Lawcover

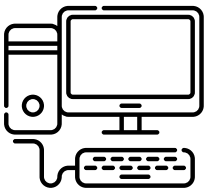
CYBER SECURITY SNAPSHOT

PROTECT YOUR HARDWARE

- Identify hardware you have, what it is used for, who uses it and where it is stored
- Enable real time protection on all devices
- Turn on automatic updates and schedule a convenient time for these to occur
- Schedule regular and full malware scans
- Encrypt hard drives to guard against unauthorised access if the device is lost or stolen
- Ensure your office or home Wi-Fi router is configured with appropriate security measures
- Never leave your device unattended
- Dispose of redundant hardware including external hard drives and USB securely
- Develop procedures and policies to ensure consistent and secure use of hardware

STEP BY STEP

IDENTIFY YOUR HARDWARE



The identification and management of hardware and devices is an important aspect of a robust cyber security strategy. By continuously monitoring and managing IT assets, a law practice can minimise their exposure to cyber security threats and reduce the risk of costly data breaches.

Create and maintain a list or spreadsheet (example below) of all your devices, who is responsible for them and where they are located. Make sure this list is kept securely and updated regularly.

Device Type	Brand	Model	Device ID/Serial Number	User	Location
Laptop	HP	EliteBook 830 13 inch Notebook PC	914CF345-1612-487E-B1F6-7B08FXC3C712	Meghan Roma	Head Office
Tablet					
Mobile					
Printer/Scanner					
Headphones					

STEP BY STEP

REAL TIME PROTECTION

Real-time protection prevents malware from entering your operating system* via email or internet. This feature compares your requested file in email or web browser against a known threat database and blocks them before they can infect your computer.

Microsoft Windows 10 onwards

1. Click the Windows logo to open the Start Menu
2. Click the gear button on the left to open up the Settings menu
3. Click Update & Security at the bottom of the list
4. Click Windows Security
5. Select Open Windows Security
6. Click Virus & threat protection
7. Click Manage Setting
8. Click the toggle to turn on real-time protection
9. Scroll down to cloud-delivered protection and click the toggle to turn it on

*The operating system is the engine of your computer. Usually this is either Microsoft Windows or Apple iOS/Mac.

Apple macOS

macOS is protected using a 3-layer defence process which is inbuilt and enabled by default by Apple. Users cannot turn off these features, therefore no further intervention is required.

IMPORTANT: If you are already using paid antivirus software, consult your IT service to prevent a conflict between the antivirus software and any real-time protection that is enabled.

STEP BY STEP

AUTOMATIC UPDATES

Cybercriminals use a variety of software vulnerabilities to launch an attack on your system. Turn on or confirm auto-updates, especially for operating systems, as it manages your device hardware and all the programs.

Microsoft Windows 10/Windows 11

By default, Windows 10/11 updates your operating system automatically.

Apple macOS Ventura 13 and later

1. Click the Apple icon in the top left corner
2. Select System Settings
3. Select General
4. Click the 'i' next to Automatic Updates
5. Ensure all settings are configured appropriately

Set a convenient time for auto-updates to occur. Weekends or overnight will avoid disruptions to work during practice hours.

Apple macOS Monterey 12 and earlier

1. Click the Apple icon in the top left corner
2. Select System Preferences
3. Open the App Store
4. Select Automatically check for updates and ensure all other check boxes are ticked

Please note that apart from these operating systems, you need to enable auto-updates for web browsers and other applications being used. Please refer to the relevant application website or user guide for more information.

IMPORTANT: If your hardware or software is older it may not auto-update, leaving your practice susceptible to technical, software and security issues. Review the age of your hardware and software and upgrade if required.

STEP BY STEP

PERFORMING SCANS

It is essential to keep up to date with evolving cyber threats. Performing weekly malware scans on your computer will help identify early risks and remediate them before they are exploited by a cybercriminal.

Microsoft Windows 10/Windows 11

1. Click the Windows logo to open the Start menu
2. Click the gear button on the left to open up the Settings menu
    a. On Windows 10, click Update & Security at the bottom of the list
    b. On Windows 11, click Privacy & Security on the left side
3. Select the Windows Security tab
4. Under the Protection areas section, click on Virus & threat protection
5. Under Current threat, click on Scan options
6. Select which scan you want to perform. It is recommended to complete a full scan

Apple macOS

Apple does not have any inbuilt malware scanning capabilities. However, you can install antivirus software to ensure your device is secure. Research your options and ensure the best fit for your needs.

STEP BY STEP

ENCRYPTING DEVICES

If a computer is stolen or lost, you can still protect against the damage to your data through full disk encryption. Encrypting the whole hard disk means the entire contents of your computer can only be accessed if the thief knows your passphrase or password. Ensure you protect the recovery key adequately; one option is to record it in a password manager.

HARD DRIVE ENCRYPTION - WINDOWS

Microsoft Windows 10/Windows 11

Device Encryption (If Trusted Platform Module (TPM) is available))

1. Sign in to Windows with an administrator account
2. Select the Start button (Windows Key)
3. Select Settings:
   a. On Windows 10, select Update & Security
   b. On Windows 11, select Privacy & Security
4. Select Device encryption
   a. If Device Encryption doesn't appear, it is not available. You may be able to use Standard BitLocker Encryption – see below

Standard BitLocker Encryption (If TPM is not available (Windows Pro and above only))

1. In the search box on the taskbar, type "Manage BitLocker", and select the Manage BitLocker app
2. Select Turn on BitLocker
3. Follow the on-screen instructions

IMPORTANT: Direct booting (an option referred to as TMP-only mode) may be vulnerable to being bypassed by an attacker with physical access to the device (a longstanding issue related to direct memory access).

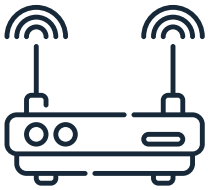
STEP BY STEP
ENCRYPTING DEVICES

Apple macOS

1. Choose the Apple menu in the top left
    a. On macOS version Monterey 12 and earlier, select System Preferences
    b. On macOS version Ventura 13 and later, select System Settings
2. Click Privacy & Security or Security & Privacy
3. Scroll down to FileVault
4. Click Turn On
5. Choose how to unlock your disk
    a. iCloud accounts: Click “Allow my iCloud account to unlock my disk” if you already use iCloud. Click “Set up my iCloud account to reset my password” if you don’t already use iCloud
    b. Recovery key: Click “Create a recovery key and do not use my iCloud account.” Write down the recovery key and keep it in a safe place
6. Click Continue

STEP BY STEP

SETUP WI-FI SECURELY



Wi-Fi router combines router and modem functions to create an internet-connected network for the devices in your home and office. In a network-based attack, these devices are usually the first target.

When establishing or reviewing your office or home Wi-Fi security:

1. Change your router's default username and password
2. Change your default Wi-Fi name and password
3. Use the strongest Wi-Fi encryption
4. Regularly update your router to use the latest firmware to avoid vulnerabilities
5. Disable remote management and Universal Plug and Play (UPnP)
6. Enable Guest Wi-Fi to restrict external user access to the main network. Ensure it is using a separate SSID from the corporate network to limit access to sensitive data
7. Consider retiring equipment that is no longer actively supported by the vendor or manufacturer. Including Internet-of-Things (IoT) devices which are increasingly targeted by a range of threat actors. This may include video conferencing equipment, Internet enabled security cameras, televisions, smart light bulbs, etc
8. Ensure that devices are procured from trusted and reputable sources to reduce the risk that they have been tampered with

WiFi routers are used as an entry point to infiltrate your home or office network. With access, cybercriminals can steal data, spy on your activities, and gain sensitive information such as banking details and passwords.

STEP BY STEP

PHYSICAL SECURITY

Never leave your device unattended!

Restrict access to server rooms and networking equipment and avoid leaving laptops in places where they might be ‘on-display’ (e.g. in cars, or in hotel rooms). Physical security underpins all security. If someone has physical access to your systems, they can easily be compromised.

STEP BY STEP

DISPOSING OF DEVICES

Disposal of old computers or hardware should be done securely. Data such as personal information, passwords, browsing history, emails on your system can be accessed accidentally or maliciously by an outsider.

When disposing of old hardware:

- Backup all the necessary files to another secure device
- Erase all the contents of your device by completing a factory reset. A factory reset should wipe off local files, usernames, passwords, and other settings to default, but only on devices that have been encrypted. If not, then data on the device may be recoverable. If in doubt, storage devices should be removed and physically destroyed
- Removable media such as USB devices may require specialist disk wiping. If in doubt, physical destruction is recommended.

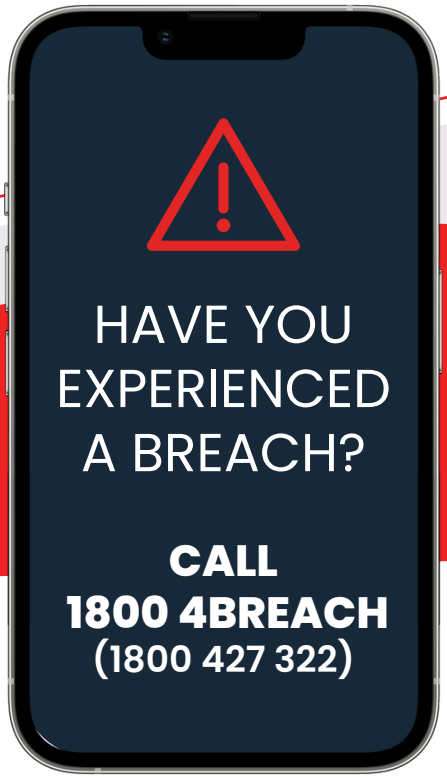
Microsoft Windows 10/Windows 11

1. Select the Start button (Windows Key)
2. Select Settings
   a. On Windows 10, select Update & Security b. On Windows 11, select System
3. Select Recovery
   a. On Windows 10, select Reset this PC > Get Started b. On Windows 11, select Reset PC
4. Follow the on-screen instructions to complete the system reset

Apple macOS

1. Sign out of all services, such as iCloud and iMessage
2. Click on the Apple menu at the top-left corner
   a. On macOS version Monterey 12 and earlier, Select System Preferences
   b. On macOS version Ventura 13 and later,
   Select System Settings > General > Transfer or Reset
3. Click Erase All Content and Settings
4. Follow the on-screen instructions

Find a recycler near you to dispose of the device according to environmental guidelines.



Lawcover®

Lawcover Insurance Pty Ltd | ABN 15 095 082 509
Phone (02) 9286 8877 | practicesupportservices@lawcover.com.au | lawcover.com.au