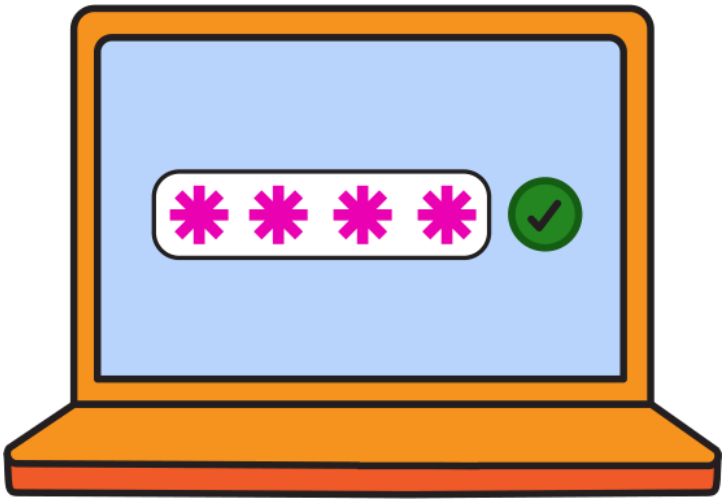
Cyber **Aware**

Advice on how to stay secure online.



Actions to improve your cyber security

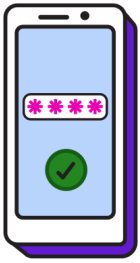
Most of us are spending more time online. So it's important to secure the **personal information** we store on the internet, and the **devices** we use to access this information.

Improve your password security

Passwords are the gateway to your online accounts. Here are three actions to ensure your passwords are working hard to protect your personal and financial information.

1 Create a unique password for your email account

If a cyber criminal accesses your email, they can use it to reset all your other account passwords (and get access to all your other accounts). This is why it's important to create a strong password for your email account, and make sure it's different to all your other online passwords.



2 Create strong passwords using three random words

Cyber criminals can easily guess weak, short passwords. You can quickly make a strong password by combining three random words to create a single password (for example PuddingTorchPizza). If you're asked to include special characters when creating a password, you can include them in your three random words (for example Pudd1ngT0rchPizza!).

3 Save passwords in your browser

Most web browsers (such as Chrome, Safari and Edge) will offer to save your passwords for you. It's safe for you to do this.

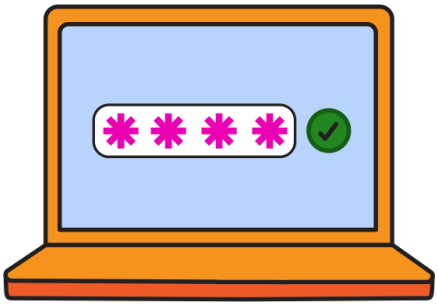
Letting your browser do this means you can use unique, strong passwords for **all** your important accounts (rather than using the same password for all of them, which you should never do).

Add extra protection

Now you've got your passwords sorted, you're ready to take cyber security to the next level.

4 Turn on 2-step verification (2SV)

Turning on 2SV will stop criminals getting into your account, even if they know your password. 2SV (also known as **2-factor authentication**, or **multi-factor authentication**) simply means you'll be prompted for a second piece of information when signing into your account. This is usually a code which will be sent via text or email.



5 Update your devices

You should update your apps and your device's software when you're prompted. Updates include protection from viruses and will often include new features. Applying these updates is one of the most important (and quickest) things you can do to keep yourself safe online. You can make things even safer by turning on **automatic updates**.

Back up your photos, documents, and other personal data

Congratulations! If you've followed these actions, you're protected from the vast majority of cyber attacks. But if something does go wrong, backing up means you will always have access to your important data.

6 Make sure your important data is backed up

A backup is a copy of your important data such as photos, documents, and other personal data stored on your IT equipment. Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup.

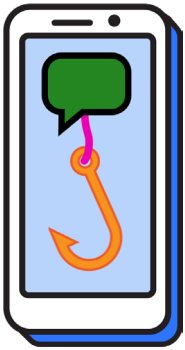
If you use products from Apple, Google or Microsoft (such as Windows computers, Apple and Android phones and tablets), you'll be able to back up your data to the internet. Check your devices to see **what** is being backed up, **how** often, how much **data** you're allowed, and that **automatic backups** is switched on.

Report suspicious messages

By reporting suspicious messages, you'll be helping to prevent others becoming victims of cyber crime.

7 Report suspicious messages

If you've received a suspicious email or text message that doesn't feel right, or visited a scam website, don't panic.



- Forward suspicious texts to 7726
- Forward suspicious emails to **report@phishing.gov.uk**
- Report scam websites to the NCSC by visiting: ncsc.gov.uk/report-scam-website
- If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at **actionfraud.police.uk** or by calling **0300 123 2040**
- If you live in Scotland, report all fraud (and any other financial crime) to Police by calling **101**

For more information on how to get secure online visit cyberaware.gov.uk. If you're a sole trader or a small business you can also find bespoke advice there.

Cyber Aware