JEFFMAYNARD.COM

CDSV
CYBER AND DIGITAL SPECIALS AND VOLUNTEERS

# PASSWORDS & PASSKEYS

**Passkeys** are a new (2022) initiative to replace passwords for access to web sites and apps. Passkeys are much more secure than passwords since nothing secret is stored on any remote server and nothing secret is transmitted from your device.

Passkeys are also much easier to use; once set up, you access a web site or app in the same way you unlock your device (fingerprint, faceId or PIN).

Passkeys do not require the additional step provided by 2SV (2FA).
Web sites will show the availability of passkeys with this logo:

Passwords
Until Passkeys are more widely available, every password that you use in your on-line life is the main line of defence against unwanted access to your device and, with it, to your bank and other accounts.

This is why every password you use should be strong (see below) and different for every account. With lots of different passwords (remember: different for every account) we recommend the use of a password manager to store securely each one (and associated login id). Search ‘password manager’ to find a range of free and paid-for solutions.

You can also store passwords in your browser (Safari or Chrome) and these can synchronise across all your devices (using iCloud or Google Sync); passwords used in apps (such a banking) are not saved in your browser.

**Strong Passwords** consist of three random words separated by one or two numbers and one or two punctuation marks. You can use upper and lower case for additional security. To better understand the importance of strong passwords, please read the ‘Password Cracking’ paper

Security to any account using traditional passwords is greatly increased using 2-Step Verification, 2SV (also called two-factor authentication, 2FA); we recommend using 2SV for all accounts where it it available.

More on why Passkeys are safer and easier to use **here**.
For more Police advice on on Passwords tap **here**; on 2SV tap **here**.