FOUR STEPS TO STAY CYBER SAFE

Act now to protect your clients, firm and reputation against email compromise and loss of trust or client money.

Law firms and their clients continue to be hot targets for cyber criminals stealing money using email compromise schemes. Cases typically notified to the LPLC involve the loss of trust or client funds paid in real estate transactions, the settlement of disputes, distribution of deceased estates and payment of third-party invoices.

This is not a new risk, we are seeing it time and time again, but some firms are still not taking proactive steps to secure their systems and email. Others are not strengthening firm procedures to check payment details before transferring money or spreading the message to their clients. If something has gone wrong, many firms are then not acting quickly enough and funds can't be recovered.

The fact is that in almost all email compromise cases notified to the LPLC, these four simple steps could have prevented the loss of client or trust money.

Strengthen the locks

Don't underestimate the ingenuity of cyber criminals. It's essential that firms secure their systems and emails and use multifactor authentication (MFA).

MFA is simple to set up and efficient to use. It prompts staff to verify their credentials on new devices with a second form of identification before accessing firm systems and email. Once you have set it up, you don't have to manually approve access every time.

For more information about how to set up MFA and securing your systems, see LPLC's cyber security resources and cyber security guide for lawyers.

Have a safety net

Expect the worst. Despite the best endeavours of practitioners, their clients and other parties in your matters, someone's email in the chain could be unknowingly compromised.

Put in place a safety net to protect client and trust money with clear procedures for transferring money. Train staff to follow the procedures every time and without exception.

At the start of a matter take down phone numbers and other contact details for the client and relevant parties. Record them on the file.

Always call to check requests to transfer money and bank account details. Use the recorded or known contact information. Contact details provided by email should not be relied on as they may have been altered or set up by the cyber criminal and you may end up speaking to them instead of the intended recipient.

Make a file note of the discussion recording the account details and payment instructions and check them against your records.

As a final check, implement a policy ensuring that the staff member making the bank transfer confirms by phone that the checks have been done.

Spread the message

An important step in protecting clients against email compromise is also telling them to be aware of cyber risks.

LPLC has seen an increase in notifications where clients have been duped into transferring money to cyber criminals in circumstances where clear warnings by their practitioner could have avoided the problem.

Tell clients to be wary of receiving emails from the firm, or other parties, changing bank account details or with urgent or unexpected payment requests. Never transfer money without first calling the intended recipient and lawyer in charge of the file, using known contact details, to check the payment and account details.

Every practitioner has responsibility for cyber security and protecting client funds. Vigilance and critical thinking are essential when dealing with any emails, messages and calls relating to the transfer of money.

Speed is of the essence

If things go wrong and money is transferred to the cyber criminal's account, there will only be a small window for either your firm or client to potentially recover it. You need to act quickly.

Firms should immediately notify both the sending and receiving banks that money has been wrongly paid and ask them to reverse the transaction. If it's a PEXA transaction, call the PEXA Support Centre first. If the client has transferred the funds directly, contact them straight away and tell them to take these urgent steps now.

Document these procedures in an incident response plan so everyone is clear about what they need to do if your firm or client is tricked by an email compromise scam.

TIPS

- Multifactor authentication is essential to secure systems and emails. Enable it now if you have not already done so.
- Always call to check requests to transfer money and bank account details using contact information known to you. Advise your clients to do the same without exception in every matter.
- At the start of a matter record the telephone number for your client so you have trusted contact details on your file.
- If money is transferred to the wrong account, immediately call the sending and receiving banks to try to reverse the transfer. For PEXA transactions, call PEXA first.

Resources

- LPLC's cyber security resources and Cyber Security Guide for Lawyers
- Australian Cyber Security Centre: Small and Medium Businesses
- Australian Competition and Consumer Commission: Scamwatch
- LIV: Cybersecurity Learning Resources and Support & Response. ■

This column is provided by the **Legal Practitioners' Liability Committee**.
For further information ph 9672 3800 or visit www.lplc.com.au.

ADOBE STOCK