Using passwords to protect your devices & data

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Passwords are an effective way to control access to your devices, data, and your online services. This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen.

For more information visit cyberaware.gov.uk

How do criminals get hold of passwords?

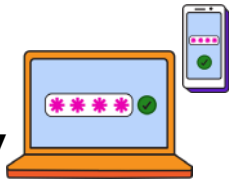
Passwords are often stolen when an organisation holding your details suffers a data breach. Criminals use the stolen passwords to try and access your other accounts.

They will also:

- try to access accounts using obvious passwords that many people still use (like **123456**)
- pretend to be somebody 'official' such as a bank, the NHS, or a government department, and trick you into revealing your password
- use sneaky techniques on social media (such as tricking you into sharing an SMS code)
- trick you into revealing passwords by creating fake phishing emails (or SMS messages) that link to scam websites

This is why you should avoid re-using the same password for different accounts, and **not** use predictable passwords that a criminal can easily guess.

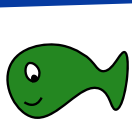
Set up two-step verification (2SV) for added security



2SV adds an extra step when you log in, usually by giving you a code to enter from an app or SMS.

- It means even if a criminal knows your pasword, they won't be able to access your accounts
- You should set it up on all your important accounts (email, social media, etc), even if you have a strong password
- Find out how to set it up on popular services at ncsc.gov.uk/2sv, or look in the security settings after you log in

Create strong passwords



The more unusual your password is, the harder it is for a criminal to guess.

- Combine three random words to create a single memorable password (for example CupFishBiro).
- Use a password manager app to create strong passwords for you (and remember them).
- Don't use predictable passwords (such as dates, family and pet names) or ones that criminals can easily guess (like '1234').
- If your smart device comes with a default password (like 0000), change it immediately.

Protect your email account

Use a strong and unique password for your email account. If a criminal accesses your email, they could:

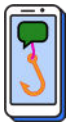
- use it to access to all your other accounts
- access information about you (including banking and social media details)
- send emails and messages pretending to be from you

Look after your passwords

Storing your passwords safely means you won't have to remember them, so you can use strong ones:

- It's OK to write down your passwords, but keep them somewhere safe, and out of sight.
- Most web browsers will offer to save your passwords for you. It's safe for you to do this (unless you're using a shared computer outside your home, for instance at college or a library).
- Password manager apps are a safe way to store passwords.

What to do if your password is stolen?



If you think your password has been stolen, or if it appears in any 'worst password' lists, change it as soon as possible.

- Indicators of a stolen password include being unable to log in, or messages sent from your account that you don't recognise.
- To check if your details have appeared in public data breaches, you can use online tools such as haveibeenpwned.com. Similar services are often included in antivirus or password manager tools that you may already be using.