# A Cautionary Tale – SMS to email

Do you communicate with clients using SMS? Does your IT system convert your incoming mobile phone messages into email?

Over the past 18 months, Lawcover has been notified of a significant number of cyber-attacks on law practices.

It's not surprising that this increase in cyber attacks has coincided with the global pandemic. Extended lockdowns have forced many solicitors to implement makeshift operations at home to keep their practices operating. When solicitors and their staff are working remotely from home offices, faced with many distractions and frequently on mobile devices, they are vulnerable to sophisticated cyber-attacks.

One such attack was recently perpetrated on a conveyancing firm. Having compromised the practice's email, the fraudsters began a payment redirection fraud.

Impersonating a client, fraudsters sent an email to the practice providing incorrect banking details for a transfer of funds held by another law practice on behalf of the client. Upon receiving the email, the solicitor forwarded it to the practice holding the funds and requested the transfer.

Prior to the transfer being completed, the practice discovered that its IT system had been compromised. The solicitor immediately contacted the practice holding the client's money and asked them to stop the transfer before calling her client to verify the bank account details contained in the email.

Working from home with poor mobile phone reception, along with background noise from her children, the solicitor asked her client to confirm her bank account details via SMS to her mobile phone.

The practice's IT system was set up to convert incoming messages sent to mobile phones as emails. On receiving the client's SMS message as an email, the solicitor was relieved to see that the bank account details matched and then called the practice holding the client's funds to approve the transfer.

Unfortunately, the 'SMS to email' message had been intercepted and the fraudsters had changed the contents to match the fraudulent bank account details previously sent by email. The funds were transferred to the fraudsters' bank account and misappropriated. To date, none of the money has been recovered.

It's a cautionary tale that reminds us that any form of communication can be intercepted if adequate precautions aren't taken.

Solicitors need to be especially vigilant on transactions involving large payments and should not rely on bank account details received via electronic means. Bank account details should always be confirmed by the solicitor in person or over the phone using a trusted phone number.

It is only with awareness, appropriate prevention measures, and constant caution that these types of cybercrimes can be prevented. Contact your IT consultant for further guidance.

If you believe you have received a fraudulent email you should take steps to ensure that your email system has not been compromised. Contact your IT consultant or the Lawcover cyber risk crisis management team on 1800 BREACH (1800 273 224).

Natalie Sullivan
Claims Solicitor