Queensland Law Society

QLS Guide: How to stop cybercriminals stealing your client's money

A quick reference guide

November 2019

Business email compromise

What it is

This scam is a relatively simple but devastatingly effective way to divert funds in transit between client and solicitor's trust accounts. It has been used to steal millions of dollars in Queensland and throughout Australia. It does not require high level hacking skills and any firm, no matter how large or small, can be targeted.

The thefts have usually involved property transactions, but criminals also use the same method to divert any funds in transit. Successful diversions include estate distributions, personal injury settlements, or even payment of counsel's invoices for a trial – in short, any large amount moving from account to account. Even a bank cheque can be diverted if it is made out to the wrong payee or deposited to a fraudulent account.

Key point: **If money is moving, money is at risk.**

How it works

The usual starting point is when a criminal obtains access to electronic communication, often by means of compromised email. When it comes time to transfer funds, the message by which one party informs the other of the destination bank account is intercepted and altered. Most banks don't check that an account name matches the account number.

The diversion can happen when money is coming **to** the firm or where being disbursed **from** the firm.

There are many possible *points of entry*. A solicitor's office system, a staff member's home computer, the firm webmail or the client's computer have all been compromised and used to launch successful attacks. Poorly set up Office 365 webmail is a prime target. There are also many possible *methods of entry*, such as Phishing, Stolen Passwords and using malware.

This guide is not concerned with keeping attackers out of your firm's email (which is of course of high importance – see the QLS website for other resources here). It is about adopting safe processes, based on the assumption that email cannot be trusted.

Remember – It can be just as effective to hack a client's computer as it is to hack the firm's, and a firm can be responsible for stolen money even if your own system was not compromised.

Key point: There are many ways into the communication stream – both at the solicitor's end or the client's. **You must assume that all email can be intercepted and plan accordingly.**

What to do about it

Like most risk management law firms need to undertake, preventing loss of funds in transit relies partly on people, partly on processes and partly technology. Firm managers and leaders are the only people who can align all of the necessary moving parts to put these defences in place – it cannot be left to IT.

People

Awareness training for firm staff (and owners) is an excellent starting point. If you are insured by Lexon, access the free online Lexon Training.

Training needs to cover:

- how these scams operate, and that any firm can be a target;
- how to spot and avoid Phishing emails;
- how to use passwords responsibly; and
- what protocols and policies the firm has in place to avoid client money being stolen in transit.

This training is not complicated and can be delivered internally or using low cost external resources. Awareness fades quickly, especially under the time pressures of a busy day so you will need to have periodic reminders. You cannot change entrenched work practice or bad habits of a lifetime by sending an email. Face to face is best, backed by resources and materials.

Process

Humans will always make mistakes, and firm policies need to be there to catch them. Some of these are mandatory (for Lexon insureds) and set out in Lexon risk packs. Always use the most up to date risk pack version. In general terms, policies should aim at the following outcomes:

- **Never** transfer money based on email communication alone. **Always** contact the client by phone bearing in mind that the number you use to ring on must be checked. Criminals can (and do) send fraudulent emails then "verify" account details either by ringing themselves or inserting a fake contact number in the email for you to ring. (Verification by other means, such as secure messaging or SMS does not satisfy the Lexon conveyancing protocol.)
- If criminals gain access to your online transaction platform or practice management software, previously verified account details can be changed. Make sure these platforms are locked down tight, and check for changes in bank account details. Ensure that helpful reception staff know not to change contact or account details based on unverified requests.
- Large transfers should be double checked by a second team member.
- Ask your team to consider what risks they see in the work they do, assuming that communication can be manipulated.
- Clients need to understand that you will **never** ask them to transfer funds by email alone. This message needs to be communicated carefully, and reinforced. Warnings in your retainer, initial engagement letter and email footers is a good first step, but clients may not understand the importance of written notices or might forget. Verbal reminders in all matters in which the client will be transferring large sums is a good practice.
- If you are insured through Lexon their risk packs will include mandatory and suggested warning protocols.

Technology

All computers, phones and other devices used to access client data (both at work and home) should have:

- up to date software and "patches";
- mandatory two factor authentication;
- new, complex passwords;
- comprehensive malware protection (the paid kind, not the free variety); and
- no unapproved software, browser add-ons or apps installed.

Every network is different, so your technical defence requirements may vary. Larger firms will have access to sophisticated intruder detection systems, but even small organisations can implement effective technology to defeat the majority of attacks.

Unfortunately, even if criminals are unsuccessful in stealing money they can do a lot of damage to a law firm by copying confidential information, so it is necessary to take all reasonable steps to keep attackers out of the system.

Key point: Firm leaders are responsible for ensuring that information security is taken seriously, and that staff have appropriate skills and resources to protect client's money and data.

This guide is only a quick reference to the most immediate steps that can be taken. Legal practice in a connected world requires a comprehensive information security strategy. QLS has many resources to support member firms of all sizes with information security.

Enquiries: David Bowles
Direct line: 3842 5937