

# CYBER ATTACK IS A MAJOR THREAT TO YOUR LEGAL PRACTICE — IT IS REAL AND IT IS HERE!

**Happy New Year I mumbled to myself as the first claim notified for 2018 involved a cyber attack on one of our firms.**

The claim I received involved an email from a client to a law firm that was intercepted by a fraudster and the account details were changed. The money was paid by the law firm into the fraudster's bank account. The funds have not been recovered. A claim has now been made by the client who has lost her money and liability is being investigated. It is not automatic.

Other Professional Indemnity Insurance schemes for lawyers in Australia have reported a number of money movement interceptions following the hacking of anyone in the transactional chain (client/law practice/agent). Once the fraudsters have visibility over the flow of funds, they impersonate the person who will be giving directions about payment (and block the legitimate email account) to divert the funds.

Anyone can be hacked. Your firm's computer system is an obvious target. A fraudster can intercept an email from your firm and then direct where money is to be paid by the client. Your client can be hacked. Even if your firm has the best IT system, what seems like a legitimate email from your client could be from a fraudster.

All firms should be focusing on the funds transfer step and should not trust email-only communications from anyone.

Another common attack comes from infected emails, whereby when someone in the office clicks on a link in the email it releases ransomware which locks down the firm's computer system and a ransom is required to have it released.

The Law Society of NSW has warned that cyber fraud on solicitors' trust accounts is increasing and is expected to become a key issue in 2018.

*All firms should be focusing on the funds transfer step and should not trust email-only communications from anyone.*

In a recent matter in NSW, the solicitor (without knowing) was actually corresponding with the client and the fraudster at the same time. In that case over $850,000 was transferred from


Image – Adobe Photostock

the solicitor's trust account. It was not until 9 days later that the client emailed her asking where his money was. Unfortunately it was too late and the money was gone.

### How do these scams work?

- Scammers hack into solicitors' email accounts and obtain client information and, in some instances, are able to redirect emails addressed to solicitors into spam emails.
- Where emails are redirected into solicitors' spam, the scammer is able to alter the account details to which funds are requested to be transferred and then put their altered email into the solicitors' inbox.
- When the scammer has a client's details, they create a new email address that looks nearly identical and then directs a solicitor to transfer monies into their nominated account.
- If a scammer is trolling through clients' computers and picks up that a conveyance or estate distribution is to take place, they then assume the identity of the client.

### How do you protect yourself?

- Always keep your computer security up to date with anti-virus and anti-spyware software and an efficient firewall.
- Ensure that all staff at your firm are aware of the scams and understand how they work, so they can identify them.
- Double-check email addresses when receiving directions for payments. This includes emails from other law practices.
- Do not seek verification by email – telephone the client to authenticate the account details.
- Call the client on the number you have on your file and not the one shown on the email.
- Keep an eye out for phony emails. The grammar of the scammers often is not at the same level as that of the client.
- Do not click on links embedded in emails from people you don't know.
- Advise your client at the commencement of a matter what your firm's payment details are and advise them that your firm will not change those details unless you speak to them first.
- Advise your client that if they are at all concerned or suspicious about the validity of any email request they receive from you, they should not action the request before contacting your office by telephone and speaking to the person that has carriage of their matter.

According to a cyber security expert lawyers are "the weakest link" when it comes to cyber fraud.

Ray Zur is the founder and CEO of security company Cybint Solutions and a qualified legal practitioner. At the 2017 International Bar Association Conference in Sydney, he warned lawyers that they will increasingly be targeted by hackers.

Mr Zur said that lawyers are a target because their data and clients are interesting. Hackers can exploit human nature not just digital vulnerabilities.

At the conference, Mr Zur demonstrated how Wi-Fi security could be compromised with two simple examples:

First, he asked the audience "who is connected to the Wi-Fi network here?" He advised, "You should know that if you're connected to the Wi-Fi network, whatever you're doing, browsing, while you're connected to the Wi-Fi network, is exposed."

*Don't delay, take action now and avoid cyber fraud.*

"Right now, by just connecting to the same Wi-Fi network, I can see what you're doing on the internet just by using a very easy-to-do attack that is called ARP [address resolution protocol] spoofing. I can download two tools for free online and do it"

Secondly, Mr Zur told the conference that he could change the name of his phone and call it "IBA free Wi-Fi" and change the password of his phone and give it the password of the conference. He did it the day before and a few people connected to the internet through him. He immediately shut it down (because it is illegal) but he did it to make people aware of how easy it is to do.

Mr Zur said every internet device is a potential access point to a law firm's data, including mobile phones, printers and security cameras.

"Your phone is not a phone, it's a computer," he said. "You need to treat it as a computer: antivirus, anti-malware…If you're doing these security measures with your computer but not with your phone, it means that if nothing else, your phone is also the best eavesdropping machine. It has a camera, a microphone, and with just one text message, if you click on it, it can become an eavesdropping machine in your office, in your board meeting, in your partners' meeting, whatever."

Mr Zur urged lawyers to stop thinking of cyber security as an IT problem, and to make sure their staff and partners are trained as fast as possible.

### Cyber risk is a major threat to legal practice

That is why the Law Society of Tasmania has been encouraging all law firms to take cybersecurity seriously. The Society has been promoting **Cyber Precedent**, which has been launched by the Law Council of Australia to help law firms protect themselves against cyber threats.

As our President published in a notice to the profession last year, Cyber Precedent has been custom-built for Australian legal professionals. The resource includes:

- A list of the essential cybersecurity precautions law firms should take;
- Advice on how to protect against ransomware;
- A response checklist in the case of cyber attack; and
- A cybersecurity toolkit for the education of all lawyers and staff.

Don't delay. Take action now and avoid cyber fraud.

**ALISON CLUES BA LLB**
**Claims Manager, Professional Indemnity Insurance Scheme**
**alison.clues@alisonclues.com.au**

*References:*

Scam alerts, Law Society of NSW (24/10/17) Cyber Security – Legal Practitioners' Liability Committee and Law Society of Tasmania, Lawyers Weekly – Big Law by Tom Lodewyke (31/10/17)