Short Minutes Transcript: Everyone's a target

Email fraud targeting law practices has become increasingly sophisticated and prevalent. Generally, the law practice has been duped by an email directing the payment of funds into a fraudsters bank account.

The emails are often sent in relation to matters involving the payment of substantial sums of money, such as the settlement of conveyancing transactions, the distribution of estates, or payment of settlement amounts in litigation.

Fraudulent emails can be very difficult to distinguish from genuine emails and are often received shortly before a deadline such as a conveyancing settlement. However, there are some simple steps that can be incorporated into everyday practice to minimise the risk of becoming a victim of cyber fraud:

- Never assume that emailed bank account details are correct. Always verify bank account details with the sender by telephone or other non-email means
- Use a known number from your client files - do not rely on a telephone number or other contact details in the email
- Build bank account details verification processes into your practice checklists and ensure that all staff are trained to follow the verification process
- Always treat last minute emails advising of a change of bank account details with suspicion. If you cannot reach the sender to check whether the new bank account details are genuine and correct it is generally preferable to delay settlement than to proceed without verification

If you believe you have received a fraudulent email take steps to ensure that your email system has not been compromised. Contact the Lawcover Cyber Risk Crisis Management Team on 1800 BREACH, that's 1800 273 224.

I'm Malcolm Heath