The ongoing threat of cyber fraud

Law practices continue to be targeted by cybercriminals who are becoming increasingly sophisticated, and persistent, in their attempts to redirect funds away from intended recipients- and into their own bank accounts.

In most cases, the fraud occurs when the law practice's email system is compromised and the cybercriminal impersonates an employee of the practice, the client or the other party's solicitor to provide updated bank account details. The transfer of funds is then made to the fraudster's nominated account without any account verification processes taking place.

In a recent claim involving a property purchase, the law practice provided bank account details to the client by email. As the solicitor did not receive the funds when required, he emailed the client requesting proof of payment.

The cybercriminals impersonated the client's bank manager and sent an email to the solicitor stating that the client had transferred the funds to an account using the incorrect BSB.

Upon making enquiries, the client's bank manager denied sending the email and a check of the email address confirmed that it was not sent from the bank manager's genuine account. The solicitor contacted the client who advised that, following receipt of the solicitor's original email, he received a further email purporting to be from the solicitor containing 'updated' bank details. In reliance on the fraudulent email, the client transferred funds to the cybercriminal's account.

Obtain or confirm bank account details in person or by phone

The safest way to provide or obtain bank account details **is in person**. This could be done when you initially meet with the client, for example at the time of an identity check in a conveyancing transaction. If bank account details cannot be obtained or confirmed in person, the next best method of verification **is by phone**. Call the sender of the email, using a credible number from your client's original instructions. **Do not rely on a telephone number contained in a suspect email.** If you provide bank account details to your client, ask them to telephone you to confirm the bank details before they transfer the funds.

Add a cyber fraud warning to your email footer

An effective method of ensuring that clients are informed about the risks of cyber fraud is by **adding a statement to your standard email signature advising that, you will never change your account details by email,** and that they should contact your office in the event they receive an email indicating otherwise.

Regardless of whether you are providing bank account details to your client, or your client is providing details to you, if those bank account details are provided by email they must be verified through an alternate method before the transfer is made.

Renee Stevens
Legal Risk Manager