Cyber criminals are targeting legal transactions

Law practices are experiencing another spike in cyber-assisted fraud claims involving emailed bank account details.

Most attacks involve clients transferring funds to criminals believing they are putting money into solicitors' trust accounts. Other attacks include fraudulent calls from the solicitor's bank, leading to theft from trust accounts.

Cyber attacks are evolving in sophistication, and there is no technical solution that can substitute for human vigilance. Be suspicious and train all staff to be vigilant about checking identity of callers before disclosing any kind of information.

Warn your clients

Make sure your clients are warned about making payments to your firm, especially where bank account details are contained in email. Warn all clients who might attempt to pay funds into your trust account that they must telephone to check bank account details with your office, and direct them to call via a telephone number advertised on your website.

For large transactions, warn clients to make small "test" payments and telephone the practice to confirm receipt. Warn clients that cyber criminals sometimes initiate phone calls pretending to confirm details, so they must call the practice's direct reception number.

Make a practice of sending this brochure to your clients warning of cyber fraud risks, and include warnings in costs agreements and email footers: https://www.lawcover.com.au/wp-content/uploads/2022/09/Cyber-Fraud-Brochure_LSNSW-and-LCI.pdf

Use multi-factor authentication on all applications

Some cyber attacks originate from cyber criminals gaining access to the law practice's email system through phishing or other scams. The risk of those attacks can be minimised using MFA on email and other applications. Lawcover has produced a useful guide on how to protect your applications using MFA which can be downloaded here: https://www.lawcover.com.au/wp-content/uploads/2022/09/Cyber-Security-Snapshot-PROTECT-YOUR-EMAIL-CHAT-APPS-MESSAGING-AND-SOCIAL-MEDIA.pdf

Be wary of any unsolicited calls from banks

Lawcover is aware of a scam involving criminals impersonating bank staff and gaining online control of law practice trust accounts, transferring money to themselves. Be suspicious of any unsolicited telephone calls and particularly wary if they ask the law practice to log on to trust accounts while on the telephone.

Double check bank details – name matching

Many banks now have name matching technology, which will provide an alert if the name you have entered does not match the bank account name. Do not ignore alerts from banking software as this can be the first indication that a fraud is being attempted.

Don't click – links and attachments

Remember to always inspect links before opening. Make sure the destination domain name matches the real business or organisation and never click on suspicious or unverified links.

Remember the Lawcover Group Cyber Risk Crisis Management Team is available on 1800 4BREACH (1800 427 322).

How to defend yourself and your clients

Warn your clients

Inform all clients that they must telephone to check bank account details and direct them to call via a telephone number advertised on your website.

Don't ignore alerts from banking software

An alert can be the first indication that a fraud is being attempted or that details are incorrect (e.g. names).

Install multi-factor authentication on all applications

Protect your applications using MFA.

Human vigilance

Don't click on unverified links and attachments. Make sure the destination domain name matches the real business or organisation and never click on suspicious or unverified links.

Phone calls

Be wary of unsolicited phone calls particularly if they ask the law practice to log on to trust accounts while on the telephone.

Education and training

Educate staff on cyber security and train staff to check the identity of callers before disclosing any kind of information.

If you believe your law practice has experienced a cyber incident, you should immediately take steps to ensure that your IT system and emails have not been compromised. Contact the Lawcover Group Cyber Risk Crisis Management Team on **1800 4BREACH (1800 427 322)**.