A cautionary tale of cybercrime, identity theft and stolen trust money

Cyber risks are constantly changing, and cyber criminals are becoming increasingly sophisticated in carrying out cyber fraud.

In a recent case involving identity theft, $110,000 was stolen from a Victorian law firm's trust account, despite multi-factor authentication being implemented to access online banking and to transact from the account.

This case is an important reminder for practitioners to be vigilant, stay informed about the changing nature of cyber threats and regularly review cyber security practices and procedures.

It is not clear how the criminal first infiltrated the law firm's system to obtain the trust account details, although it seems likely that they had gained access to the Principal practitioner's email account at some point. We do know the cyber criminal accessed and used the mobile phone number, date of birth and address of the practitioner to impersonate them in dealing with their mobile phone service provider and bank to orchestrate the theft.

Timeline of events

7.30pm - posing as the practitioner, the cyber criminal logged on to the online help facility of the practitioner's mobile phone provider and was able to change the practitioner's contact details to an email address controlled by the criminal.

7.50pm - the cyber criminal then rang the mobile phone company to confirm the change in contact details and to activate call-forwarding on the practitioner's phone. With personal identification questions, call forwarding can be activated remotely without access to a physical handset. From this point, the practitioner's phone calls and messages were forwarded to a phone number controlled by the criminal.

8.50pm - the cyber criminal then telephoned the law firm's bank, 10 minutes before their telephone help was due to close, and said they were tired of using the current multi factor authentication system for accessing online banking and the firm's trust account. They instructed the bank to change over the security token being used to a SMS system where the bank sends a code to the practitioner's mobile phone.

8.55pm – the bank made the change and because the cyber criminal had forwarded the practitioner's calls and messages to the criminal's phone, they were then able to access the SMS code and transact from the trust account.

11.40pm - the cyber criminal's plan went into full swing. Over the next few hours, $110,000 was transferred from the firm's trust account in a series of transactions. Money was transferred to digital bank accounts set up by the criminal and BPAY payments were also made to a bitcoin market website.

5.30am –the practitioner logged on to check the trust account activity overnight, discovering the theft and immediately notified the bank. The practitioner's diligence in checking the account routinely meant that the fraud was identified quickly, and the bank was able to freeze the trust account to prevent further theft and recover the stolen funds.

Key takeaways – how to minimise the chances of this happening

Be mindful of distributing personal information including your date of birth and address. Secure social media accounts and profiles and carefully screen 'long lost' acquaintances who make contact.

Use a password manager and have different passwords for everything. Don't create passwords that might be easy to guess from information that is publicly available about you. If possible, don't share work phones, laptops and tablets at home or at least have separate profiles and passwords.

Ask your bank and telecommunications provider to reject any requests to change account security or details remotely by phone, email or online. It is preferable for these sorts of changes to be made in person at a branch or store with appropriate identification.

When considering multi-factor authentication, be mindful that SMS codes are less secure than using security tokens, keys, apps and smartcards. This is because the criminal doesn't need to get hold of the physical device to intercept the code or pin number if they can activate call-forwarding.

Regularly check trust account balances and activity and notify the bank immediately in the event of any unusual activity.

Relevant links

Cyber Security Guide For Lawyers

Cyber Security Checklist

Article: Client Money At Risk

Article: Enable multi-factor authentication – a simple thing that could save you

Cyber Poster – Don't fall for it!