Cyber update – developments in methods of attack

Whilst cyber security is now a familiar risk subject for all solicitors, professional negligence claim notifications recently received by Lawcover provide a timely reminder that cyber related scams are always evolving, and fraudsters are developing new methods of tricking law practices or clients into transferring funds to a fraudster's account.

To avoid a claim, solicitors should always take steps to confirm the identity of the person they are dealing with, when receiving an unexpected call or email, and verbally confirm account details prior to making any transfer of funds.

Recently a law practice notified Lawcover of a significant loss of funds following a fraudster gaining access to the practice's trust account. The initial contact was made by a phone call from a person purporting to be a representative of the practice's bank. The fraudster possessed accurate details in relation to recent transactions on the account and used that information to build trust and confidence. The fraudster advised that there had been suspicious activity on the practice's account, and that the purpose of the call was to verify which of those were legitimate transactions. During the call the fraudster instructed the practice to reset their password as a security measure and during that interaction, key security details were revealed that enabled the fraudsters to gain access to the practice's account. This is an example of 'social engineering', where the goal is to manipulate people into performing certain actions or revealing private information for illegitimate reasons.

In another incident a practice was distributing funds to a client and had been previously provided with the account details by email. One transfer had taken placed when the practice received an email, purporting to be from the practice's client, providing updated account details for the second transfer of funds. The practice then sent an email advising they would be in contact to confirm the new account details. Shortly after the email was sent, the practice received an incoming call from a fraudster impersonating the client who verbally confirmed the updated account details. The practice had a policy of ensuring verbal confirmation and the solicitor mistakenly thought that they had spoken to the client when those details were confirmed.

Solicitors should always take steps to confirm the identity of the person they are dealing with when receiving an unexpected call or email, and verbally confirm account details prior to making any transfer of funds.

Unfortunately, just hearing someone's voice on the phone without taking additional steps may not be sufficient. In both of these examples, the scam could have been avoided by taking additional steps to identify a contact number through the practice's records or

Sophie Duffy
Claims Solicitor

the internet and then calling back to verify the identity of the person. When an unexpected call is received in relation to a practice's bank account or a client's account details and the person on the end of the phone is not someone whose identity and voice is instantly recognisable, Lawcover recommends taking steps to verify their identity. All calls confirming the identification or financial information of a client should be separate and outbound calls made by the practice, without prior notice of the anticipated time or date of the call. To avoid a cyber fraud claim, solicitors should always take steps to confirm the identity of a person calling or emailing, and verbally confirm account details prior to making any transfer of funds.

For more information, including step by step guidance refer to Lawcover's Guide to Cyber Security.

Have you experienced a breach?

Call 1800 4BREACH
(1800 427 322)

When holidays start, cyber criminals strike

Cyber criminals are looking for a holiday bonus and target law practices and their clients in the busy lead up to the holiday season. Be particularly vigilant about checking and verifying bank account details directly with clients on transactions settling around the end of year. Also be aware that cyber criminals present plausible excuses such as being overseas or applying fake timing pressure to create a sense of urgency, which can lead to solicitors being duped into fraudulent mispayments.

Other helpful tips to keep your practice cyber safe include:

- Confirming your IT and/or relevant service provider's operating hours and staffing availability to ensure you have adequate support should an attack occur.
- Keeping operating systems (including mobile devices), antivirus software, and all applications up to date with the latest security patches.
- Verifying websites before making online purchases. Ensure you're on a legitimate website by checking for "https://" in the URL, looking for a padlock symbol in the address bar, and confirming the website's authenticity.
- Being wary of electronic gift cards or electronic greeting cards - verify with the sender before clicking or downloading any attachments.
- Ensuring you have an up to date back up of all data to external storage in case of a ransomware attack or data loss.
- Ensuring multifactor authentication is enabled on email and web based programs to maintain an extra level of security
- Avoiding using public wi-fi. If it is essential, use a VPN (Virtual Private Network) to encrypt your connection.

Helpful resources:

Lawcover's Cyber Security Guide

Lawcover's Cyber Resources