Client money at risk – EFT email fraud a continuing threat

Lawyers retained in transactional matters involving the electronic movement of client funds are continuing to be targeted by cybercriminals through compromised email accounts and fraudulently sent or altered emails.

There is no worse feeling for a practitioner than a phone call from a client saying they haven't received the money they were expecting, and that monies have somehow ended up in the wrong bank account controlled by fraudsters. How could this have happened?

It's not a new risk – practitioners know or should know about it and be taking proactive steps to minimise the risk of becoming embroiled in email scams.

The most galling scenario is that the firm's email system has been compromised by cybercriminals and emails to your inbox have been altered before you receive them, or outgoing emails intercepted and altered before being on-sent to the client.When the emails contain directions for the payment of money, the consequences of not verifying payment instructions or bank account details by a phone call to the client are obvious.

But there are other variations too – for example, the compromised email account may belong to the client or to a third party, such as a real estate agent or another party involved in the transaction. The email you receive is different to the email sent by the client or third party, or it may be a completely fictitious email created by cybercriminals. The lawyer may be no more than an innocent conduit passing on emailed bank account details to a third party without verifying them, and the third party assumes they are correct and doesn't verify them either.

The troubling thing for practitioners is that in all of these scenarios money has gone missing and a claim against the lawyer may well ensue.

The following three measures will help law firms minimise the risk of having client funds paid to the wrong bank account.

1. Secure your computer systems including setting multifactor authentication.
2. Independently verify all email instructions received with bank account details for electronic funds transfers – verify account details through a known phone number for the client, not one included in the email.
3. Train staff to be alert for email fraud – be suspicious of any changed payment directions, particularly where the email suggest there is urgency in activating the request.

Securing your system

Securing your external permitter defences includes installing fire walls, anti-virus software, email filtering software, web filtering software and keeping all your software up to date. It also means implementing protocols like limited number of password attempts before the system locks, and by enabling multifactor authentication (MFA) on devices.

Multifactor authentication is easy to do

Multifactor authentication is quick and easy to set up and every firm needs to have it in place.

MFA, sometimes referred to as two factor authentication, means you are not relying on a password alone to gain access to your account. There is a second step which involves not something you know (like a password) but something you personally have such as a code sent by text message to your phone, or an app on your phone that requires you to approve access.

Once you have MFA set up on a device you don't have to do it again or for extra security you could choose to do it every time you access the account.

If the cyber-criminals are able to use brute force to guess your password, or deception to get you to put your password into a false site, they won't be able to access your account from their device without the extra authentication.

You can find more information about how to set up multifactor authentication in our Cyber security guide for lawyers.

Verify bank account details

You CANNOT trust bank account details sent by email, whether in the body of the email or in a PDF or other attachment. You need to verify that the purported sender of the email actually sent the email and that it was not altered before it reached your inbox.

The validity of the payment details must be verified independently of the email. The best means of verification is a phone call, or videoconferencing is another option now that many lawyers have adapted to that technology. Do not rely on a phone number or contact details in the email as they may have been set up by the cyber-criminals.

We know verification can be time consuming, especially if the sender is overseas, but it is more difficult conversation to have to tell the person later their money was stolen.

Be the person who always verifies the bank account details, no matter what.

Download a copy of our Don't fall for it poster to display in your office to remind you and your staff of the steps to keep your client's money safe.

Add our Call and verify before you pay email footer to your firm's standard email signature.

These email compromise attacks are not going away and law firms need to take action now to protect their computer systems and their clients' money from these attacks.