PATFox

blueprint for FREE SPEECH

# CYBERSECURITY BEST PRACTICES FOR LAWYERS

Co-funded by
the European Union

**Author:**

Naomi Colvin

@ Blueprint for Free Speech

For further information related to this publication, please contact the author:

naomicolvin@blueprintforfreespeech.net

**DISCLAIMER**

This report was developed for the Pioneering anti-SLAPP Training for Freedom of Expression (PATFox). The PATFox project has received funding from the European Union under grant agreement n° 101051559.

Detailed information about the project can be found on: https://www.antislapp.eu/

# Table Of Contents

# 1. Introduction

Legal firms find themselves under increasing risk of cyberattack. Lawyers have a special obligation of confidentiality to clients. That duty to protect confidential information makes them an entity of interest for both targeted and opportunistic attacks from criminals operating online.

In June 2023, two European digital security agencies, the UK's NCSC and France's ANSSI separately warned that they were seeing a growth in targeted attacks against legal firms in order to acquire information relevant to ongoing cases.[1] The attackers in some of those cases were working for third-party clients. Further afield, attackers launched brazen attacks specifically aimed at law firms. In 2023, cyber attackers breached data protections at Australia's largest law partnership, HWL Ebsworth and stole 2.5 million files. The attack affected 65 government agencies, as well as banks and insurers.[2]

If anything, the problems are heightened for lawyers representing clients targeted with SLAPPs. SLAPP cases are, by definition, highly adversarial with those initiating such cases seeking to make the experience of the defendant as difficult as possible.

[1] https://www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-004.pdf

[2] https://www.theguardian.com/australia-news/2023/jun/26/hwl-ebsworth-hack-sensitive-information-from-dozens-of-government-agencies-may-be-compromised.

Powerful adversaries may have the capacity to initiate targeted attacks – but even where a client's adversaries do not have or use such capabilities, in the context of a stressful SLAPP case, they can be perceived as having that ability. Online harassment is often correlated with SLAPP cases and the perception of digital vulnerability can add to the psychological toll exacted on those defendants. Providing cybersecurity advice for clients is not only useful in itself, it can be a valuable confidence building measure.

The advice provided below is divided into two sections: the *advice for individuals* is applicable to everyone. The *advice for organisations* includes some additional steps that should be taken in order to secure information and resources organisations typically share internally. We anticipate the advice for organisations primarily being of use to legal firms – but, if their clients include NGOs or media organisations which communicate with duties of care towards those whom they communicate with, they may also benefit from the organisational advice.

### 1.1 Whistleblowing and Ricochet

Whistleblowing is an area that deserves special consideration. Blueprint for Free Speech publishes specialist guidance for journalists working with whistleblowers.[3] A separate PATFox resource will be released for anti-SLAPP lawyers on whistleblowing law.

[3] https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea072671e7db3106f3479c9/1587573352563/Blueprint_Perugia_Principles.pdf

In terms of practical tools, Blueprint has developed Ricochet, a desktop-based peer-to-peer messaging app that allows users to communicate securely and anonymously. You can find out more about Ricochet and download it here: https://www.ricochetrefresh.net/

The free, open-source software allows two people to transfer files completely anonymously, as well as chatting online anonymously via a peer-to-peer network. All transfers and chats are also private, protected by end-to-end encryption.

### 1.2 Sourcing

Best practice in cybersecurity changes as tactics and tools change. The following advice is drawn from a number of recently updated sources which we consider reliable, including advice from Australia's Cyber Security Center, the UK's National Cyber Security

Centre, EFF's Security Self-Defence resources, the NetAlert project and Consumer Reports (US).[4] Ricochet aside, we deliberately do not give specific advice on products in this guide, but some guidance is available in the resources section under each heading.

[4] Links including https://netalert.me/resources/en/secure-accounts/2-step-in-2-minutes/

# 2. Key Steps for Individuals

## 2.1 Keep your devices updated

**Why this important:** the majority of cyberattacks are opportunistic, taking advantage of known vulnerabilities. Developers fix these on an ongoing basis, but to take advantage of this you must ensure that devices can receive updates and that these are applied. In 2017, Equifax was hacked using a known vulnerability in their customer complaint system that had not been patched (fixed), leading to the

exposure of personal data of hundreds of millions of people[5].

**What to do**: Regularly update personal and business phones, tablets, and computers, changing settings to receive automatic updates where that is appropriate. For businesses, it is particularly important to ensure that internet-facing servers and network devices are updated promptly, and this may have to be done manually. Check that devices can still receive updates – older phones and computers may not, and you should replace these.

**Context**: transitioning from a legacy IT system to a more modern option can be challenging. However, the global media is full of data breach stories from organisations that just didn't update their systems. The organisations found their reputations in the toilet and their clients and partners fleeing out the door. Sometimes organisations don't have up to date systems through poor management. More often the IT staff didn't get the budget they needed to sufficiently update all the IT – the board or the division head took a gamble and they lost. The outcome was bad.

**Resources:**

- Update your devices – includes instructions for iPhone, Android, MacOS and Windows users[6]
- Which Phone support calculator – check your phone is still able to receive updates[7]

[5] https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

[6] https://www.cyber.gov.au/learn-basics/explore-basics/update-your-devices

[7] https://www.which.co.uk/reviews/mobile-phones/article/mobile-phone-security-is-it-safe-to-use-an-old-phone-a6uXf1w6PvEN#which-phone-support-calculator

## 2.2 Use multifactor authentication (MFA)

**Why this is important:** passwords can be weak or compromised. MFA (sometimes called two-factor authentication or 2FA) makes it more difficult for attackers to access your online accounts, by requiring logins to be authenticated by a second method or device. The (US) Consumer Cyber Readiness survey from 2023 show that almost three-quarters of respondents used some form of MFA on at least one of their online accounts. However, SMS is still the most-used method of MFA, with just 50% of respondents reporting using some kind of app-based form of authentication.[8]

**What to do:** Turn on MFA wherever it is offered, paying particular attention to your most important online accounts. These typically include email accounts, online banking, and social media accounts, which are key to a journalist's or a law firm's reputation. Different methods of MFA are available. MFA methods that send push messages to your phone or use an authenticator app are generally preferable to MFA via SMS text message.

**Resources:**

- Turn on multifactor authentication[9]
- 2-step verification in 2 minutes (Net Alert)[10]

- Set up 2-step verification now (Net Alert)[11]

[8] https://www.aspeninstitute.org/wp-content/uploads/2023/10/Consumer-Cyber-Readiness-Report_October-2023.pdf
[9] https://www.cyber.gov.au/learn-basics/explore-basics/mfa
[10] https://netalert.me/resources/en/secure-accounts/2-step-in-2-minutes/
[11] https://netalert.me/resources/en/secure-accounts/2fa-docs/

## 2.3 Back up your devices

**Why this is important:** cyberattacks that deprive you of access to your personal digital files or business data can be particularly damaging. Having access to backups of the most important artefacts in your digital life or business-critical data reduces the impact of such attacks to inconvenience and provides confidence that you can recover from attacks should other kinds of protection fail. In 2020, Hackney borough council in London suffered a crippling ransomware attack. The lack of viable backups mean that council services experienced severe disruption for several years[12].

**What to do:** back up phone, tablet, and computer data, either to an external device or to the cloud Many modern operating systems offer a default backup route, though you may have to pay a subscription to make full use of these. For additional assurance, keep an external backup in a separate location to your main system and protect those backup files with encryption. That way if there is a physical catastrophe, such as flooding or fire, your data will be safe.

**Resources:**

- Set up and perform regular backups – includes instructions for iPhone, MacOS and Windows users[13]
- Backing up your data[14]

[12] https://www.wired.co.uk/article/ransomware-attack-recovery-hackney
[13] https://www.cyber.gov.au/learn-basics/explore-basics/set-and-perform-regular-backups
[14] https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

## 2.4 Use a password manager

**Why this is important:** where MFA is not available, a strong password is all that stands between your online accounts and an attacker. Strong passwords are at least 14 characters long, unpredictable, and only used for one account. Current advice for strong passwords suggests using three or four random words – a passphrase rather than a password. Most people have problems remembering strong passwords for each of their online accounts. As such, it is a good idea to use a password manager, which allows you to create, store and access login credentials for all your online accounts. Despite this usefulness, password managers are one of the less-observed recommendations we make here. The 2023 Consumer Readiness survey showed only 37% of respondents using one.

**What to do:** install a password manager and ensure that you use a unique, strong password for each of your online accounts, starting with those that are most important (email, banking, social media).

**Resources:**

- Consumer Reports (US) assessed a range of password managers in 2023[15]
- Choosing a Password Manager (Surveillance Self-Defense)[16]
- Passphrases are the more secure version of passwords (Australian Cyber Security Center) [17]
- Consumer Cyber readiness report[18]

[15] https://www.consumerreports.org/electronics-computers/password-managers/best-password-managers-review-digital-security-privacy-ease-of-use-a7337649384/
[16] https://ssd.eff.org/module/choosing-the-password-manager-that-s-right-for-you
[17] https://www.cyber.gov.au/learn-basics/explore-basics/passphrases
[18] https://www.aspeninstitute.org/wp-content/uploads/2023/10/Consumer-Cyber-Readiness-Report_October-2023.pdf

### 2.5 Use encryption and encourage your contacts to do the same

**Why this is important:** end-to-end encryption protects your messages while they are moving between devices; not even the operator of the service you are using can read

the content of your messages. This is an important assurance for sources and other confidential contacts. Website encryption protects information about the websites you are visiting.

Device encryption helps ensure that your data stays private even if you lose access to your device. Most modern phone operating systems will encrypt your data by default. Desktops and laptops typically have Filevault and Bitlocker to provide native encryption capabilities for MacOs and Windows respectively. Consumer Cyber Readiness survey indicates that the understanding of device encryption is low, with 86% respondents saying they definitely do not have software installed for encrypting the device they use most[19].

**What to do:** Use encrypted IM messages and/or emails and install HTTPs Everywhere on your internet browser.  Encourage your contacts to do the same.

**Resources:**

- How strong encryption can help avoid online surveillance[20]
- How to use Signal[21]

[19] https://www.aspeninstitute.org/wp-content/uploads/2023/10/Consumer-Cyber-Readiness-Report_October-2023.pdf
[20] https://ssd.eff.org/module/animated-overview-how-strong-encryption-can-help-avoid-online-surveillance
[21] https://ssd.eff.org/module/how-to-use-signal

## 2.6 Watch out for phishing attempts and other scams

**Why this is important:** Many cyberattacks rely on attackers tricking a user doing something (visiting a website, opening an attachment, transferring finds) that is either directly beneficial to them or reveals sensitive information that can be exploited. Such messages may seem apparently trustworthy – they may seem to come from trusted institutions or individuals, for example, at first glance.

The advent of generative AI systems that can produce natural-sounding text may

make these approaches even more convincing in the future. Phishing attempts are incredibly common. Interpol considers it "t*he most prevalent cyber threat in the world, and it is estimated that up to 90% of data breaches are linked to successful phishing attacks, making it a major source of stolen credentials and information*".[22]

**What to do:** Think carefully about the messages you receive. There are some characteristics common to many scam attempts: messages claim a form of authority (perhaps pretending to originate from someone official), they may try to create an impression of urgency and engage the receiver emotionally. They may also offer you something in short supply, related to current events.

If you are in any doubt about a message, you can double-check directly with the person or entity that sent it to you. Do not use the details given in the message you have been sent to make this check: use another

[22] https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

method that you trust. This may mean phoning the organisation, visiting their official website, or logging in to your account via hand-typing in the web address you know by heart. Organisations may previously have let you know about things to look out for – for instance, your bank may have told you that they will never ask directly for your password.

**Resources:**

- Spotting Scams and Can You Spot a Scam? Quiz[23]
- Phishing and Civil Society – examples of real-life scams aimed at civil society groups (Net Alert)[24]

[23] https://www.cyber.gov.au/protect-yourself/spotting-scams
[24] https://netalert.me/resources/en/secure-accounts/account-phishing/

# 3. More Key Steps for Organisations

## 3.1. Manage shared accounts

**Why this is important:** sharing account credentials increases the risk of an attacker being able to access them and makes safeguards like MFA less effective. When multiple individuals share a single account, it makes it more difficult to work out if and when an attacker has gained access.

**What to do:** avoid using shared accounts where possible - ideally create individual accounts for staff members that are accessed using MFA. Management tools are available that provide more secure ways of enabling multiple accounts to post to a social media channel. If it is essential to use shared accounts, make sure that MFA is enabled and keep a list of every staff member that has access. Passwords and other credentials should be changed when roles change, or individuals leave the business.

**Resources:**

- Social media: protect what you publish - includes advice on using social media management tools[25]

[25] https://www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish

### 3.2 Use access controls

**Why this is important:** limiting the amount of internal information staff members have access to reduces the potential for damage if their account is compromised. When staff members have administrative privileges, the risk of damage is increased.

**What to do:** review the files, accounts, and data each staff member has access to

only give administrator privileges to users who really need them. When roles change, or someone leaves the business change or revoke permissions as appropriate.

**Resources**

- Introduction to identity and access controls[26]

### 3.3 Use security software

**Why this is important:** using antivirus software and anti-ransomware protection can defend business devices. Antivirus software scans devices for suspicious files and programs and removes them from your device.

**What to do:** Many modern operating systems come with built-in security software. Third party solutions are also available.

[26] https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

**Resources:**

- Antivirus software- includes guides for common phone and computer operating systems[27]
- Consumer Reports (US) guide to antivirus software[28]

## 3.4 Secure your network and external devices

**Why this is important:** using antivirus software and anti-ransomware protection can defend business devices. Antivirus software scans devices for suspicious files and programs and removes them from your device.

**What to do:** Many modern operating systems come with built-in security software.

Third party solutions are also available.

**Resources:**

- Antivirus software- includes guides for common phone and computer operating systems[29]
- Consumer Reports (US) guide to antivirus software[30]

## 3.5 Secure your website

**Why this is important:** websites are, by definition, a major target for cyberattacks. Worse, when there is a security breach, the attackers can actually use your site to silently infect others who come to your site.

27 https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/antivirus-software
28 https://www.consumerreports.org/electronics-computers/antivirus-software/
29 https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/antivirus-software
30 https://www.consumerreports.org/electronics-computers/antivirus-software/

**What to do:** protect your website's admin pages with a strong passphrase and -preferably – MFA. It is important to make sure that website systems and any plugins are updated promptly. It is a good idea to back up your website in case anything goes wrong. You may want to implement defences against denial-of-service attacks.

**Resources**

- Quick wins for your website [31]
- Preparing and responding to denial-of-service attacks[32]

## 3.6 Restrict use of MS office macros

**Why this is important:** macros are small programs used within MS Office to

automate certain tasks. Unfortunately, they are also a well-known and long-standing entry point for cyberattacks. Attacks using this route can bypass other security measures you have in place.

**What to do:** disable macros for all MS Office users. Where your workplace uses macros, you should investigate ways of replacing this functionality and – in the meantime – restrict the use of macros to the minimum necessary.

**Resources:**

- Macro security for Microsoft Office[33]

[31] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/web-hardening/quick- wins-your-website

[32] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/preparing-and-responding-denial-of-service-attacks

[33] https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office

## 3.7 Keep your devices physically secure

**Why this is important:** business data is an attractive target to cybercriminals and special duties of confidentiality apply to some types of business data. Physically securing the devices on which data is stored makes that data less vulnerable.

**What to do:** limit physical access to your business devices. To authorised personnel. Secure devices with password, PIN, or biometrics and set them to automatically lock after a short time. When disposing of devices, it is important to reset or wipe them first. A factory reset will usually wipe the data on a device, but special procedures may be necessary where devices have stored data where strong duties of confidentiality apply.

**Resources:**

- Securing your device[34]
- Securing your mobile phone[35]

## 3.8 Train employees and make an emergency plan

**Why this is important:** cybersecurity practices can only be as strong as your colleagues' willingness to follow them. Having an emergency plan including who to contact when something seems wrong and how the organisation will operate in the meantime can reduce the impact of any attack attempt.

[34] https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/how-dispose-your-device-securely

[35] https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/secure-your-mobile-phone

**What to do:** train staff about common cybersecurity threats, ways to prevent them and what to do if they have concerns. Training should be part of an induction process for new staff and refreshed at regular intervals. Additionally, create a ransomware plan for who you will call, in what order, if the organisation suffers a major attack. Keep this plan accessible in hardcopy (paper) format not just online.

**Resources:**

- NCSC's cyber security training for staff now available[36]
- Cyber security toolkit for boards[37]

[36] https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
[37] https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

# 4. A ransomware response plan

Be prepared:

- follow the guidance above, in particular:
- make regular backups of your most important data (see Backup your data above)
- prevent malicious software reaching your devices (see 1,5, 9, 10, 11, 12)

Think about what might happen if your organisation were subject to a malware or ransomware attack: in a worst-case scenario, computer systems may become inoperable and it may take weeks for data to be restored, if that is even possible[38].

- Identify your critical assets and what the impact of an attack would be. How long would it take to restore the most important parts of the system from a backup?

- Determine who is a member of the technical response team, what are the criterial for determining whether there has been a security incident, what steps they should take and who has the authority to take remediation action (for instance, disconnecting a system from the wider network). The response team should have the means of communicating with each other outside normal office hours, and via different channels. It's crucial to have multiple ways for the team to stay in touch – practiced ahead of time – in case some go down.

[38] https://english.ncsc.nl/publications/publications/2022/augustus/2/incident-response-plan-ransomware
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

- Develop a communication strategy – there are a variety of internal and external stakeholders who will need to be contacted. Internal stakeholders

  could include: incident response team, other IT, senior management, legal, PR, HR, board members and insurance.

External communication is important in this instance to protect the organisation's reputation and restore trust.

- Response and recovery plans need to be stored in a way that is accessible even if the rest of the network is not. This includes having a means to be in touch with the key contacts the organisation needs in order to function.

- Decide how the organisation will respond to a ransom demand, if one is made, and what the response to internal information being posted online would be. Governments typically recommend not paying ransoms – as this supports the criminals' business model. Communication may enable you to better assess the extent of damage.

- Understand what your legal and regulatory responsibilities are – who you need to report the incident to (including data protection authorities and the police), and by when.