CYBER SECURITY GUIDE **FOR LAWYERS**

A practical guide to help lawyers be cybersafe

LPLC LEGAL PRACTITIONERS' LIABILITY COMMITTEE

lplc.com.au

Law firms of all sizes, including sole practitioners, are targeted every day by cyber criminals from all over the world. Most law firms transact large amounts of money and hold confidential information that criminals can sell or use to extort a ransom payment.

Failure to protect your business and your clients' money and information could be costly both financially and to your firm's reputation.

Basic information for everyone

Every staff member in a law firm is responsible for keeping the firm safe from cyber-attack. There are many things that everyone can do, and this guide addresses the five basic areas to focus on to help lock the door on cyber-crime. It is important that everyone in a firm understands what the risks are and what part they must play in keeping the firm safe.

The Australian Government's **StaySmartOnline** website is a good place for everyone to start to review basic information about protecting your business online. Register for StaySmartOnline's **Alert Service** to receive updates on scams, risks and preventative action to protect your firm and your clients.

It is everyone's business

Cyber security is not just an IT issue. It is an essential part of today's legal practice and everyone in your firm has a critical role in preventing cyber-crime. There is no silver bullet to protect your firm and your client's money. The concept of cyber security must be built into everything people do in a law firm.

The approach to cyber security needs to be multi-pronged. This guide sets out five key areas to address, underlines **why** they are important, **what** can be done and **how** to do it. Included in this guide are links to valuable resources and information.

SECURE YOUR TECHNOLOGY

WHY **This is the way in for fraudsters. You don't leave the door to your office or your house open or unlocked when you are not there, and you should not leave your computers and other technology, which are linked to the internet, unsecured and easily accessible by any cyber-criminals.**

1 SECURITY SOFTWARE

Install reputable security software on all computers, including for remote access, with at least daily updates to the signature database and a daily full scan of files.

- Use an IT security professional who understands cyber security to provide you with advice, to set up your security and provide maintenance services
- You can check suitable security software products at AV Test website the Independent IT Security Institute
- Use this guide as a starting point for a conversation with your IT professional

2 BUSINESS GRADE

Use a business grade hosted email service, rather than using a free web-based email account as the security offered is much higher.

- Ask your IT security professional to assist you to choose an email service that provides business grade filtering such as Microsoft 365

3 CUSTOM DOMAIN

Use a custom domain name for your email rather than a free or generic email account like Gmail or Hotmail.
This makes it harder for cyber criminals to impersonate your email address and provides better security and spam filters.

- Ask your IT security professional to assist you to set up a domain name for your email

SECURE YOUR TECHNOLOGY

4 SOFTWARE UPDATES

Register for alerts to all software updates and promptly install them.

- Check your IT professional is doing this or delegate the task to someone in the office

5 MULTI-FACTOR AUTHENTICATION

Implement multi-factor authentication for all devices and cloud-based systems. If using Office 365 ensure you turn on two factor authentication.

- Ask your IT professional to set up multifactor authentication for you
- For more information see Implementing Multi-Factor Authentication on the Australian Cyber Security Centre website
- If doing it yourself, read How to use multi-factor authentication to combat cyber-crime

6 WEB FILTERING

Use Domain Name Server (DNS) web-based filtering service to block high-risk websites.

- Ask your IT professional about an appropriate Domain Name System (DNS) based web filtering service

SECURE YOUR TECHNOLOGY

7 BACKUP FILES

Backup files automatically, at least daily.

- Ensure your IT professional is backing up your system or delegate the task to someone in the office
- See StaySmartOnLine Backups and Backups for business

8 USER SECURITY

Ensure users return office devices, and can no longer access office systems, once their employment ceases.

- Create an office policy and checklist to ensure this happens

9 STRONG PASSWORDS

Have a documented policy and process for:

- creation of strong passwords changed regularly
- restricted use of removeable media like USB sticks, DVDs, CDs, memory cards

- Ask your IT professional to set criteria for passwords on your computer system
- See StaySmartOnLine Passwords for business

More information

Law Institute Victoria (LIV): Cyber security essentials for law firms
StaySmartOnline website: Protect your assets & Do things safely
Australian Cyber Security Centre: guides & publications

ESTABLISH POLICIES AND PROCEDURES

WHY **Written policies clarify what should happen and how people need to act. It gives you the opportunity to consider the risks and put in place strategies to prevent problems before they happen. Written policies and procedures about cyber risk issues provide clarity on how and what every staff member is expected to do to minimise the risk of a cyber incident.**

1 ELECTRONIC FUNDS TRANSFERS

Electronic transfers of money, including trust money, and email payment instructions.

- Be alert to and wary of any instructions received via email
- Any emailed payment details must be verified by phone or in person before transferring funds in accordance with LPLC's recommended process

2 SECURITY MEASURES

- Require multi-factor authentication
- Consider encryption of emails
- Require strong passwords, changed regularly
- Restrict use of removeable media like USB sticks, DVDs, CDs and memory cards to stand alone devices that have no access to the web
- Prohibit the use of public wi-fi such as provided in cafes, hotels, train stations and airports on firm devices

Regularly review these as security measures are continually changing as cyber threats evolve

ESTABLISH POLICIES AND PROCEDURES

3 CLIENT INFORMATION

- Consider the firm's Privacy Act obligations, and where necessary create a publicly available policy
- Allocate responsibility to a staff member for detecting and reporting breaches
- Specify how personal information is to be collected, stored, used and deleted, or de-identified, at the end of the information lifecycle

4 SYSTEM ACCESS

- Limit staff's access to files and applications on the computer system to what is necessary for their role ("need to know")
- Provide remote access only where necessary and specify conditions of use
- Specify conditions for use of personal devices for work purposes

5 STAFF TRAINING

- Schedule regular cyber security training for all staff including students and interns

More information

StaySmartOnline website: Protect your assets page.

Law Council Cyber Precedent website:
- Your firm their data
- Developing a cyber security strategy podcast
- Cyber security essentials
- Privacy principles and cyber security

CREATE A CULTURE OF CYBER RISK AWARENESS

WHY **Many cyber incidents, particularly business email compromise, occur because someone clicked on a link that allowed the cyber-criminal into the firm's computer system. Cyber-criminals use sophisticated social engineering to entice people to click.**

It is easy to operate at a fast pace and not stop to think about possible cyber risks in routine work. Developing a culture in the office of healthy scepticism and a 'pause before you act' approach for anything internet related is important to avoid getting caught out. Don't become a casualty of a casual attitude.

1 CREATE A SECURE EMAIL CULTURE

Require everyone to:

- always verify emailed payment details before transferring funds in accordance with office policy
- never open unknown or suspicious attachments or links
- regularly audit staff email settings, particularly their email rules to ensure their emails are not being redirected by cyber criminals
- not use public wi-fi for work purposes
- be alert to anything unusual or suspicious and check it appropriately
- adhere to the firm's policies and procedures about cyber security
- have an email retention/deletion policy

- Create policy, procedures and checklists to ensure payment details are verified
- Conduct audits to ensure the process is being followed
- Prominently display LPLC's Cyber Risk poster at your premises
- Send a regular reminder to have staff check their email settings
- READ:
  - National Archives Australia website on managing email
  - Australian Law Reform Commission on data security and information destruction and retention requirements
  - Australian Government Business website on how to keep the right records

CREATE A CULTURE OF CYBER RISK AWARENESS

2 UP-TO-DATE STAFF TRAINING

Provide regular and up-to-date training to all existing staff and new joiners, including students, interns and temporary staff about:

- cyber risk and their role in minimising it
- the firm's relevant policies and incident response plan
- who to contact if a suspected incident has occurred. 'See something, say something'

- Use the cyber security training toolkit on the Law Council of Australia Cyber Precedent website
- There are lots of providers offering training. Contact us if you want some direction in finding them

3 APPOINT RESPONSIBLE STAFF MEMBER

Appoint a staff member to be responsible for ensuring:

- the steps outlined in this guide are implemented
- cyber security news, updates and recent issues are regularly communicated and easily available as a reference.

- Join the StaySmartOnLine community and receive cyber risk alerts

4 CENTRALISED INFORMATION

Have a centralised place for storing cyber risk information, including the firm's cyber action plans, policy and up-to-date points of contact which can be accessed by all staff.

- Store on the firm's intranet or joint drive
- Keep paper copies in a readily accessible place

WARN CLIENTS ABOUT CYBER RISKS

WHY **Clients are equally susceptible to receiving fake emails from cyber criminals and being duped into paying money into the wrong bank account.**

1 EXPLAIN RISKS TO CLIENTS

Explain the risks of fraudulent emails to clients in your first face-to-face meeting.

- Use LPLC client brochure Cyber security – how to protect yourself

2 CONFIRM RISKS

Confirm the risks of fraudulent emails to clients in writing.

- Update your precedent letter of engagement

WARN CLIENTS ABOUT CYBER RISKS

3 VERIFY EMAIL REQUESTS

As part of your retainer, tell clients, and confirm it in writing, that you require them to verify any email requests by your firm for payment before transferring money.

- Update your first interview checklist and your precedent letter of engagement

4 INCLUDE A WARNING MESSAGE

Add a warning to your email footer about the risks of relying on payment details in email.

- See LPLC blog **Protect your clients from cyber fraud**
- Download and use LPLC's **Call before you pay** email footer or develop your own

HAVE AN INCIDENT RESPONSE PLAN FOR PROMPT ACTION

WHY **Cyber-attacks or incidents are now an inevitable reality for everyone, even law practices, as more cyber-criminals see law firms as a soft and lucrative target.**

It is important to ACT QUICKLY to limit any potential damage if you discover you have sent money to a fraudster's bank account or your computer system has been compromised resulting in data breaches and or your system locked.

Having a plan will make taking action faster and easier, reduce some of the stress and may well be an essential prerequisite for making a claim against any cyber insurance policy the firm has.

1 DOCUMENT A PLAN

Document what to do if a cyber incident occurs.

- authorise appropriate people to act immediately
- specify a contact for urgent IT assistance
- document a procedure in the event trust money is paid to the wrong account, including:
  - if it is a PEXA transaction, contact PEXA first
  - who to contact at the firm's bank
  - immediately contact the sending and receiving banks putting both on notice money has been wrongly paid
  - contact LPLC to notify a possible claim
- See Law Council of Australia Cyber Precedent website: What to do if you are cyber-attacked
- See the information at StaySmartOnline website: Recover when things go wrong
- See LPLC list of Cyber-crime bank contact details
- See LIV Cyber security essentials for law firms
- Check your IT provider's response capability
- Consider buying a cyber insurance policy with immediate incident response capability particularly for *Privacy Act 1988 (Cwlth) data breaches*
- See LPLC's cyber insurance information at lplc.com.au

HAVE AN INCIDENT RESPONSE PLAN FOR PROMPT ACTION

2 DOCUMENT PROCEDURES TO HELP CLIENTS

Document what to do if your client pays money to the wrong account.

Your plan should include:

- immediately contacting your client and asking them to reverse the transaction with their bank
- asking your client for a copy of the email they acted on
- obtaining instructions to enable you to put the receiving bank on notice that money has been wrongly paid
- notifying LPLC of a possible claim

3 TEST PLANS AND PROCEDURES

Test that everyone is clear about what they are required to do if something goes wrong.

- Hold a training session
- Develop a scenario that might happen
- Practice how the scenarios would be handled

USEFUL **WEBSITES**

Law Council of Australia – Cyber Precedent – strengthening the legal profession's defence against online threats

Australian Cyber Security Centre

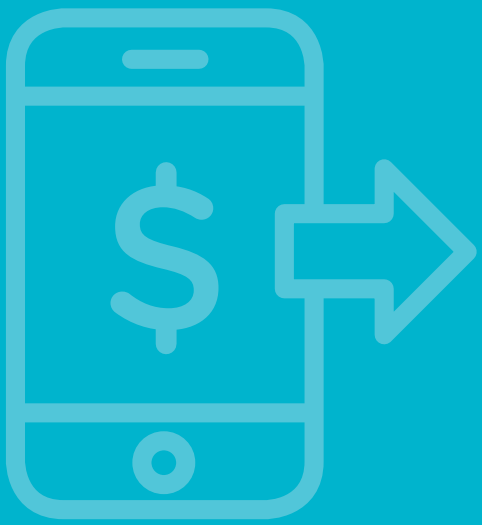
Australian Competition and Consumer Commission

Australia's Cyber Security Strategy

Australian Government Stay Smart Online

Australian Cybercrime Online Reporting Network

IDCARE – National Identity and Cyber Support



December 2019

LPLC LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Phone +61 3 9672 3800
Email lawyersrisk@lplc.com.au
lplc.com.au/cyber