Enable multi-factor authentication – a simple thing that could save you

This week is Australian Cyber Week and a timely reminder for law firms to review their cyber security strategy and, at a minimum, implement multi-factor authentication (MFA) if you haven't already done so.

All too often LPLC is contacted by law firms with compromised email accounts. In almost all instances the infiltration would have been prevented had MFA been enabled on the law firm's devices and networks.

What is MFA and where is it?

MFA requires a user to enter more than one piece of information or credential, in addition to a username and password, to verify identity and gain access to an account. The user typically needs something they personally have such as a mobile phone app, SMS code or token.

MFA systems can be set up so that you are not required to enter an authentication every time an account is accessed, but instead only when you log in via a new device or IP address. So even if a cyber-criminal gets access to your password, they can't access your account on their device without access to the extra factor sitting on your mobile phone or token.

There are many readily available MFA options. At a minimum, MFA can be enabled on Office 365 as well as most popular email and social media platforms including LinkedIn, Facebook, Instagram, WhatsApp, Gmail, Microsoft/Outlook Mail and iCloud. A search of the platform security and privacy settings will reveal simple steps to set it up.

Key takeaways

If your firm does not currently use MFA, we urge you to contact your IT professional to enable this on your devices and systems as soon as possible.

In addition to MFA, there are some other basic cyber security measures you can take which includes:

- ensuring staff passwords are sufficiently strong (passphrases of 20 or more characters are recommended)
- maintaining up to date software on your devices and
- educating staff in relation to cyber risks.

Cyber security risks are constantly evolving and protecting your firm's network and data requires vigilance.

Don't wait until it's too late and you experience a cyber-attack before taking these simple steps. The statistics tell us that this is a matter of when, not if - regardless of the size of your firm.

More information on how to set up MFA can be found in the LPLC's **Cyber Risk Guide for Lawyers** and **Implementing Multi-Factor Authentication** on the Australian Cyber Security Centre website.

Other tips and strategies for improving cyber security are detailed in the Cyber Risk Guide and in the **Cyber Security** section of our website.