Key Actions:

- **Use strong passwords**
  - Consider using THREE RANDOM WORDS. This provides a good opportunity to create a strong but memorable password, e.g. **TelephoneStreetApple** (please do not use this example)
  - Add complexity with special characters and numbers, e.g. **Telephone9Street*Apple** (please do not use this example)
  - Ideally 13+ characters in length
  - Unique password for each account
  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
- **Consider the use of a password manager / book**
  - Most of us have lots of online accounts, so creating different passwords for all of them (and remembering them) is hard.
  - A password manager (or a web browser) can store all your passwords securely, so you don't have to worry about remembering them.
  - You can use a notebook to write passwords down. Make sure it is **not** clearly labelled; keep it somewhere secure.
  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
- **Always use Two Step Verification (2SV, 2FA, MFA)**
  - Turning on 2SV is one of the most effective ways to protect your online accounts from cyber criminals.
  - Can be set up to send codes over SMS, email, WhatsApp. More secure to use an "Authenticator App" or biometrics (fingerprint or face scan)
  - **Never share the codes with anyone!**
  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email
- **Use Passkeys where available**
  - You prove who you are with something you have (your device) and something you are or know (a fingerprint, face scan or simple PIN).
- **Back-ups of data and Updating devices & software**
  - Consider a backup as a copy of your important data that's stored in a separate safe location, usually on the internet (cloud storage), or on removable media (such as USB stick, SD card, or external hard drive).
  - You should apply updates to your apps and your device's software as soon as they are available. Updates include protection from viruses and other kinds of malware, as well as improvements and new features.

Useful resources:

- **Police CyberCheck tool**
  for step-by-step actions and links:
  https://cybercheck.southeastcyber.police.uk/

- **HaveIBeenPwned** website to check for data breaches:
  https://haveibeenpwned.com

- **Stop! Think Fraud** for advice on spotting fraud and scams, where to report and how to recover after a fraud:
  https://stopthinkfraud.campaign.gov.uk/

- **Take Five**
  https://www.takefive-stopfraud.org.uk/

- **Age UK** for advice on using the internet safely
  https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/

- **Reporting:**
  - Action Fraud for reporting of fraud and cybercrime
  - Phishing Emails – forward to report@phishing.gov.uk
  - Spam SMS – Forward to 7726
  - Contact the Fraud Team of your bank – Dial 159

- **Links to useful videos:**
  - CiFAS Coffee Shop - data privacy:
    https://www.youtube.com/watch?v=sq-0tjv4_BA
  - Starling Bank AI voice cloning:
    https://youtu.be/E_jP1R6aiUU?feature=shared

- **Contact us** if you know of other groups or organisations who would benefit from our training:
  cyber.protect@thamesvalley.police.uk