

CYBERCRIME ALERT

The message the Trust Accounts Department is continually putting out there is to be VIGILANT. The following incidents highlight that need. The Cyber Criminals are exceptionally good at what they do and every time we try and plug the holes they come back with a fresh approach.

Since the last alert.

The practice manager's computer had been compromised by an email received from a friend. When the principal of the law practice emailed a request to make a payment of \$153,000 to a client the email was intercepted by the hacker and the client's bank account details altered. The money was lost, and the law practice had to transfer their own funds into the trust account to cover the payment.

In another incident the law practice was awaiting the receipt of a tax invoice from a barrister. When they received the invoice for \$16,500, they made payment only to learn later the barrister had not received the payment. In this instance the barrister's computer had been hacked and the hacker was reading the barrister's emails. When the barrister prepared the tax invoice and forwarded it to the law practice the email was intercepted by the hacker prior to delivery to the law practice and the barrister's bank account details altered.

Ransomware

There has been another ransomware attack, identified as coming from Russia. All files, trust and office records were encrypted and lost to the law practice. A ransom was paid to retrieve the encryption key and restore the data.

Don't forget – a ransomware attack is only possible if someone has downloaded the malware. Hence, the need to be forever vigilant. Do not click onto links or open attachments from people/organisations you do not know, and where you do know them, where you are not expecting any such attachment.

Recent SCAM

The solicitor was contacted by persons who convinced him they were from the Fraud Units of (1) the ANZ Bank and separately (2) Amazon. They provided very convincing identifications and he allowed them access to his computer. Once in, they identified 5 bank accounts including the trust bank account, and the passwords to these accounts.

They emptied the various bank accounts of many thousands of dollars including \$16,000 that was transferred out of the trust account into the business account.

The solicitor personally restored the \$16,000.

BE AWARE AND BE VIGILANT.

These scammers are very convincing and the documents they produce are very authentic looking. These people can get enough information of you to serve their purpose by 'GOOGLING' your website.