Cybersecurity Red Flags
Guidance for Lawyers

Victorian Legal Services
BOARD + COMMISSIONER

Cyber-safe practice is a professional competency crucial for all lawyers. Lawyers must be able to recognise and respond quickly to potential and actual cybersecurity breaches. This involves understanding the 'red flags' or warning signs of a breach or cyberattack, as well as knowing what good cybersecurity habits entail.

This guidance aims to help you identify cybersecurity red flags and take swift action to mitigate the impact of a cyberattack, thereby preventing further harm to your clients and workplace. Watch out for the types of red flags below to help promptly identify and report potential cybersecurity incidents:

Phishing attempts

Phishing scams use emails or texts that appear to be from a person or organisation you know or trust to trick you into disclosing sensitive information or login credentials (e.g. passwords or multi-factor authentication (MFA) codes), handing over money, or downloading malware.

Spear-phishing is a highly targeted form of phishing that involves contacting individuals in specific organisations, often in a personalised and seemingly credible way, or even by using a colleague's hacked email account.

Phishers employ psychological tactics to get you to act quickly without stopping to think or question their request. They may claim to be someone in authority, demand immediate action, or make overt or veiled threats. Examples include an email or text urging a funds transfer for a client's emergency settlement or unsolicited emails linking to "offers" or "free trials".

Never respond to urgent or unusual emails or texts, especially those involving financial transactions or changes to sensitive information. Do not open unknown or suspicious attachments or links. Verify requests by contacting a confirmed representative of an organisation or the client through alternative channels, such as phone calls or in-person conversations.

To avoid being fooled, we recommend following the checklist in the Law Council of Australia's cybersecurity training toolkit:

- **Slow down:** Don't let pressure to act quickly influence your careful review of an email or a pop-up on a website or your computer. Phishing emails and fake antivirus warnings try to make you act first and think later. If the message conveys a sense of urgency, be even more sceptical.
- **Check the facts:** Be suspicious of unsolicited phone calls or emails from service providers. Do your due diligence by calling the company directly or using a search engine to find the company's website and contact information. Double-check key details such as misspelt email addresses, spelling or grammar errors, or unusual email headers and attachments.
- **Confirm information requests:** Ignore any email requesting financial information or passwords, and never provide personal information unless you expected the request and can verify the sender. Contact the client or relevant parties through a known and trusted communication channel. Find out more about verifying client identities in matters involving financial transactions.

Physical threats to cybersecurity

Not all cybersecurity threats are online. Be vigilant about physical threats, such as people using other people's computers, watching others enter their PIN or password, gaining unauthorised access to secure areas, or strangers accessing offices and equipment.

Adhere to security measures and report anyone who looks suspicious or behaves like they don't belong. Exercise good personal security by locking your computer screen when leaving your desk and securely storing laptops, mobile devices, and external drives when not in use.

Suspicious changes to sensitive documents or electronic devices

Subtle changes to important details, like default user logins, last login times, file ownership or modification dates, or email unread markers, may be the only indicators of a cyberattack.

Keep an eye out for suspicious alterations or deletions of client files or records without proper documentation or justification. If you are unsure why changes were made, investigate promptly. Monitor for unusual attempts to open, copy, or modify those files, as this may indicate a cyberattack is happening or has already happened.

Unauthorised access attempts

Repeated failed login attempts, password reset emails, unexpected login requests that require you to enter a code from your phone, or sudden password failures could indicate someone is trying to access your computer system. This may also mean that your login details for both that account and your email account have been compromised.

Act promptly on unauthorised attempts to reduce the risk of malicious actors accessing your account and potentially using it to target other lawyers, clients, and courts within the legal ecosystem. Change your password or passphrase immediately.

Unusual network or computer activity

If your computer or network (e.g. internet, intranet, or shared drive) slows down suddenly, you see unusual pop-up messages that look different from your usual security alerts, or your antivirus program warns you about viruses or other dangerous programs, it may signify malware or hacking.

Never download or install anything unless you know where it comes from. When in doubt, contact your organisation's IT or cybersecurity contact for assistance.

If you notice any of these red flags, immediately report them to your organisation's IT or cybersecurity contact. Early detection and swift action are essential for reducing the harm caused by cyberattacks and protecting both client data and the reputation of your law practice.

Cybersecurity Good Practices
Guidance for Lawyers

Victorian Legal Services
BOARD + COMMISSIONER

Cyber-safe practice is a professional competency crucial for all lawyers. Lawyers must be able to recognise and respond quickly to potential and actual cybersecurity breaches. This involves understanding the 'red flags' or warning signs of a breach or cyberattack, as well as knowing what good cybersecurity habits entail.

This guidance includes tips about good cybersecurity practices that can help you avoid a breach, along with specific advice about verifying client identities before acting on email requests. Having good cybersecurity habits is an important way to reduce the risk of cyberattacks. Here are six simple practices you can integrate into your day:

Be wary of social engineering techniques

These involve malicious actors attempting to trick you into revealing confidential information or providing access to your computer system. For example, they may impersonate authority figures (e.g. your boss or a bank representative), IT staff (e.g. telecommunications or internet service providers) or clients, and ask for your login details or changes to key information. Always double-check the authenticity of requests before acting. Remember, legitimate sources will never ask for your password or MFA codes.

Be careful about what you share on social media

Malicious actors can exploit personal details to impersonate employees, establish relationships through ongoing engagement, or gain access to confidential information. Exercise caution when accepting friend or connection requests from unknown individuals or responding to unsolicited emails from organisations.

Never reuse a password

If a website or service you use is hacked, and your password is leaked on the Dark Web, hackers will rapidly attempt to use the compromised password with every account and email address associated with you. Use different passwords for each account, regularly update them, and change them immediately after a suspected cyber-incident.

Don't use unknown USB sticks and external hard drives with your work computer

These devices may carry malware that could compromise your system's security. Only use USB sticks and external hard drives on work devices if they are from sources you are confident are legitimate, and also use your antivirus program to confirm they are not compromised.

Exercise caution when using personal devices for work

Ensure personal laptops, smartphones, and tablets have up-to-date security software, strong passwords, and encryption turned on. Only use personal devices for work activities if you have permission to do so.

Never connect to unsecured public Wi-Fi networks for work without using a secure business VPN

These networks can be hotspots for hackers to intercept sensitive data and monitor your online activities.

SIGHT or SPEAK: Our expectation regarding client verification

Malicious actors may attempt to steal money or information by impersonating your clients or other lawyers. While it is convenient to receive email instructions from clients, there is a risk involved. Hackers can alter emails in transit or on your computer, manipulate bank account details, and deceive you into transferring money into the wrong account.

As the regulator, we expect you always to make sure any request for information or funds is legitimate by directly checking with the client. **Never act on email instructions without proper verification.**

To ensure you are receiving valid instructions, either meet your client in person (**SIGHT**), talk to them on a pre-arranged contact number (**SPEAK**) or do both through video chat. This is especially important if a client makes last-minute changes to their instructions or key information (e.g. bank account details).

We endorse the LPLC's Five Cybersecurity Steps to Protect Yourself:

1. **Identify:** Don't accept email requests on face value. An email asking you to redirect money might look genuine but could be sent by a hacker.
2. **Verify:** Call the sender personally to check authenticity. Use a known number, not one suggested in the email. Ask for the account number, write it down, then compare it with the email.
3. **Note:** Make a file note that you made the call and confirmed the payment instructions, so you can prove it.
4. **Warn:** Inform the client that they might be targeted with fake emails from you and should not act on email payment directions without calling to check. Include this information in your engagement letters.
5. **Double-check:** Involve a second person in the process and don't action payment requests without proof that steps two and three have happened.

If you notice any unusual or suspicious activity, report it to your organisation's IT or cybersecurity representative without delay.