Sending and receiving emails

Setting up an email account is really helpful – not only can you send emails to friends and family, but you'll probably need an email account for lots of the other things you might want to do on the internet, such as shopping or banking.

This sheet will:

1. **Help you set up your own email account.**
2. **Help you send your first email.**
3. **Help you look out for dodgy emails.**

Setting up your account

First things first, before you can start sending and receiving emails you need an email account. So, how do you set one up?

Step 1: Pick a provider

Before you set your account up, you'll need to decide who to set the account up with. There are lots of different providers, but some of the most widely used are Google Mail (Gmail), Yahoo and Outlook so they're a good place to start.

Step 2: Create the account

Whichever provider you use, you can set up your account on their website. When you've searched and found the website you're after, there's likely to be an option to 'Create an account' or something similar. Give that a click.

Step 3: Fill out your details

You'll be asked to fill out your details – this may be used to verify your account, so you'll likely receive a text with a code that's needed to open the account.

What is a 'strong' password?

A strong password is likely to include a mixture of letters (including capitals), numbers and special characters. It can also be three random words such as YellowTableSink (don't use this example though).

Whatever password you're creating, the website should make it clear if it needs to meet certain criteria and indicate how strong your password is. Don't use the same password for different accounts and never use personal details, such as important names or dates.

Spotting dodgy emails

Whether you're sending your first email or you've sent hundreds, everyone can fall victim to email scams. It can be unsettling, but the tips below can help you know what to look out for.

Fake websites: Scammers can create websites that look official (such as the HMRC) and ask for your personal and financial information or claim an account of yours has been compromised and you need to log in to sort it via the email. These are known as 'phishing' emails.

Spam or junks emails: Sometimes there'll be an attachment on an email. You'll be encouraged to open it and it can download things to your computer or harm your device (malware).

Prize emails: These are emails that claim you've won a prize and suggest you have to be certain things to claim it.

Emails claiming to be from people you know: These won't actually be from people you know, but can look like they are. They might ask for money or say they're in need, or might just encourage you to open a harmful attachment. It's likely their account has been hacked. If it looks suspicious, get in contact with that person (not via email) and ask them if they sent it.

If an email seems at all suspicious because it doesn't sound like the person, it seems too good to be true or there are spelling and grammar errors then it's probably a scam.

Notes

We've added this section in so you can jot down some notes. This could be handy little tips you come up with that help you remember things as you go along, or notes and suggestions someone else gives you if they're helping you through this sheet.
Remember not to write down any personal information or passwords.

Age UK is here is for you

If you need more information about getting online or making the most of your device, you can use your new skills to go to our website. There's more information, as well as links to other helpful websites and resources.

Visit us at **www.ageuk.org.uk/get-online**

For more general information and advice, don't hesitate to get in touch. You can:

- Visit us online at **www.ageuk.org.uk**
- Call the Age UK Advice Line on 0800 169 65 65 (8am-7pm, 365 days a year)
- Contact your local Age UK.