# Email Assisted Fraud – new and evolving threats

Lawcover has seen an increasing number of email assisted fraud claims since 2017 and they tend to be similar in nature:

- The client is expecting a monetary settlement
- The solicitor's or client's email is intercepted or 'hacked' by a fraudster
- The fraudster (posing as the client) redirects the payment to their own bank account, usually by issuing new instructions to the solicitor.

Over the years we have seen these attacks become more sophisticated, as fraudsters develop new ways to circumvent increased security.

One of the new ways in which fraudsters target solicitors and their clients involves interaction between multiple law practices. For example, a law practice receives an email purporting to be from another known practice. This email includes three documents to be opened along with instructions on how to open them. If the instructions are followed, their email system is infiltrated with spyware and/or malware by a fraudster, designed to monitor email activity within the practice.

In the weeks that follow, emails to the practice containing account details for the payment of deposits by the practice's clients are intercepted and the bank account details changed. The practice then forwards these altered emails to its clients who subsequently pay their deposit into the fraudster's bank account.

Fraudsters understand our email habits and how we are likely to behave when we receive emails, particularly when they are from known contacts or trusted sources.

Fortunately, there is a lot that can be done to stop fraudsters in their tracks:

- By installing and maintaining email security software, you'll add an extra layer of assurance that alerts you when a suspicious email is received. Suspicious emails can be flagged by your security software and blocked from further infiltration.
- Exercise judgement and scrutinise every email you receive:
  - If you are even slightly suspicious, don't open the email. If you know the sender, call them and check before proceeding
  - Do not click on links or attachments in suspicious emails, even if they are from a trusted source.
  - If unable to confirm the authenticity of an email, delete it and make a note of the sender.
- Make that call - always confirm emailed bank account details over the phone
- Inform and educate - make staff aware of evolving scams and ensure that they, and your clients, are aware of the risks associated with emails.

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).

Lawcover's Cyber Risk e-module is available free of charge and contains real examples of cyber fraud and how these can be recognised and prevented, as well as useful resources for solicitors and staff.

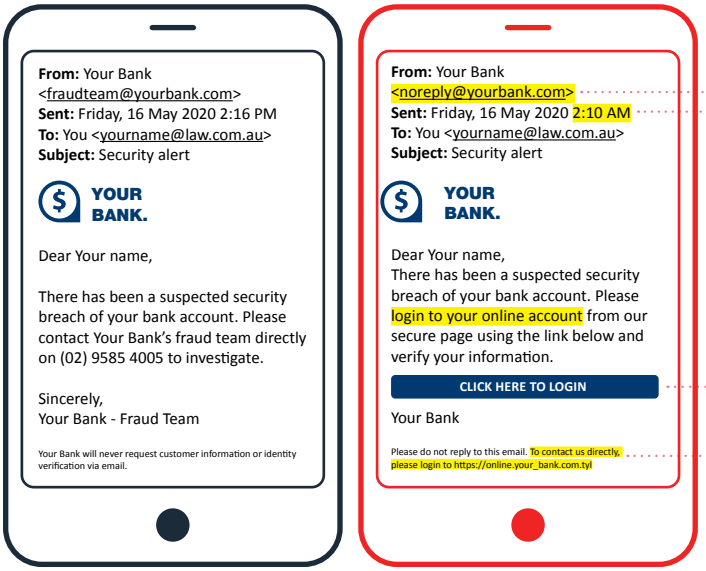
For further information on cyber fraud and how to avoid it, visit the cyber resources page on Lawcover's website.

Candice Perriman
Risk Education Manager
Practice Support Services

# Warning Signs

## RANSOMWARE

**Spotting suspicious emails**




## BUSINESS EMAIL COMPROMISE

**Spotting suspicious emails**