POLICE SCOTLAND
POILEAS ALBA

Passwords and 2SV

Police Scotland Cybercrime Harm Prevention Team
04.03.2025

Passwords

Create strong passwords using **3 random words**.

Do not use words that can be guessed (like your pet's name or personal information). You can include numbers and symbols to make it stronger. For example, 'Bec@uselegiblefo1der'.

Three random words - NCSC.GOV.UK

You should have separate passwords for all our online accounts including online banking, shopping, social media and email accounts. Having a separate password for all our online accounts is an effective way to protect these from unauthorised access. Creating strong, separate passwords and storing them safely is a good way to protect yourself online.

How to change your password in:

Gmail (opens in a new tab)
Yahoo! Mail (opens in a new tab)
Outlook (opens in a new tab)
BT (opens in a new tab)
AOL Mail (opens in a new tab)

If your email provider is not listed above, please search online for advice from your provider on how to change your email password.

Password managers: using apps to safely store your passwords.

When you use different passwords for your important accounts, remembering them all can be a challenge. Password managers can store all your passwords securely, so you don't have to worry about remembering them. This allows you to use unique, strong passwords for all your important accounts (rather than using the same password for all of them, which you should never do).

Password managers:

- Synchronise your passwords across your different devices, making it easier to log on, wherever you are, and whatever you're using.
- Let you know if you're re-using the same password across different accounts.
- Notify you if your password appears within a known data breach so you know if you need to change it.
- Work across platforms, so you could (for example) use a single password manager that would work for your iPhone and your Windows desktop.

How to protect your saved passwords.

Make sure you protect your saved passwords in case your device is lost or stolen. Someone who gets access to your device may be able to use your saved passwords to access your accounts. This kind of cybercrime is much less common than remote attacks over the internet, where passwords can be cracked using software.

To make sure you are protected:

- Don't share your password(s) with anyone.
- Turn off or lock your device(s) when you are not using them.
- Use strong passwords to protect your device(s).
- Turn on Two-Step Verification (2SV) for all your devices and accounts.
- Turn on biometrics (Face ID or Fingerprint recognition) if your device(s) supports this.

Two-Step Verification (2SV)

Two-Step Verification is also known as Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). 2SV helps to stop hackers from getting into your accounts, even if they have your password.

Some online banking uses 2SV automatically. It does this by asking for more information to prove your identity, such as:

- A PIN, password or One Time Passcode (OTP)
- Biometrics - a fingerprint or face ID

How to activate Two-Step Verification (2SV).

You will need to manually activate 2SV for most of your accounts. Not all accounts will offer 2SV.

Turn on 2FA for **email**.

Gmail (opens in a new tab)
Yahoo (opens in a new tab)
Outlook (opens in a new tab)
AOL (opens in a new tab)

Turn on 2SV for **social media**.

Instagram (opens in a new tab)
Facebook (opens in a new tab)
X (opens in a new tab)
LinkedIn (opens in a new tab)