LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Protect your clients from cyber fraud

Just as you need to protect your firm against scam emails directing payment of trust money to cyber criminals, you need to be proactive in warning clients they might be targeted with fake emails from your firm.

We are aware of several instances where clients received scam emails purportedly from their law firm directing payment to a new bank account. Typically, the fraudster became aware of the work the firm was doing for the client after gaining access to either the client or firm's email account.

At the start of every matter, tell your clients:

- your firm's trust account details are in its engagement letter and will not be changed
- if the client receives an email from your firm containing changed trust account payment details, they must telephone the firm to verify the position, and not respond to the email.

Put this information along with trust account details in your firm's standard engagement letter. Consider providing clients with a cyber security brochure like the one on LPLC's website.

We also suggest adding a warning to your firm's standard email signatures along the lines of:

> *WE TAKE THE RISK OF CYBERFRAUD SERIOUSLY AND SO SHOULD YOU. Hackers have impersonated law firms and requested payment via email using their own account details. It is important you take the extra step to verify any bank account details you receive in an email from our firm by speaking to us before transferring money. Use a search engine to find our website and verify our phone number and call us. Do not reply to any emails asking for payment before verifying its authenticity with us.*

Finally, discuss this important issue with colleagues and other firms, so everyone is aware of the risks.