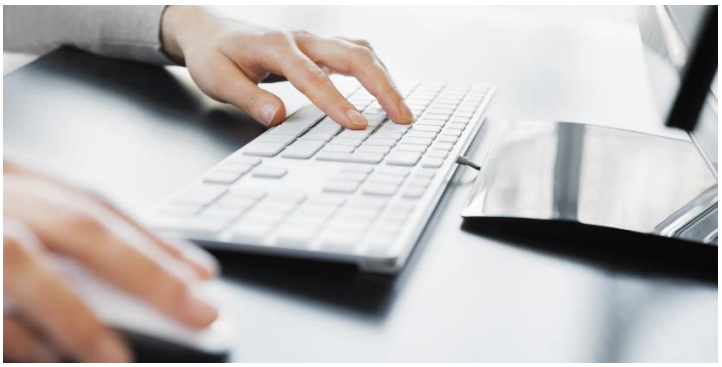
Do not rely on email instructions with respect to payment & account details

GRANT FEARY, DEPUTY DIRECTOR, LAW CLAIMS



According to recent research, a large percentage of Australian property lawyers are not aware of the scale of the risk of fraud in property transactions. This is worrying as there has been a huge amount of publicity surrounding these matters for some time now.

In a survey of 170 property lawyers and conveyancers, conducted by Research Company Global X, 46% of respondents were unaware of the latest scams which are targeting property investors and home buyers. These scams include impersonating lawyers or conveyancers then emailing clients regarding changing account details so that money is sent to fraudulent accounts, and hacking client lists so that the fraudsters can impersonate clients and request that the lawyer or conveyancer direct funds to fraudulent accounts.

Cyber thieves are clever. They target lawyers (and property transactions in particular) because we direct transfers of large sums of money and they want to steal it. Interesting and recent examples of the problems caused to lawyers and conveyancers by cyber-fraud and, in particular, identity theft, can be found in the English cases of *P & P Property Pty Ltd v Owen White & Catlin LLP and Dreamvar (UK) Ltd v Mishcon De Reya [2018] EWCA Civ 1082* which were decided on 15 May, 2018. These cases will be the subject of a future Risk Watch article.

The Legal Practitioners Liability Committee in Victoria have produced a very helpful single page document entitled "*Cyber Fraudsters will get in any way they can. Make sure it's not through you*" which should be read and understood by all. The document, as shown on the opposite page, can be downloaded at: **https://lplc.com.au/risk-management/cyber-security-2/cyber-fraud-dont-fall-for-it/**. We encourage every Law Practice to do so and display in the staff kitchen and/or other shared spaces so it is seen by everyone.

The message about being suspicious of and never relying on email instructions with respect to payment instructions and account details needs to be ingrained into all practitioners. Such instructions need to be confirmed on the telephone or in person from someone who you know is your client and has proper authority.

The risk posed by bogus email instructions is by no means the only type of cyber security risk but it is a risk that should be able to be addressed. Legal practices, no matter how small or how large, need to realise that these things do happen and to get over the assumption that "*it won't happen to me*".

If you suspect funds have been stolen, stop payment at the Bank immediately.