Bookham Seniors Computer Club

Security on PCs, Laptops and Phones

Protecting your digital life

13 February 2026

Why Device Security Matters

- Laptops and smartphones store personal and sensitive data
- Good security reduces the risk of data loss and misuse
- Cybercrime comes in many forms including:
  - Malware or malicious and unwanted code
  - Viruses
  - Worms
  - Trojans
  - Phishing and Identity Theft
  - Credit Card Theft/Fraud
  - Spoofing
  - Denial of Service
  - Sniffing (e.g. eavesdropping)
  - Ransomware
  - System Failures (e.g. Software design flaws).

Passwords

- Passwords
  - Websites determine minimum and maximum length and required combination of uppercase, lowercase, numbers or symbols
  - Dos and Don’ts:
    - Don’t use personal information
    - Don’t use words found in the dictionary
    - Length is stronger than complexity
      - Recommended length is at least 12 characters, with 14 – 16+ being better.
    - Don’t use the same password for every account
    - Use a combination of uppercase, lowercase, numbers or symbols depending on what is allowed
    - Use a phrase that you can remember and take the first letter from each word.
  - Suggestions
    - Add or replace a letter with a number, e.g. replace e with 3 (Baker > Bak3r)
    - Add or replace a letter with a symbol, e.g. Replace i with ! (e.g. Brian > Br!an).

Passwords

- Changing Passwords
  - If you think someone knows your password, go into your account and change it
  - If you change your password, you should get an email telling you that has happened
  - If you get an email that says you have hanged your password and you haven't, someone else my have changed it
- Passwords are stored remotely:
  - Passwords are therefore transmitted across networks and the internet
    - https: makes passwords significantly safer by encrypting data in transit between your browser and the website server, preventing hackers on the same network from eavesdropping.
    - If a site is not using https:
      - preferably do not use it
      - If you do use it, do not use public Wi-Fi (unless you use a VPN)
- Security of passwords also depend on the website:
  - Poorly implemented websites might store your website in plain text or poorly encrypted
  - Passwords will not be protected if the website's database is breached
  - If using a public computer always ensure you do not save your password and log out.

Passwords

- There are lots of free password strength checkers (and they produce different results):
  - security.org https://www.security.org/how-secure-is-my-password/
  - bitwarden https://bitwarden.com/password-strength/

- There are websites that will check if your password or email address has been exposed in a data breach:
  - Have I been Pwned https://haveibeenpwned.com/

Passwords

- Where should I store may passwords
  - Password Notebook
    - Dedicated notebook kept in safe or hidden in a secure location away from your computer
    - Keep usernames and accounts in a separate location from passwords
    - Use a memory cipher (e.g. Add complex or long phrase and add a unique element for each website)
  - Secure Local File
    - Password protected file such a Word document or Excel spreadsheet
    - Ideally encrypted or using a logical formula
  - Browser Storage (Built-in)
    - Google Chrome Password Manager (Menu > Passwords and Autofill > Password Manager)
    - Microsoft Edge Password Manager (Settings > Profiles > Passwords)
  - Third-Party Password Manager
    - 1Password, Bitwarden, Proton Pass, LastPass and many more
    - Free password managers are usually feature-limited versions of their premium password managers.

Passwords

- In 2025, the most common passwords continue to be dominated by weak, easily guessed, and numerical sequences, with "123456" remaining the top global choice, while "admin" and "password" dominate in the UK and US
- These predictable, and often reused, credentials are responsible for 80% of data breaches
- Top 20 Common Passwords 2025 (UK/Global Trends):

1. 123456
2. admin
3. password
4. 12345678
5. 123456789
6. Password1
7. Password (capitalized)
8. 12345
9. Lennon11
10. 1234567890
11. Password123
12. Fortnite21
13. password1
14. qwerty123
15. qwerty
16. 123qwe
17. abc123
18. Strongman12
19. daday123
20. Liverpool1

PIN (Personal Identification Number)

- What is a PIN (Personal Identification Number)
  - A secure way to protect your computing device (PC, laptop, tablet or phone)
  - A unique, personal code that you enter into your device, so that only you can gain access
  - At least four characters, usually numbers, which are easy for you to remember but difficult for anyone else to guess
  - Susceptible to observation
  - Android devices also allow a Swiping Pattern (known as a “graphic” lock)
    - Continuous swipe on a 3x3 matrix
    - Less secure as possibilities are limited and more susceptible to observation than a “numeric” lock
    - Not available on Apple devices
- Unlike a password it is stored on your computing device
  - Generally speaking, limits are placed on how frequently you allowed input of incorrect pins before being temporarily locked out from making further attempts
  - This rule works as a means of deterring anyone from trying various possibilities until finding the right combination that fits thus stopping individuals from abusing authentication procedures.

Biometric Authentication

- What is Biometric Authentication
  - A superior security, high convenience, and non-transferable access by a using unique biological trait such as Fingerprint, Face or Voice
  - Not a PIN (i.e. not a secret sequence of characters but a unique biological characteristic)
  - Advantages include:
    - Difficult to forge or steal
    - Fast, user-friendly, and eliminates the need to remember, enter, or reset passwords
    - Ensures the authorised user is physically present, preventing password sharing or unauthorised or fraudulent access
    - Stored locally rather than on a server.
  - Disadvantages include:
    - If biometric data is stolen it cannot be changed
    - False Positives/Negatives
      - Systems may incorrectly identify users or deny access due to environmental factors (e.g., wet hands, poor lighting)
      - Requires a fallback mechanism such as a PIN
      - Susceptible to “spoofing attacks," where attackers use high-quality photos, masks, or synthetic fingerprints.

Biometric Authentication

- How do I set up Biometric Authentication?
  - Depends on the device and application
  - Examples
    - In Windows, navigate to Settings > Accounts > Sign-in options and select Windows Hello Face or Windows Hello Fingerprint (there are other options)
    - On a Samsung Phone, go to Settings > Security and privacy > Biometrics > Fingerprints. Enter your PIN/password, tap "Continue" or "Add fingerprint," and place your finger on the sensor (screen, side button, or back) repeatedly until it reaches 100%
    - To set up Fingerprint on an iPhone, go to Settings > Touch ID & Passcode, enter your device passcode, tap Add a Fingerprint, then follow the prompts to lightly touch and adjust your finger on the Home button until it's fully registered, allowing you to use it for unlocking and app purchases
      - This feature requires a physical Home button, as newer iPhones use Face ID.
  - Other devices and Apps
    - How do I set up fingerprint [*or face*] recognition on my *[device].*
  - You should use Biometrics not just to open your phone but on all banking and other secure apps.

Passcodes and Passkeys

- What is the difference between a Passcode and a Passkey?
  - A passkey is a digital cryptographic credential (a pair of keys - one public, one private) that replaces passwords, while a passcode is a numeric or alphanumeric string to unlock devices or apps.
  - Passkeys offer higher security by preventing phishing and password theft, as they cannot be shared or stolen, unlike traditional passwords or passcodes.
- Passkeys
  - Passkeys are a newer standard designed to replace passwords
  - Whist a password or a PIN can get you into a device, a passkeys can sign you into an account using your face, fingerprint, or PIN
  - A fingerprint or face is not the passkey itself, but it is a primary method used to unlock and activate a passkey
  - How They Work Together
    - When you log in to a website or app using a passkey, your device needs to verify that it is actually you
    - Instead of typing a password, you use your fingerprint (or face scan/PIN) to unlock the device's secure storage, which then authorises the use of the cryptographic passkey to sign you in.

Passcodes and Passkeys

- How They Work Together
  - When you log in to a website or app using a passkey, your device needs to verify that it is actually you
  - Instead of typing a password, you use your fingerprint (or face scan/PIN) to unlock the device's secure storage, which then authorises the use of the cryptographic passkey to sign you in
- Summary:
  - Biometrics (Fingerprint, Face, Voice etc)
  - Cryptographic Key (Passkey): Biometrics are the "lock" for the credential, not the credential itself.
  - On-Device Security: Your fingerprint or face data stays on your device and is not shared with websites or apps when you use a passkey.
  - Convenience: Passkeys allow you to use your phone's screen lock (fingerprint/face) to log in to accounts across different devices.

Two Factor Authentication (2FA)

- Two-factor authentication (2FA) is a security method that requires two forms of identification to access an account. It's also known as two-step verification or multi-factor authentication.
- How it works
  - Users provide a username and password, which is the first factor
  - Users provide a second factor, which is something they have or something they are
  - The second factor can be a code sent to a phone or email or generated by an app
- Key Steps for Setting up 2FA
  - Locate Settings: Go to your account's security section (e.g., in Google account, go to "Security" -> "2-Step Verification").
  - Choose a Method:
    - Authenticator App: Scan a QR code with an app like Google Authenticator or Microsoft Authenticator.
    - SMS/Text Message: Receive a code via phone.
    - Email: Receive a code via email.
  - To verify, enter the code provided by the method to confirm the setup
  - Save any backup codes provided in case you lose access to your primary device.

One-Time Password (OTP)

- A One-Time Password (OTP) is a secure, temporary, and dynamic code - typically 4 to 8 digits
- Valid for only one login session or transaction
  - Even if stolen, the OTP becomes useless immediately after use
- Used primarily for two-factor authentication (2FA), OTPs enhance security by preventing unauthorised reuse, mitigating phishing risks, and protecting against replay attacks
- They are commonly delivered via SMS, email, or Authenticator apps
  - SMS-based OTPs can be intercepted making them less secure than app-based alternatives such as email and Authenticator apps
  - Codes generated via apps (e.g. Google Authenticator) that expire within 30–60 seconds, are generally more secure than SMS and email and are sometimes referred to as TOTP (Time-based OTP)
- You should hide ‘Notifications’ on your lock screen
  - Settings > Lock Screen > Notifications > Hide content.

Anti-virus

- Do I need an anti-virus product on my PC or laptop?
  - An anti-virus program is essential for protecting against phishing, malware, spyware and ransomware
  - Windows 10 & 11 built-in Microsoft Defender provides strong, free, real-time protection sufficient for many users who practice safe browsing habits including when installing apps hat are not from the Microsoft Store
  - Always on and updates automatically
  - More security-conscious users or businesses might opt for paid anti-virus programs for extra layers and advanced features (such as VPNs) against advanced threats like sophisticated phishing
    - Only one primary anti-virus program should be installed to avoid conflicts.
- Do I need anti-virus products on my smartphone and tablet?
  - Not normally, provided that you only install apps and software from official stores such as Google Play and the Apple App Store (*Source: The National Cyber Security Centre*)
  - You should also set your apps (and the tablet/smartphone itself) to update automatically.

Ad-Blockers

- Ad-blocker browser extensions, such as Adblock Plus, uBlock Origin and AdGuard, are tools designed to automatically remove disruptive ads, pop-ups, and trackers from websites, resulting in faster load times, improved privacy, and enhanced security
- These extensions are available for browsers like Chrome, Edge and Firefox to customise browsing experiences.
- Key Features and Benefits
  - Ad & Pop-up Blocking: Removes ads on social media, video platforms (YouTube), and banner ads
  - Privacy Protection: Stops third-party trackers from monitoring online activity
  - Malware Protection: Blocks malicious ads and phishing attempts
  - Increased Speed: Faster page load times as resource-heavy ads are not loaded
  - Customisation: Allows users to create whitelists for favourite sites to support them
  - Installation and Use: Ad-blockers are typically installed via the respective browser's store (e.g. Chrome Web Store). Once installed, they run automatically and their settings can usually be managed via a toolbar icon.

Ad-Blockers

- Top Free Ad-Blocker Browser Extensions
  - Adblock Plus
    - One of the most popular, open-source options that blocks banners, pop-ups, and video ads on sites like YouTube
  - uBlock Origin
    - Known for efficiency, low memory usage, and wide-spectrum filtering capabilities
  - AdGuard
    - Provides comprehensive protection against ads, trackers, and malicious sites
  - Ghostery
    - Focuses heavily on privacy by blocking trackers and speeding up webpage loading
  - AdLock
    - A strong contender that works well against diverse ad types.


SECURITY