Emails: Danger, handle with care

Simone Herbert-Lowe is Manager, Strategy and Innovation at Lawcover.

Lawcover

BY SIMONE HERBERT-LOWE

Snapshot

- Email scams are targeting law practices.
- It is prudent to confirm any payment instructions received by email using another method.
- Warn clients about email scams targeting funds transfers.
- Educate everyone in your law practice about potential risks associated with email.

Email is now an indispensable tool of professional life. It is fast, convenient and inexpensive – but unfortunately not always secure or reliable. While many law practices have in place security gateways to detect and block malicious emails, IT programs can't prevent all risks. While technology solutions are important, how do we factor in the 'human' component of professional risk – that is, the way the human who receives an email interprets the messages contained in it?

Adopting a less trusting and more critical mindset

Lawcover has recently noticed a spike in notifications from law practices reporting email-enabled impersonation fraud or serious damage as a result of ransomware or other malicious software that has been delivered by email. Some examples are below.

Email scams leading to the redirection of funds held on trust or pursuant to a settlement

These have included fake emails from a client to a lawyer, a lawyer to a client, or even lawyer to lawyer, in which the recipient is requested to transfer funds to a bank account accessible to a fraudster. Sometimes these emails have been sent from the sender's *actual* email account, for example where a scammer has gained access to the account of the client (or lawyer) via a weak password, or where a password has been copied while the user has accessed an insecure (often free) wi-fi network. On other occasions, access may be obtained via targeted hacking of a computer network or as a result of malware which has enabled the scammer to gain access. In other instances, fake emails have been sent from an entirely *different* account, but with an email address that is identical/nearly identical to the apparent sender, so that it appears genuine ('spoofing').

It may be the recipient's response to the email that will determine whether a fraud is successful

At this point, the vulnerability lies with the human rather than the technology. For a profession that is famously sceptical by nature, are lawyers too trusting when we receive emails? Lawyers who would be unwilling to transfer funds based on an unsigned authority may have a greater level of comfort in the same instructions received by email. Unfortunately, that level of trust can be dangerous.

Whenever an email contains instructions to transfer funds into a specific account, and regardless of whether it is apparently from a client, another lawyer or perhaps a real estate agent, it is prudent to verify these details by telephone first, ensuring also that the telephone number used to verify the directions has been obtained from a direct and secure source such as original instructions (and not from any telephone numbers appearing on the potentially fraudulent email). To prevent clients from transferring funds into an incorrect account after receiving a fake email from *your* office, consider informing them at the time of engagement that you will never change your account details by email and that they should call your office to confirm account details if they ever receive an email that appears to be from you providing directions for payment. Law practices can potentially reduce their vulnerability to spoofed emails by implementing a Sender Policy Framework ('SPF'), which is an email validation system designed to detect and block forged or spoofed emails. This is done by verifying the sender's email server before delivering all legitimate emails to a recipient's inbox.

Given the speed at which funds are now transferred electronically, and with all property transfers in NSW to occur electronically from 1 July 2019 via the PEXA platform, lawyers will not be able to rely on bank processes such as waiting for cheques to clear to ensure that payments are made into the correct account. Be aware also that banks often do not check account numbers against the account holder's name when transferring funds via EFT. It is timely for all lawyers to revisit their procedures and processes to check they contain sufficient protections for their practice and their clients.

Ransomware and other malware

Lawcover has also received reports from law practices that have received malware delivered via 'phishing' emails, where an employee of the practice has either clicked on a link or opened an attachment. Recent cases notified under Lawcover's professional indemnity policy and the new Lawcover group cyber policy (underwritten by Barbican Insurance) have reported serious levels of damage to servers, denial of service, loss of trust account records and encryption of both local data and back-ups as part of a ransomware attack. **LSJ**