Staying safe online

While you're getting to grips with using the internet you might be particularly worried about using it safely. But the truth is, anyone can fall victim to an online scam or virus. The key to staying safe is thinking about what you're doing online and knowing the things to look out for.

This sheet will:

1. **Highlight what sort of scams are out there and what to look out for.**
2. **Help you know what to do if you fall victim to a scam.**
3. **Help you know what you can do to be as safe as possible.**

Knowing what to look out for

Whether you're online for the first time, or you've been using the internet for years, you can fall victim to a scam. They can be complex and are designed to catch you out. But some of these scams are more common than others. Before you worry about what you can do to stay safe, it's a good idea to know a bit about the sort of scams you might come across.

Email scams

Scammers send emails to try and get you to give them your personal details. They might either try and direct you to a fake website, claim something's wrong with an account or device you own or claim you've won a prize.

Sometimes there might be a file attached to the email. The scammer wants you to open or download this as it could harm your device by releasing or downloading a virus (malware).

You should look out for:

- Errors in the spelling or grammar, or wording that just doesn't seem quite right.
- Requests for personal information, such as usernames, password or bank details.
- Anything that's time-sensitive and wants you to act fast.

Top tip

Don't open any attachment or click on any links that you're suspicious of.

Fake websites

Scammers set up fake websites as a way to get your personal information. This could be a fake banking website where they ask you to update your details or account information, for example.

There are also websites set up to get you to pay for free services. These are usually government services, such as renewing your passport.These websites aren't illegal, but are set up to make you pay for free services.

You should look out for:

- Although these websites are designed to look very similar, look out for any details of the website that don't look quite right.

Top tip

Don't fill out any personal details or make any transactions on a website until you're sure it's safe. If online banking, always search for the website yourself.

Other scams to be aware of:

- **Relationships scams:** some people will use social media or dating websites to contact you. They try to gain your trust and then might start asking for money, often by telling an emotional story. These can be hard to spot, especially for those directly involved, so it's always good to talk to someone else about the situation if you're suspicious. Never send personal or financial details.
- **Health scams:** scammers make false or misleading claim about certain products, such as miracle cures. These medicines can be expensive, poor quality and in some cases even harmful.

What to do if you fall victim to a scam

Anyone can fall victim to a scam. There's nothing to be embarrassed about and you shouldn't hesitate to let someone know if you think you've been scammed. But who should you tell?

- **You should let the police know first.**
- **You should then let Action Fraud know online at www.actionfraud.police.uk or by calling 0300 123 2040. Provide as many details as possible.**
- **You might want to talk to a loved one about what's happened as it can be upsetting.**
- **If you think the scam has had an effect on your computer, such as a virus, you should talk to a computer technician to get it fixed.**

Action Fraud

Tel: 0300 123 2040

www.actionfraud.police.uk

How to stay as safe as possible

There are several things you can do to stay as safe as possible online.

- **Pause and think.** It might seem simple, but it's one of the best things to do to stay safe. We can all be guilty of doing or clicking things online without thinking. But if you're at all suspicious of an email or website, then don't act. Take your time, trust your instincts and get in touch with the organisation directly through their official website or contact number. If it seems dodgy or too good to be true, it probably is.
- **Use strong passwords.** A strong password is a very effective way to stay safe online. Avoid common words, anything easily guessable (such as 'password' or '123456') and don't include personal information. Websites often have certain criteria for a strong password. It's important to use different passwords for different accounts and never share them – genuine companies will never ask for your full password.
- **Protect your wireless network.** Make sure you have a 'key' – a type of password – on your wireless network (Wi-FI) so no one else can access it. There should be instructions on how to do this that come with your wireless router.
- **Install software on your computer.** Anti-virus software will detect and remove viruses before they can infect your computer. Anti-spyware software will prevent unwanted adverts and pop-ups and can stop anyone tracking your online activity, such as credit card numbers and bank details. You can buy packages online or in a shop from reputable sources such as Norton or McAfee. There are also free, safe versions available online from companies such as AVG, Avast and Microsoft.
- **Keep your devices safe.** You may use your mobile phone or tablet to access the internet. You can install similar software to protect yourself from viruses (companies such as Avast, Kaspersky and Norton offer mobile options) as well as password-protecting your device. It's also important to keep the operating system of your device – such as Windows or Mac OS – updated as these help keep your device as safe as possible.

Top tip

You might be worried about installing anything on your device or computer. If you're unsure, check the source, reviews and check with someone you trust.

Remembering your passwords:

It can be tricky to remember passwords so we've left space for you to jot down hints to help you remember yours. Please do not write your password here and make sure hints are nothing that could help someone else guess your password.

Device/account	Password hint
.....	.....
.....	.....
.....	.....
.....	.....

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.