National Cyber Security Centre
a part of GCHQ

Cyber security tips for barristers, solicitors and legal professionals

In June 2023, the NCSC updated the Cyber Threat Report for the Legal Sector to help law firms, lawyers and legal practices understand current cyber security threats, and the extent to which the legal sector is being targeted.

As the report explains, cyber criminals are not fussy about who they attack, which means law practices of all sizes are at risk, from sole practitioners, high street and mid-size firms to barristers' chambers, in-house legal departments and international corporate firms.

The following steps are aimed at sole practitioners and also small/medium-sized legal firms, to help them to reduce the likelihood of becoming victims of a cyber attack. Larger sized organisations should consult with their in-house IT/support teams.

Create and test backups of your important data

Creating backups regularly (and testing you can restore the data they contain) means you'll be able to access client data, even if you are a victim of a computer virus or ransomware attack.

- How to make cloud backups resistant to destructive ransomware (NCSC)
- Windows - Back up your Windows PC (Microsoft Support)
- macOS - Back up your Mac with Time Machine (Apple Support)
- iOS - How to back up your iPhone or iPad with iCloud (Apple Support)
- Android - Back up or restore data on your Android device (Android Help)

Keep software up to date and enable automatic updates

Software updates include protection from viruses and other kinds of malware, and will often include new features. You should also turn on 'automatic updates' in your device's settings so you don't have to remember to apply them.

- Windows - **Keep your PC to to date (Windows support)**
- macOS - **Update macOS on Mac (Apple Support)**
- iOS - **Update your iPhone or iPad (Apple Support)**
- Android - **How to update the Play Store & apps on Android (Google Play Help)**

Turn on encryption

Turn on the free encryption products included with your Windows or Apple devices, so cyber attackers can't access your sensitive data if your device is lost or stolen. Make sure encryption is enabled on your mobile device (this is done automatically on modern Android/Apple devices).

- Windows device or BitLocker encryption - Turn on device encryption (Microsoft Support)
- FileVault for macOS - Protect data on your Mac with FileVault (Apple Support)
- iOS - Advanced Data Protection for iCloud
- Android - Devices are encrypted by default provided you've set a lock screen

Protect email accounts using strong passwords and 2SV (2-step verification)

Use strong and unique passwords to protect your email and other important online services (such as banking and social media). A password manager can help you create (and remember) strong passwords. You should also turn on 2-step verification (2SV), which is sometimes called multi-factor authentication (or MFA).

- Create a strong password using three random words - **Three random words (NCSC)**
- Turn on 2-step verification - **Using 2SV for email, social media, and other accounts (NCSC)**
- Using password managers - **Using browsers and apps to safely store your passwords (NCSC)**

Control access to devices

Turn on screen lock for mobile devices, which should be combined with a passcode or biometrics (face or fingerprint) where supported. You should also lock your laptop/computer when you're not at your desk.

- **Windows Key+ L** locks computer. For macOS, use **Control-Command-Q**
- iOS - Use a passcode with your iPhone, iPad or iPod touch – Apple Support (UK)
- Android - Set screen lock on an Android device - Android Help (google.com)

Turn on your firewall

Your devices can be visible to others connected to the internet or public networks. Using a firewall prevents unwanted connections to your devices. Most popular operating systems, including macOS and Windows, now include a firewall.

- Windows - **Turn Microsoft Defender Firewall on or off (Microsoft Support)**
- macOS - **Block connections to your Mac with a firewall (Apple Support)**
- iOS - **Use the built-in privacy and security protections of iPhone (Apple Support)**
- Chromebook - **Chromebook Help (Google Support)**

Limit the number of 'administration' accounts

Administrators can change security settings, install software, delete users, and access all files on the computer. Limiting the number of 'admin accounts' you use reduces the opportunity for a cyber criminal to gain that level of access (for example by a phishing attack).

- Windows - Create a local user or administrator account in Windows (Microsoft Support)
- macOS - Add a user or group on Mac (Apple Support)
- iOS - Sign in with your Apple ID (Apple Support)
- Ensure you know how to defend your organisation against phishing attacks (NCSC)

Turn on antivirus software

Make sure you are running antivirus software on your desktop or laptop, which can protect against malware and also detect infected devices. The NCSC provides **tips to help you understand how to use antivirus tools.**

- Windows - **Stay protected with Windows Security (Microsoft Support)**
- macOS - **Protect your Mac from malware (Apple Support)**
- iOS - **Use the built-in privacy and security protections of iPhone (Apple Support)**
- For Android phones, refer to the support site of the manufacturer (such as Samsung or Google)

Make sure lost/stolen devices can be tracked, locked or wiped

You can track or (if required) remotely delete the data on your device, so that unauthorised individuals cannot access your confidential data if the device is lost or stolen.

- Windows - Find and lock a lost Windows device (Microsoft support)
- macOS and iOS - Set up Find My on your iPhone, iPad, iPod touch or Mac (Apple Support)
- Android - Be ready to find a lost Android device - Android Help (google.com)

Audit and review your privacy permissions

Some applications will ask for access to other apps, data or system features. Minimise the risk that this brings by ensuring staff only have access to apps that are needed to carry out their jobs.

- Windows - **App permissions (Microsoft Support)**
- iOS - **Control access to information in apps on iPhone – Apple Support (UK)**
- Android - **Change app permissions on your Android phone - Android Help (google.com)**

If you experience a cyber attack

If you've been the victim of a cyber attack, you should:

- report an ongoing incident directly to **Action Fraud** (on 0300 123 2040 which is available 24/7)
- for data breaches under the GDPR, report to the **Information Commissioner's Office**
- for any major cyber incidents, **report to the NCSC**

In England and Wales, the Solicitors Regulation Authority (SRA) Code for Firms and Individuals requires solicitors to **report promptly to the SRA** so that they can investigate whether a serious breach of regulatory arrangements has occurred, or exercise their regulatory powers.

In England and Wales, the Bar Standards Board (BSB) Handbook requires barristers and BSB regulated entities to **promptly report certain matters** to the BSB so that they can investigate whether serious misconduct has occurred.

1. If you are a barrister that works within a firm that is regulated by the SRA, they should be notified where a solicitor's client has been affected
2. You also should consider whether the incident has an impact on other firms / legal professionals and their clients and consider notifying them accordingly

All firms are strongly recommended to report incidents to the NCSC. The NCSC:

- provides support and incident response to mitigate harm
- works to ensure organisations have understood how they came to be a victim of a cyber attack
- ensures organisations have understood the cyber security implications (and taken steps to protect themselves from future attacks)