MANAGE FOR WHEN, NOT IF

Cyber attacks by email are on the rise and law firms of all sizes are at risk.

Cyber attacks on law firms of all sizes, but particularly smaller practices without the necessary safety measures in place, are on the increase. It is everyone's problem. What you need to know is set out here.

How they get into your email system

The most common way to get into your system is to send a phishing email encouraging someone in the firm to click on a link. The email usually looks like it has come from someone you know because their email account has already been hacked. Sometimes clicking on the link is enough to download software onto your system that allows the cybercriminal access. Sometimes the link takes you to a fake site, often looking like Office 365 or Dropbox, that requires you to enter your email address and password. This gives the cybercriminal access to your email account.

How to stop them

Be suspicious and don't click on links unless sure of their legitimacy. Call the sender to verify if you are unsure.

Don't put your email and password details into a website unless you are sure it is legitimate. Be wary of impersonations of common-use platforms like Office 365.

Use an advanced spam filtering tool – this stops the initial phishing email from reaching your email account.

Turn on multifactor authentication for accessing email accounts. This will prevent the cybercriminal from accessing the email account from other devices – even with the password.

If using Office 365, ask your email account administrator to check and turn on the audit setting to enable you to track activity in an email account later, even if the emails have been deleted. If using other email systems look for similar settings. With this setting on you will be better able to track what client data has been compromised.

What they do

Once the cybercriminals are in your email account they sit and watch the email traffic, often for many weeks. They often set up email rules that divert emails with certain words like settlement, bank account, BSB in them. They will intercept any emails containing bank account details, change them to divert money to themselves and on send. They will prevent relevant emails you or your client might send from getting to the recipient. Fake emails they send are either immediately deleted or moved to an unused folder like the RSS Feed folder.

Cybercriminals can, and often do, harvest all your contact email addresses and send further phishing emails to everyone you know from your email account. This often results in your inbox being inundated with bounce backs or return emails and a switchboard full of people calling to ask what is going on.

In a more recent attack, the cybercriminals had removed the lawyer's exchange licence and the account was in the process of being deleted when the practitioner called us. It appeared they may have been trying to steal the practitioner's data.

What to do when it happens

If you think your email account has been compromised immediately call your cyber insurance contact if you have cyber insurance. If you don't have cyber insurance, seek expert cybersecurity advice about the steps you need to take relevant to the situation. Your IT service provider may not know enough about these attacks to address all the issues. We can refer firms with LPLC PI insurance to relevant cybersecurity experts.

If your email account has been accessed, simply changing your password might not be enough if there is malware installed on your computer that allows the cybercriminals to track your key strokes and decipher your new password.

Even if changing your password locks the cybercriminals out of your email account, they may still be receiving emails via email rules and have already harvested your email contacts which they can then use to send further phishing emails from a bogus address. You will need technical advice to work out what the cybercriminals have done.

Consider what obligations you have to report this incident to your clients or to the Office of the Australian Information Commissioner as a notifiable data breach under the *Privacy Act 1988*.

Firms should consider cyber insurance to help mitigate the financial cost of dealing with the aftermath of a cyber attack. LPLC has worked with Marsh Insurance Brokers which has arranged a cyber insurance policy tailored to the needs of law firms whose professional indemnity insurance is placed with LPLC. A detailed explanation, FAQs and other information about the Marsh/Chubb cyber insurance policy can be accessed on LPLC's cyber page along with more cyber risk information at lplc.com.au/cyber. ■

This column is provided by the **Legal Practitioners' Liability Committee**. For further information ph 9672 3800 or visit www.lplc.com.au.

TIPS

- Be suspicious about links in emails.
- Don't put your email and password details into a website unless you are sure it is legitimate.
- Turn on multifactor authentication.
- Turn on the setting in your email account that enables you to track activity in an email account later.
- If your email account is compromised, immediately contact your cyber insurer if you have one or ask LPLC for a cybersecurity expert.

ADOBE STOCK