Two Factor Authentication and Passkeys

Mendlesham Computer Club

By Giles Godart-Brown

How to make your online accounts safer without making life complicated

The Big Picture

- Passwords are still common.
- 2-step verification (2SV), also called 2-factor authentication (2FA) or MFA, adds another check.
- Passkeys are the newer option: the UK National Cyber Security Centre (NCSC) now recommends passkeys wherever they are available see https://www.ncsc.gov.uk/section/advice-guidance/you-your-family.
- Where passkeys are not available, the NCSC recommends a strong, unique password plus 2FA.

2SV, 2FA and MFA — are they different?

- For everyday use, these terms are often used interchangeably.
  - 2SV = two-step verification.
  - 2FA = two-factor authentication.
  - MFA = multi-factor authentication.

- The important thing is that there is an additional security check beyond your password.

Why passwords are not enough

- A password can be stolen in a data breach.
- A criminal may trick you into entering it on a fake website - this is phishing.
- Using the same password on several sites increases the risk if one site is breached.
- Even a strong password can be stolen.
  2FA gives you another layer of protection

What does 'two factor' actually mean?

- The idea is to prove that you are indeed you using two different kinds of evidence.
  - Something you KNOW - such as a password or PIN.
  - Something you ARE - such as your fingerprint or face.
- using something you HAVE - such as your phone, authenticator app or security key.
- Two steps do not necessarily mean two separate devices.

A normal 2FA login

- Step 1: enter your username and password.
- Step 2: prove it is you by entering a code, authenticator app, approval notification, security key or another method.
- The service then lets you in.

- You normally will not need the second step every single time on a trusted device.

SMS text-message codes

- The website sends a one-time code to your mobile phone.
- It is much safer than using a password alone.
- However, SMS is not the strongest form of 2FA.
- If SMS is the only option offered, it is still worth turning it on.
- Never tell a caller or texter the code you receive.

Authenticator apps

- Examples include Microsoft Authenticator and Google Authenticator.
- The app produces temporary codes or may ask you to approve a sign-in.
- It does not normally require a mobile signal to generate a code.
- Authenticator apps are generally preferable to SMS when available.

Approval notifications

- You may receive a notification email asking: 'Is this you?'
- Only approve a login that YOU have just started.
- If repeated unexpected requests arrive, choose 'Deny' or 'No'.
- Several unexpected approval requests can be a sign that someone knows your password.
- Do not approve a request just to make it go away.

What is a passkey?

- Think of it as a special digital key that your device keeps for a particular website that replaces the password and is stored securely on your device.
- Your device recognises the website and uses the correct key automatically.
- You prove that you are allowed to use the key by Face ID, Touch ID, a fingerprint, or your device PIN. The website does not receive your fingerprint or face data.
- There is no password for a criminal to trick you into typing into a fake website.
- The NCSC now recommends passkeys over passwords wherever they are available.

Where are passkeys stored?

- On Apple devices they may be managed through Apple Passwords / iCloud Keychain.
- On Android devices they may be managed through Google Password Manager
  or another credential manager.
- Windows PCs can also use passkeys through supported credential managers and security features.
- The exact screens vary between devices and services.

The five rules to remember

1. Use Passkeys as a preference
2. Turn on 2FA if a service does not offer passkeys.
3. Use a different password for important accounts
   if not supported by 2FA or passkeys.
4. Never share a password, PIN, or 2FA code.
5. If a message makes you feel uncomfortable, stop and check.