or a nickname.

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.

Webmail: A way of accessing your email through your web browser.

Wireless network, or 'WiFi': How your phone, tablet, laptop or computer connects to the internet without using wires or cables. You can access public WiFi networks, for example when out and about, or arrange a contract with an internet provider so you can use WiFi at home.

4. When to share your email address

4. When to share your email address

Email is a great way to keep in touch with people and is much faster and more efficient than traditional letter writing.

As well as communicating with friends and family, you might use your email address for other purposes, including:

- signing up to email newsletters
- shopping online
- online banking
- paying bills online.

We'll go into each of these in a little more detail, so you can get to grips with when it might be appropriate to share your email address.

Signing up to email newsletters

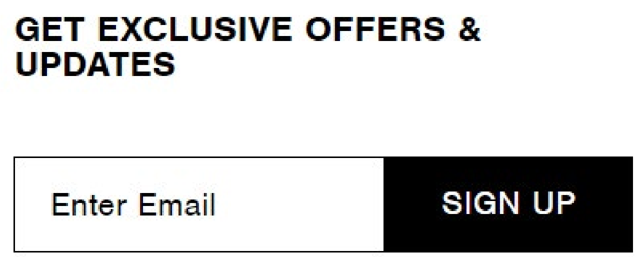
Many companies and organisations send out email newsletters to their customers sharing their latest news, updates and offers.

A retailer, for example, might send customers emails about their latest sales and offers. A charity might send out a newsletter to their subscribers about their latest fundraising campaign.

If you shop somewhere regularly, you might also receive a newsletter offering you a special discount code or voucher to receive money off your next purchase.

Email newsletters are a great way to keep up to date with companies and organisations you like. To receive email communications, you need to opt in to an organisation's mailing list.

You can do this by going directly to their website and usually somewhere on the homepage you'll find an email sign-up box. Here is an example from M&S:



GET EXCLUSIVE OFFERS & UPDATES

4. When to share your email address

Another way to sign up to email newsletters is when you buy something online. Often when you're about to pay online, you'll be asked if you'd like to opt in to receive email marketing from the company you are buying from and any third parties they are associated with. If so, you can tick a box confirming that you'd like to be added to their mailing lists.

If you decide you no longer want to receive these emails, you can unsubscribe. **See page 18** for more details on unsubscribing from emails.

Note: sometimes companies ask you to opt out of receiving email marketing, rather than to opt in. This means you'll be automatically added to the mailing list unless you tick this box. The easiest way to know if or not you're signing up for email newsletters is to read the small print.

Using your email address to shop online

Whenever you shop for goods or services online, you'll be asked to share your email address. This is so the company can send you an email to confirm your order and to notify you when it has been dispatched.

It's generally safe to share your email address when shopping online with a legitimate company. For tips on knowing if a website is legitimate or not, **see page 20.**

It's worth noting that even though you are sharing your email address with a company, this doesn't give them the right to start sending you unsolicited emails. Under the Government's data protection guidelines, if you have opted out of a company's mailing list for other marketing, they should only email you about orders you make. For more information about data protection, go to **www.gov.uk/marketing-advertising-law/direct-marketing.**

Using your email address to sign up to online banking

You may have already read our 'A beginner's guide to doing shopping online'. Online banking is a great way to keep track of your finances without having to go into a high street bank. Each bank has a slightly different process to getting set up online, so it's best to contact them directly to talk through exactly what you have to do.

As part of the sign-up process, you'll be asked to share some personal information, including your email address. This is so your bank can notify you when your latest account statements are ready to view (if you've opted for paperless billing) and to keep you updated with their latest news and offers.

Your bank will never email you to ask you to transfer money or send them your login details or password. If you do receive an email like this, it is most likely a scam and should be ignored.

4. When to share your email address

If you're ever unsure whether an email is genuine, use a trusted phone number to contact your bank to make sure. Never use a contact number from an email you're suspicious of.

Using your email address to pay bills online

Most utility companies like gas, electric, broadband and phone companies encourage you to set up online accounts to keep track of your latest bills and tariffs, rather than send mail in the post.

To access this information, you need to register an online account with your utility provider. Usually this will require entering your name, account number, email address and setting a password.

If you are a new customer, this can usually be done online when you sign up.
If you are an existing customer, you might need to call the utility company to request instructions or information. Have your account information handy when you call so they can easily identify who you are.

Once you have created your online account, you can opt in to paperless billing.
This means rather than send you bills in the post, they'll email you to let you know when your latest statement is ready to be viewed online.

5. Authorising your email address

5. Authorising your email address

Most websites ask you to confirm your email address before they add you to their mailing list. They usually do this by sending you an automated email with a link to confirm your email address.

It will usually say something like: ‘Thank you for signing up to our mailing list. To confirm your subscription please click here.’ It will then give you a web link to click on.

If you are confident you have signed up to the mailing list, then click on the link, which will take you to the company or organisation’s website and to a page that will say something like: ‘Thank you. Your email subscription is now complete’.

This means you will now receive regular email correspondence from that particular company or organisation.

If you receive an email like this that you weren’t expecting from a company, don’t click on it. Instead, mark it as spam or junk mail.

6. Unsubscribing from mailing lists

6. Unsubscribing from mailing lists

If you've ticked a box to opt in to regular emails from an organisation that you no longer want to receive, there's usually an option at the bottom of the email to opt out.

Open the latest email you received from them and scroll to the bottom of the email. Usually, you'll find the word 'Unsubscribe' in small print. Click on it and it should take you to a website where you'll be asked to confirm that you no longer wish to receive emails from them.

Once you've done this, you will be removed from the company's mailing list and should no longer receive their emails.

7. Protecting your personal information online

7. Protecting your personal information online

Going online makes life easier in a lot of ways but there is also risk of scams or online fraud. This is why it's important to familiarise yourself with some basic online security.

How to spot fake websites

One of the ways cyber criminals try to access your personal information and bank details is by pretending to be a legitimate company. They do this by setting up a fake website that looks really similar to the real thing to dupe you into entering your details.

Useful tips on spotting fake websites are to:

- **Check the web address (domain name).** Scammers will often use web addresses that reference the products they're selling but they'll look questionable. For example, a website pretending to be Apple might use the name www.ipadsforeveryone.org. Or a website pretending to be easyJet might use the name www.cheapflightsforall.net. To protect your personal information, only shop using official retailers.
- **Look for 'https' at the start of the web address.** This indicates that the website is secure and any personal information you share, including your email address, will be encrypted. Websites that begin with just 'http' are not secure.
- **Avoid 'too good to be true' offers.** If you click on a website with high value items at really low prices, chances are the website is untrustworthy. The goods are either fake, stolen or don't exist at all, meaning you could be conned out of your money if you make a purchase.
- **Browse the website.** Scan the website to see if it looks legitimate. Signs of fake websites include spelling mistakes, poor product descriptions and a lack of contact information. Any company selling goods or services should provide a company address, phone number and/or email address.
- **Check the ways to pay.** Legitimate websites will never ask you to pay by bank transfer. They'll ask you to pay through a secure payment platform, using your debit card or credit card or a money transfer service like PayPal. Avoid paying for goods and services by transferring money directly into someone else's account as you might never receive the goods and it can be difficult claiming your money back.

More online security tips

As well as following the tips already mentioned in this guide, there are a few more things you can do to stay safe online:

- **Choose strong passwords.** As mentioned in our 'Beginner's guide to email', it's important that you choose different passwords for different online accounts. If you have the same password for everything you are exposing yourself to hackers. The National Cyber Security Centre recommends you use three random words as your password, for example, 'cupwalldog' or 'raincowbox'.

- **Keep your devices up to date.** It doesn't matter whether you use a laptop, computer, smartphone or tablet to go online, you need to make sure your operating system and apps are up to date. Developers release new computer programs all the time to fix bugs and install the latest security. If you get a notification on your device telling you an update is available, don't ignore it.
- **Think before using online accounts in public.** While it might be tempting to log-on to your online accounts, like your bank, using public WiFi, it's best avoided. This is because it's easy for cyber criminals to access these public WiFi networks and hack into your browsing history and online accounts.
- **Don't overshare.** If you're new to going online, you may have decided to set up a Facebook or Instagram account to keep in touch with friends and loved ones. There's absolutely nothing wrong with interacting with others online but be careful what you share on public platforms. Hackers can use your social media profile to guess your online passwords and answer security questions about you. To stay safe, boost your privacy settings and limit who can see your social media accounts to people you know.

For more tips on protecting your personal information online, read 'A beginner's guide to staying safe online'.

We hope you've enjoyed working your way through this guide and now understand how to use your email address to sign-up to online accounts. We also hope you found the online security guidance helpful.

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**

Age UK is a charitable company limited by guarantee and registered in England and Wales (registered charity number 1128267 and registered company number 6825798). Registered address: 7th Floor, One America Square, London EC3N 2LB. Age UK and its subsidiary companies and charities form the Age UK Group, dedicated to helping more people love later life. ID204747 01/22.