Cyber criminals continue to exploit firms without MFA

We continue to see firms who do not have multi factor authentication (MFA) in place fall prey to cyber criminals. The best gift you can give your firm and your clients this festive season is to implement MFA on your email accounts.

Without MFA your firm's email account is much more vulnerable to cyber crime — the firm's only line of defence is the account password which cyber criminals may be able to obtain via phishing, social engineering or other sophisticated techniques. With MFA in place, cyber criminals must also get past a second line of defence to authenticate access credentials to the email account (such as an SMS code) and this is much more difficult for them to do.

The absence of MFA has been a common feature of all successful cyber claims notified to LPLC in recent times where emails were either created or altered by cyber criminals to dupe firms or clients into transferring funds electronically to the wrong bank account.

Once cyber criminals are in your email account they can send emails to clients and other third parties from the account as if they were from you. The criminals can also configure your email account to create rules to divert these emails from your 'Sent' or Deleted Items' folder and hide their existence from you.

Cyber criminals are opportunists and will be taking advantage of staff in a rush to complete things before the holiday period and operating with an overlay of general fatigue after two years of a pandemic and lockdowns. They don't care who you are or what size your firm is. They care about what you have that they want — control over client money transfers. Every law firm is a potential target. Don't be the practitioner that has to explain to a client that there has been a cyber breach involving their money.

Protect your firm and you client's money by, **at a minimum, doing these four things before you go on leave** and making them an essential part of your firm's cyber security policy.

1. Set up Multifactor Authentication now on all devices, business systems and especially email software.

2. Implement and stick to — no exceptions — a 'call before you pay' policy. You should call your clients to verify bank account details before paying funds by electronic transfer.

Cont...

3. Warn client of the risk of fraudulent emails communications and advise them to phone your office to verify any email from you relating to the payment or transfer of money.

4. Check your email rules to make sure any rules that are there have been created by you and not a cyber criminal who has gained access to your system.

If, despite the steps, something does go wrong, initiate action immediately with the sending and receiving banks to investigate fraudulent transactions and stop money transfers before they are completed and funds are cleared. Banks are often able to trace and recover fraudulently diverted funds if they are provided with 'real time' information, or as close to that as possible.

More information and resources

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.

Watch LPLC's short explainer video about the importance of MFA and how it works.

Download LPLC's 'Call before you Pay' email footer and add it to your email signature as a reminder to recipients to confirm financial transfer details with a known source.

Keep LPLC's Cybercrime bank contact list handy so that you can contact sending and receiving banks quickly.

Listen to LPLC's podcast Cyber Security — not just a technology risk

In the event of any urgent cyber incidents during the 2021–2022 holiday season shutdown period, LPLC insured legal practices can contact us by emailing: Alix.Osborn@lplc.com.au