

Cybercrime alert

Since the last alert

The Trust Accounts Department has been made aware of 4 more incidents: 3 of which involving either the law practices' computers or the clients' computers being hacked, and the Rule Changes being made in Outlook (previously /discussed in other Alerts). The 3 incidents involved amounts of \$270,000, \$70,000 and \$19,000.

In the fourth incident, being very recent; and still being investigated; it would appear the computer was hacked and \$28,000 transferred from the law practice's trust account to an employee's personal account. \$10,000 was then transferred from the personal account to a Cryptocurrency account from which it cannot be recovered.

The reader may recall what the writer had to say about the Emotet Virus in an earlier alert:

- Emotet can go undetected by antivirus software and can forward itself to every email contact of the victim.
- The body of the email directs the recipient to open a word or PDF attachment.
- If Emotet has infected your computer, it can steal password and financial information.
- It will then forward itself to everyone in your Outlook address book.
- It can open a back door that will allow the cybercriminal to inject ransomware

At the time of preparing this alert the Trust Accounts Department received an email dated Sunday 31 October 2021 requesting immediate response.

The law practice involved reviews their trust account bank statements on a daily basis. The Business Manager reviewed the trust account banks statements on the Sunday and noted that sometime during Friday evening (29th October 2021) the trust account had been directly debited by \$5,000. When the writer spoke to the Law Practice's Business Manager, he said he had already been in contact with the bank on the Sunday and they had determined someone had set up a direct debit on the trust account of \$5,000 every month. We still await the outcome. It appears that we cannot stop people directly debiting solicitor trust accounts. The writer, Law Society General Counsel, and Senior Manager, Strategy and Projects have sat down with representatives of the Commonwealth Bank in an attempt to preclude this happening again. The Commonwealth Bank said they could not stop it.

SO BE VIGILANT – CHECK YOUR BANK STATEMENTS FREQUENTLY, AS DIRECTLY DEBITING TRUST ACCOUNTS HAS NOW HAPPENED ON NUMEROUS OCCASIONS, AS PREVIOUSLY REPORTED IN OUR ALERTS.

The writer also received a call early last week from someone who noticed a small credit to the trust account by PayPal. The advice given to the caller (and as explained in previous Alerts) "Contact your bank to stop any debits to PayPal accounts as someone has just established the link to debit your trust account".



Scams

The Trust Accounts Department is being inundated with calls from solicitors reporting attempts to (1) compromise their computers by sending emails allegedly from other legitimate law practices asking them to open links or attached documents or (2) falsely impersonating them to other law practices and asking that law practice to open links or attached documents. Unfortunately, it would be a never-ending task to continually report every incident, as requested by some solicitors.

Remember, do not open any links or attachments in emails if they are completely unexpected and do not open attachments from clients if you are not expecting the attachment.

As previously suggested, if in doubt Google that law practice and telephone the number given. Ask them if they have sent you an email. In all cases the email address of the sender has not been identical to that of the law practice's email address. In most cases it will appear identical, however, fails on very close scrutiny. In some cases, the email address of the sender has no resemblance at all to the proper email address.

Recommendation

If you have not already looked at the Law Society Website for 'Cyber Fraud' please click [here](#).

The Law Society of NSW and its partner insurer Lawcover are alerting lawyers about the growing risk of cyber fraud as legal practitioners increasingly shifted their businesses online due to the pandemic. This will take you to:

For more information and to download resources go to [Lawcover's website](#).

[Checklist: how to prevent cyber fraud](#)

[Flyer: reduce your client's risk of cyber fraud](#)

The Trust Accounts Department encourages all solicitors to have a conversation about Cyber Fraud with the trust account investigators during the course of all routine trust account investigations.