Cyber Attacks - People and procedure are the first line of defence

Cyber attacks on law practices are increasing and your practice is not immune

Barely a week goes by where there isn't a media report of a high profile cyber attack. So far in 2021 everything from media companies to government have been attacked, and law practices are no exception.

Over the summer break, Lawcover witnessed a spike in cyber attacks on law practices. Large sums of money have been lost when solicitors and clients were duped by email into transferring funds to a fraudster's bank account.

> In most instances, the hackers had been masquerading as the solicitor or client for some time before bank account details were changed.

Educating staff

Law practices need to continually educate staff about all forms of cyber attack, particularly email fraud.

While not the only fix, educating staff is probably the most important tactic to curtail a potential threat. Make sure all staff are aware of, and adhere to, any procedures put in place.

Visit Lawcover's Cyber Resources page for more information on how to protect you and your law practice.

Adherence to procedure

Implement robust procedures that ensure proper steps are taken when transferring funds and validating client details e.g., always check client phone numbers against those held on file before making contact. Cyber criminals use fake telephone numbers and create seemingly plausible excuses to explain why it's not possible to confirm account details over the telephone.

Three top tips

Keeping in mind the above, there are three simple things you can do to prevent this type of cyber attack:

1. Pick up the phone

Check bank account details are correct by phone before transferring any funds.

2. Train your staff

Ensure staff are aware of email fraud and that a consistent procedure is followed to prevent this type of fraud.

3. Warn your clients

Inform clients that you won't accept emailed bank account details from them and will never communicate your bank account details by email. Never rely on emailed bank account details, even if they seem to come from a legitimate source.

Cyber criminals are becoming more sophisticated, evolving their tactics as they uncover the methods firms use to combat them. It is essential that law practices stay on the front foot, continually educating staff with awareness training and ensuring effective policies and procedures are adapted and implemented.

If you believe that you may have received a fraudulent email, it's important to take immediate steps to ensure that your email system has not been compromised. Contact your IT consultant or the Lawcover group cyber risk policy crisis management team on 1800 BREACH (1800 273 224).