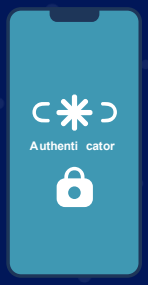
Government Security



Authentication

‘Authentication’ is the process of checking that you really are the person you are claiming to be.

Passwords are a common form of authentication but even if you've always looked after your passwords (and taken the time to create a strong one and avoided the worst passwords that millions of people still use), they can still be stolen through no fault of your own.

Turning on 2-Step Verification (2SV) is one of the most effective ways to protect your online accounts from cyber criminals.

2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password.

You should protect your most important accounts (such as email, banking, social media and online shopping) by making sure you have 2-step verification turned on for each of them.

Follow this link to **Find out how to turn on 2-Step Verification**

Or for more advice on how to stay secure online visit the National Cyber Security Centres **Cyber Aware** pages

Always report any unusual activity within your work accounts or device by following your department’s security protocols.