10 March 2023

LEGAL PRACTITIONERS' LIABILITY COMMITTEE

No multifactor authentication? Say hello to a double excess from 1 July 2023.

Key points

From 1 July 2023 LPLC's policy wording will add a deterrent (double) excess where a claim arises due to the absence of multifactor authentication (MFA) on your email account.

This measure has become necessary to emphasise the importance of email security, with compromised email accounts having become a prime vehicle in recent years for cyber criminals to steal client funds.

The MFA deterrent excess will reinforce the existing 'call before you pay' deterrent excess (which will continue) where a claim arises from a payment or electronic funds transfer (EFT) made without the firm having taken reasonable steps to verify the purported instruction or authorisation.

If you have not yet implemented MFA on your email account, the time for doing so is now.

Email compromise is a major risk for law firms

LPLC is continuing to see cyber-related claims against practitioners where email accounts have been compromised and EFT payment directions are fraudulently altered by cyber criminals.

Preventing email accounts from being compromised in the first place is the best way to stop these claims from occurring. Without access to the firm's email account, cyber criminals cannot monitor, intercept and create fraudulent emails purporting to be sent by the firm.

One of the easiest and most effective ways to prevent your email account from being compromised is by enabling multifactor authentication (MFA). MFA requires anyone seeking access to the account to authenticate their account credentials in more than one way.

Since 2019 LPLC has been recommending MFA be utilised on all law practice email accounts. We know that many firms have heeded this message, but as these cyber claims have continued to persist it appears many firms have not yet done so. They are at higher risk of suffering an email compromise and exposing themselves and their clients to the risk of loss of client money from cybercrime.

To underline the importance of MFA and encourage greater implementation by law firms, from the commencement of the next policy year (1 July 2023) LPLC's insurance policy will include a **double excess** where a claim arises from unauthorised access to an email account used by any insured person where MFA was not enabled after 30 June 2023.

This will mean that if a firm does not implement MFA and a relevant claim arises, the firm will be required to bear a greater portion of the loss itself. If the firm's standard excess is $5,000 it will double to $10,000. If the firm's standard excess is $10,000 it will double to $20,000 and so on.

If your firm has not yet implemented MFA, the time for doing so is now.

What is MFA?

MFA in this context, requires a user to enter at least two or more pieces of information or credentials to verify identity and gain access to an email account. The user typically needs something they personally have such as a mobile phone app, SMS code or token to use as a second factor of authentication.

Authentication factors can be at least two or more of the following:

- something you know – e.g. a password, personal identification number (PIN) or response to a question
- something you have – e.g. a mobile phone app, SMS code or physical token such a one-time PIN token
- something you are (physically) – e.g. a fingerprint or iris scan.

LPLC's policy will not prescribe a specific mode of MFA. It is a widely understood concept and different online accounts or platforms may enable MFA to be implemented in different ways. The policy will only require that **a method** be implemented.

Most business platforms allow MFA to be easily set up via their privacy and security settings. 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.

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.

What do I need to do now?

If your firm has already implemented MFA across the firm's business devices, the change to the policy wording does not require you to take any further action.

If your practice is yet to implement MFA as an essential cyber security measure, time is running out. To ensure you will not be exposed to a double insurance excess should you suffer a cyber claim arising from email compromise, implement MFA NOW without delay before the policy change commences on 1 July 2023.

More information, resources and help to set up MFA

If you are unsure how to implement MFA on your email account (or any other online application), ask your IT professional to set it up for you now.

Australian Cyber Security Centre — multifactor authentication information including practical guides for setting it up on various platforms.

LPLC — information about multifactor authentication.